

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

---

Volume 5 | Issue 6

---

2022

© 2022 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

---

This article is brought to you for “free” and “open access” by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact [Gyan@vidhiaagaz.com](mailto:Gyan@vidhiaagaz.com).

---

**To submit your Manuscript** for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to [submission@ijlmh.com](mailto:submission@ijlmh.com).

---

# Financial and Systemic Fraud

---

MUSKAN SHARMA<sup>1</sup> AND SAVYA ATREY<sup>2</sup>

## ABSTRACT

*Systematic Financial frauds are widely regarded as white-collar crimes that not only affect the general society but also have a negative impact on the economy. White-collar crimes are non-violent crimes that are carried out for personal financial gains. In most cases financial frauds involve misappropriation or manipulation of public funds for the financial gains of fraudsters. What is surprising is that with the evolution of technology these frauds have only increased. India as a country has seen many big online financial frauds over the years. The fraudsters commit such crimes online hiding behind the anonymity that the Internet offers. Even though it is not easy to give an exhaustive definition to the term financial frauds it can be regarded as the intentional act of deception that involves financial transactions. However when such an act is carried out online with the help of technology it is known as online financial frauds. Some examples of online financial frauds include KYC frauds, Identity Frauds etc. Nevertheless steps have been taken by the legislators to hold these fraudsters accountable and to ensure that the online financial frauds are reduced in number. The legislative framework that helps in the same includes the Information Technology Act, 2000 and Indian Penal Code, 1860. The above has been discussed in detail in the subsequent parts of the paper.*

**Keywords:** Financial Frauds, Economic Growth, Preventive Measures.

## I. INTRODUCTION

When someone intentionally deceives a person in a wrongful manner it is referred to as fraud. Whereas financial frauds take place when an individual is deprived of his money or financial health through acts that are deceptive, misleading or involve practices that are illegal.<sup>3</sup> When such frauds take place on an online platform they are known as Online Financial Frauds. They target a large number of individuals every year through different online modes. Various types of Online Financial Frauds have been identified over the years and the same have been discussed in detail below. They are-

1. **Phishing-** Phishing is one of the most widely used modes by cyber criminals. In this type of online Financial Frauds a cyber criminal targets an individual by contacting them

---

<sup>1</sup> Author is a student at Symbiosis Law School, Pune, India.

<sup>2</sup> Author is a student at O.P Jindal University, India.

<sup>3</sup> Prof. Milan Ram, Financial Frauds in India, Vol. 8, IJMR, PP. 276, (2018).

through emails, phone calls or text messages. They use the data available in the public domain to make the first contact. They then pose to that individual as someone from a legitimate institution in order to extract important and sensitive data from them. This data they usually sought to extract includes personal information relating to the identity of such persons, banking details, credit card details, important passwords, etc.<sup>4</sup> These details are then either monetized by the fraudsters by selling it in the dark web or is used to make fraudulent payments. This sensitive information can also be used for identity theft or impersonation.<sup>5</sup>

2. **Malware-** Malware attacks are also a common type of online financial frauds wherein a malware, which is normally malicious, carries out unauthorized actions of the victims computer system. The fraudsters with the help of such malwares scan the entire network of a computer with the intention of gaining information regarding financial transactions. This is done in order to commit online banking frauds.<sup>6</sup> These malwares are so able that they have the ability to bypass sophisticated technologies that are specifically built to protect the sensitive information of the financial institutions as well as the customers.
3. **Mobile Device Threats-** In the recent years mobile phones have become an indispensable part of our lives. With payments being made through mobile phones and mobile banking becoming the new norm it has as a result has become a lucrative place of attack for the fraudsters. Even though most of the threats are the same as that on a computer, the only difference is the fact that mobiles unfortunately do not offer the same level of protection that a desktop offers. The fraudsters thus end up stealing the secured financial information stored in the device through hacking, malwares, etc.<sup>7</sup>
4. **Payment Systems Compromise-** While making online payments, Payment Service Providers provide a safe and secure gateway or terminal for payments. They do so by processing data from diverse channels that include face-to-face card payments, online payments and contactless payments. These service-providing platforms are often a great target for online financial fraudsters as they can target them in order to seek the payment data. This is done by either compromising the software vulnerabilities or by exploiting the unauthorized access to these gateways.<sup>8</sup>

---

<sup>4</sup> Phishing Org, <https://www.phishing.org/what-is-phishing> (March 27, 2022, 7:30 PM)

<sup>5</sup> Jyoti C, [hishing and Anti-fishing Techniques: Case Study, Vol 5, IJARCSSE, (2013)

<sup>6</sup> Rieck, K., Holz, T., Willems, C., Düssel, P., Laskov, P, Learning and Classification of Malware Behavior. Vol 5137, LNSC(2008).

