BANKING FRAUDS: REFORMS BY GOVERNMENT AND ARTIFICIAL INTELLIGENCE

Shruti Sinha*

ABSTRACT

The economy of a country is its driving force, and the driving force of the economy is Banks. Anything that happens to the banks is inevitably reflected in the whole market, that is why, the maintenance of their health is of utmost importance for the efficient functioning of the economy and consequently, the country. One of the biggest challenges faced herein since the very existence of such systems has been that of the Banking Frauds, and as a matter of concern, it has only continued to increase ever since, in terms of both quantity and quality. Accordingly, the authorities have also consolidated themselves with contemporary advancements to tackle 'modern problems with modern solutions'.

Keywords: Bank, Fraud, RBI, Artificial Intelligence.

"Cash is King, but Digital is Divine."

-Reserve Bank of India [1]

INTRODUCTION

It is not a matter of doubt that Banks are the 'backbone' of an economy. They manage not only the national market along with its international operations but also the finances of the government as well as the entire population. The Central Bank i.e., the Reserve Bank of India

*FIRST YEAR, BLS LLB, GOVERNMENT LAW COLLEGE, MUMBAI.

[1] Reserve Bank of India, *Assessment of the progress of digitisation from cash to electronic* (2020) <https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/CASHB74203395BD64E2ABC1BD5F68D8AEF13.PDF>

(RBI), controls the flow of money in the market, and increases decreases, or stabilizes it, in view of the present requirements of the economy. Hence, the proper functioning of the banking sector is vital for controlling large-scale matters like inflation, unemployment, income levels, etc. And a major hindrance to this subject shall be that by the Banking Frauds, especially the online ones these days. With the era of technological evolution, in addition to the exponential rise in the precedent cases, the frauds in banks have now expanded their range to the digital dimension of the financial sector as well.

WHAT IS A FRAUD?

Fraud can be defined as the commission of an act, or the omission of an act when one had been bound to do so, or the manipulation or forgery of evidence to fake legitimacy, for the availment of unauthorized access or wrongful enrichment, causing financial injury to an individual or organization, including the government and banks. As per Section 17 of the Indian Contract Act, 1872[2], conditions that constitute a Fraud include:

- Suggesting a fact to be true when one knows or believes it to not be true
- Actively concealing a fact, one has the knowledge or belief of, despite having the duty to disclose it
- Promising without any intention of performing such
- Doing any other act that may deceive
- Commission or omission of any act that has been declared fraudulent by the law

In India, the RBI has been conferred with the authority to monitor and control monetary transactions as well as issue the guidelines thereof, under Section 35A of the Banking

[2] Indian Contract Act, 1872 <https://legislative.gov.in/sites/default/files/A1872-09.pdf> Page 14

Regulation Act, 1989. Hence, according to its master guidelines [3], the cases of Fraud can be classified into:

a) Misappropriation or Criminal Breach of Trust
b) Cheating or Forgery
c) Obtaining money via manipulation of documents, fake accounts, conversion of property, etc.
d) Obtaining money via unauthorised access to accounts or identity theft
e) Cash shortages and the Negligence thereof
f) Irregularities in foreign exchange
g) Any other type of fraud aside from the abovementioned

STEPS BY THE GOVERNMENT

The RBI is the primary body that lays down the 'recourses of action' dealing with the problems related to banks. It strives to spread financial awareness so that people save themselves from getting into such predicaments beforehand. After all, another major reason behind the bank fraud is the ignorance of the system guidelines by the people, including the banking staff.

Illustration: The Punjab National Bank (PNB) Scam, 2018, of more than Rs. 10000 crore, by Nirav Modi, Mehul Choksi, and others, is dubbed as one of the biggest frauds in the timeline of Indian banking. It had happened because of the overlooking of the RBI guidelines, regarding the import of precious gems, by the overseas branches of Indian banks, due to which proper communication of information to the PNB could not happen. Later, taking the advantage of this oversight, the offenders had defrauded the PNB, with more than 1200 fake guarantees,

[3] Reserve Bank of India, *Frauds – Classification and Reporting* (2009) <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/58FLC010709_F.pdf >

availing a sum of approximately Rs. 14000 crores therefrom. Such had not been detected for almost six years, from March 2011 till May 2018, owing to a blind spot in the SWIFT network technology, used for inter-bank communication that had been misused by the PNB employees to prevent the recording of transactions in the core system of the bank management.

To prevent the cases such as the one illustrated above, several comprehensive measures have been taken by the government [4], such as:

- A "Framework for timely-decision, reporting, investigation, etc. relating to large value bank frauds" had been issued to the Public Sector Banks (PSBs) for the evaluation of their Non-Performing Assets (NPAs)– any account exceeding the sum of Rs. 50 crore, if classified as an NPA, shall undergo examination for detection of any potential fraud and the report of the findings thereof shall be submitted to the bank's Committee for Review of NPAs.
- Fugitive Economic Offenders Act, 2018– allows the government to confiscate the property of the offender and disentitles them from defending any civil claim.
- PSBs have been advised to obtain a certified copy of passports of the authorities of a company availing a loan of more than Rs. 50 crores.
- PSBs have also been given permission to publicly publish the photographs of frauds as approved by the board.
- PSBs have been directed to strictly ensure the rotational transfer of all their employees at the due times.
- The government has established the National Financial Reporting Authority to ensure adherence to the auditing standards and evaluate the quality thereof.

[4] Ministry of Finance, *Comprehensive measures taken to curb incidence of frauds in Banks* (*PIB Delhi* July 27, 2021) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1739661> accessed 13 April 2022

Aside from these traditional reforms, the help of technologies like Artificial Intelligence is also being deployed to combat the battle against cybercrimes.

BANKING FRAUDS VS ARTIFICIAL INTELLIGENCE

With the lightning-paced developments in technology, a new arena has been opened to propagate crimes. Currently, cybercrimes are a hot topic in India. Understandably so as India has ranked the third globally, in the number of cybercrimes reported in 2020[5], and the majority of these cases, as high as 45 percent of the cybercrimes, have been that of online financial frauds[6]. There have been a lot of ways of online defrauding lately, like:

- Phishing– Fraudsters circulate links through messages, attachments, advertisements, and other media, clicking on which redirects to fake pages, identical to the original websites of banks, e-commerce platforms, social media, etc., where their targets fill in their credentials, and those get stolen.
- Vishing / Wire Fraud– Imposters acting as the representatives of banks, firms, insurance agencies, government, etc. contact people on the phone or other media, to obtain information such as passwords, OTPs, PINs, etc. through trickery or persuasion, and gain unauthorized access to their accounts.
- Malicious apps– Fraudsters prompt to download unknown apps via messages, advertisements, freebies, etc., installing which provides them access to the target's device for getting information such as OTPs or already-stored credentials.

[5] Internet Crime Complaint Center, *Internet Crime Report 2020* (2021) 17 <https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf>

[6] Pushpita Dey, 'Banking Frauds Using Communication Devices Rose By More Than 65% Post Covid' (*Outlook India*, 18 December 2021) <https://www.outlookindia.com/website/story/business-news-banking-frauds-using-communication-devices-rose-by-more-than-65-post-covid/405699> accessed 15 April 2022

- ATM Card skimming– Devices are installed in the ATM machines that can copy the data from the target's ATM card as well as its PIN using which money can be withdrawn.
- SIM Card cloning– Fraudsters may duplicate the Subscriber Identity Module (SIM) card of the registered mobile number linked with the bank accounts to steal the identity of the target and defraud them.
- QR Code scam– Fraudsters may trick their targets by making them scan malicious Quick Response (QR) codes which would provide them hidden access to the target's device for gaining information.

Moreover, alarmingly, the number of online financial frauds has doubled since the advent of Covid-19. One way these fraudsters may catch tartar is by making them taste their own medicine. With more and more financial institutions turning to AI and Machine Learning (ML) tools to solve this problem, spending more than $217 billion, it has been reckoned that the usage of such technologies has helped reduce the investigation time by 70 percent and has improved the accuracy of fraud detection by 90 percent[7].

Some ways through which the AI and ML may integrate themselves with the banking system to help ensure the safety of the consumer are:

- Many tech companies, like Teradata and Datavisor, program personalized AI fraud detection software for banks.
- AI software analyse the transaction patterns of the consumers, builds profiles based on such data, and detects in case anomalous action happens.

[7] PYMNTS, 'How AI And Machine Learning Can Address Banks' Fraud-Fighting Weaknesses' (*PYMNTS*, 09 July 2021) <https://www.pymnts.com/fraud-prevention/2021/ai-ml-banks-fraud-fighting/> accessed 15 April 2022

- AI surveillance at ATMs and offices, like that provided by Uncanny Vision, monitors the actions of the person, informing in case of any suspicious activity.
- Biometric security scans the unique biological prints of a person like that of the retina, thumb, and fingers, to confirm the identity.
- Know Your Customer (KYC) integrates all the information, including the biometric ones, to prevent unauthorised access with multiple-stage authentication.
- Security software warns against the downloading of unknown apps that have not been verified by them and are likely to cause unauthorised harm to the device.
- Email platforms, like Gmail, detect millions of spam messages every minute that could phish its consumers had it not been discarded.
- Various software, like the TrueCaller app, identifies spam or fraud calls and informs of such beforehand. Some insurance companies also use similar apps to detect potential fake claims.

The usage of AI in fighting fraud is not only secure and faster but also maximizes the user experience, giving personalised solutions, and reducing the possibility of human mistakes or expenses. AI is a self-learning program that automatically updates and adapts itself in real-time to give as efficient and effective solutions as possible.

SUGGESTIONS AND CONCLUSION

However, in the end, it is one's duty to take the proper preventive measures, so that the question of fraud compensation never arises. In that view, the RBI has advised the banks to take some steps to improve the customer's security, like:

- Enable two-factor authentication
- Convert strip-based cards into chip-based cards that have better encryption

- Assign threshold limits to the usage of cards
- Regularly confirm the user's identity
- Send alerts of transactions or other important activity
- Velocity check of the number of transactions per day

Similarly, consumers are also advised to not disclose their confidential information to anyone else and to financially educate themselves to be able to understand the system better and follow the guidelines more properly. The safety of each person is in their own hands. Effective as it may be, the system of AI, however, is not full-proof security. Some experts show concern over the fact that AI is not much transparent and can also be bypassed. Hence, it is up to the consumers to be smart and not fall for such trickery.