<sup>7</sup> Reader's Digest, <https://www.rd.com/article/mobile-security-threats/>, (March 27, 2022, 8:30 PM)

<sup>8</sup> Upasana Ghosh, Online Financial Frauds And Cyber Laws In India - An Analysis, Vol. 10, VOR, (2021).

## II. LEGISLATIVE FRAMEWORK GOVERNING ONLINE FINANCIAL FRAUDS

Various legislations are in place in order to curb these online financial Frauds. Some of these legislations include the Information Technology Act, 2000 and the Indian Penal Code, 1860. The specific legal provisions have been enlisted below-

- 1) **The Information Technology Act, 2000-** Various sections of this Act deal with online financial frauds for instance section 66C of the act deals with the Punishment for Identity Theft. It gives out the punishment for the dishonest or fraudulent use of electronic signature, passwords, etc.<sup>9</sup> Additionally Section 66D of the I.T Act, 2000 deals with the Punishment for cheating by using Computer Source and prescribes the punishment for personation that is done through any communication device or computer source.<sup>10</sup> On the other hand Section 43 of the act deals with the penalty and compensation for damage to a computer system and states that if any individual without prior permissions destroys, uses, or alters the information on a computer with the intention of damage will be liable to pay damages.<sup>11</sup> Furthermore, Section 43 A prescribes the Compensation to be given incase the corporate body dealing with the sensitive information fails to maintain reasonable security measures.<sup>12</sup>
- 2) **Indian Penal Code, 1860-** In case the provisions of the IT Act are Insufficient the law enforcement authorities can penalize the fraudsters under various sections of the Indian Penal Code. For instance section 379 of the act prescribes the Punishment for theft and since many online financial crimes take place through stolen computers and mobile phones, this section is applicable.<sup>13</sup> Similarly Section 420 of the act can be used to implicate the fraudster. Section 420 deals with Cheating and dishonestly inducing delivery of property. Many cyber crimes take place through creation of fake websites and the same are chargeable under this section.<sup>14</sup> Additionally, section 463 of the Act is also applicable as it deals with the creation of false documents or electronic records and prescribes the punishment for the same.<sup>15</sup> Another section is Section 468 that talks about the commission of forgery with the intention of cheating. The online fraud of email spoofing is punishable under this section.<sup>16</sup>

---

<sup>9</sup> Information Technology Act, 2000, Section 66C, 21, Acts of Parliament, 2000 (India).

<sup>10</sup> Information Technology Act, 2000, Section 66D, 21, Acts of Parliament, 2000 (India).

<sup>11</sup> Information Technology Act, 2000, Section 43, 21, Acts of Parliament, 2000 (India).

<sup>12</sup> Information Technology Act, 2000, Section 43A, 21, Acts of Parliament, 2000 (India).

<sup>13</sup> Indian Penal Code, 1860, Section 379, 45 Act of Parliament, 1860 (India).

<sup>14</sup> Indian Penal Code, 1860, Section 420, 45 Act of Parliament, 1860 (India).

<sup>15</sup> Indian Penal Code, 1860, Section 463, 45 Act of Parliament, 1860 (India).

<sup>16</sup> Indian Penal Code, 1860, Section 468, 45 Act of Parliament, 1860 (India).

### **III. ROLE OF AUTHORITIES AND GOVERNMENT IN TAKING PREVENTIVE MEASURES TO PREVENT ONLINE FINANCIAL FRAUDS**

Even though every individual should be responsible and should take adequate measures to ensure that he is safe from all types of financial frauds, it is the duty of the legislators, judiciary and well as other regulators to ensure that stringent laws are created to punish the fraudsters. At the same time a mechanism is created in order to protect and help the victims. With the increasing number of financial frauds and the subsequent harm to the public and society in general various steps and preventive measures have been taken by the Legislators, government and other stakeholders in order to prevent online financial Frauds. This includes-

- 1) The Indian Ministry of Home Affairs has composed inter- Ministerial Committee on Phone Frauds which includes members from the Ministry of Electronics and Information Technology, Department of Financial Services, Department of Telecommunication, Reserve Bank of India and law enforcement agencies.<sup>17</sup>
- 2) An advisory has been issued to all the states by the Centre on steps to check phone frauds.<sup>18</sup>
- 3) The central government launched a National Cyber Crime Reporting Portal that allows all victims to submit complaints against all types of Cyber crimes including online financial frauds.<sup>19</sup>
- 4) The central bank that is the Reserve Bank of India has on various instances has released guidelines for safe digital banking in order to create consumer awareness and prevent frauds like phishing, Remote Access, etc.
- 5) Various Online fraud awareness programs are organized regularly to educate the citizens against such frauds.
- 6) Banks and Payment Gateways that regulate online payments send messages to the customers regularly informing them that the OTP should not be shared and further that their employees never ask for the OTP.<sup>20</sup>

### **IV. SUGGESTIONS TO IMPROVE LEGAL SYSTEM TO DEAL WITH FINANCIAL FRAUDS**

From the above discussion it is amply clear that there are various provisions and laws in place

---

<sup>17</sup> Ministry of Home Affairs, India Website, <https://www.mha.gov.in/>, (March 27, 2022, 8:30 PM)

<sup>18</sup> Ibid.

<sup>19</sup> National Cyber Crime Reporting Portal, [www.cybercrime.gov.in](http://www.cybercrime.gov.in), (March 27, 2022, 9:30 PM)

<sup>20</sup> Reserve Bank of India, [www.rbi.org](http://www.rbi.org) (March 28, 2022, 10:00 AM)

that deal with online financial frauds. However in the last two years there has been a reported rise of about 12 percent in the number of such cases. The police is finding it difficult to address and solve such crimes due to issues relating to jurisdiction, unaware public as well as the increase in cost of investigation due to use of sophisticated technology. Therefore it is important that a specialized department be made within the police that specialize with the same. Additionally the laws must be regularly updates as the fraudsters are using new and new techniques. Coordination and cooperation between departments should be encouraged that will help in making the investigation easier. Apart from the above citizens should be made aware about being cautious about these frauds and two step verification must be enabled on all apps. Complaint mechanism should be made easier and regular regulations must be issued by the Ministry of Electronics and Information Technology, Department of Financial Services, Department of Telecommunication, Reserve Bank of India and law enforcement agencies in order to fight this menace.

## **V. CONCLUSION**

Therefore, from the above discussion it is safe to conclude that ever since the Internet and technology has grown, financial frauds too have grown at the same pace. With everything from payments to investments being made online, fraudsters have devised different ways to trick people and misuse their funds. Even though online financial frauds are governed by legislations like the Information Technology Act, 2000 and the Indian Penal Code, 1860 the crimes have only increased. The government too has taken up preventive measures like launching a Ministerial Committee on Phone Frauds and e-complaint platform to curb this menace. However, it has become imperative for the regulators and stakeholders to take this up in a stricter manner and to create awareness about these kinds of frauds and regularly give out regulations that deal with the same.

\*\*\*\*\*

**VI. REFERENCES****(A) Research papers-**

- 1) Sood, P., Bhushan, P. A structured review and theme analysis of financial frauds in the banking industry. *Asian J Bus Ethics*.
- 2) Prof. Milan Ram, *Financial Frauds in India*, IJMR.
- 3) Jyoti C, [hishing and Anti-fishing Techniques: Case Study, Vol 5, IJARCSSE.
- 4) Rieck, K., Holz, T., Willems, C., Düssel, P., Laskov, P, *Learning and Classification of Malware Behavior*, LNSC.
- 5) Upasana Ghosh, *Online Financial Frauds And Cyber Laws In India - An Analysis*, VOR.

**(B) Statutes-**

- 1) *Information and Technology Act, 2000*
- 2) *Indian Penal Code, 1860*.

**(C) Website-**

- 1) *National Cyber Crime Reporting Portal*, [www.cybercrime.gov.in](http://www.cybercrime.gov.in).
- 2) *Reserve Bank of India*, [www.rbi.org](http://www.rbi.org)
- 3) *Ministry of Home Affairs, India Website*, <https://www.mha.gov.in/>
- 4) *Phishing Org*, <https://www.phishing.org/what-is-phishing>
- 5) *Reader's Digest*, <https://www.rd.com/article/mobile-security-threats/>

\*\*\*\*\*