BEYOND THE SCREEN: THE SILENT CRISIS OF ONLINE FINANCIAL EXPLOITATION IN INDIA

Paridhi Sankhla, Gujarat National Law University, Silvassa Campus

ABSTRACT

This article explores the burgeoning epidemic of cyber-enable financial crimes and their disproportionate impact on India's most vulnerable populations. As India undergoes a rapid digital transformation, a surge in scams – ranging from AI-driven deepfakes and "digital arrests" to predatory lending apps which has created a pandora's box of cyber-crime. This article identifies the elderly, low-income individuals, rural women and students as primary target, citing low digital literacy, socio-economic pressure and psychological manipulation as key driver of their vulnerability.

Despite the existence of Information Technology Act, 200 and RBI guidelines, the study reveals that justice is frequently stalled by jurisdictional hurdles, low conviction rates etc. Ultimately, online fraud as a matter of social injustice, calling for transition from receiving policing to a victim centered model that prioritizes localized digital literacy and hold platform intermediaries accountable to protect most vulnerable citizen.

Keywords: Cyber Crime, Digital Literacy, Predatory Lending Apps, Digital Arrest, Phishing, IT Act, RBI regulation.

Introduction

What is online fraud and how certain group of people are more vulnerable to this more than other? Online fraud also known as internet fraud involves internet services and access to internet-based application to take advantage of victims in form of extorting money. It is broad category of cybercrime consisting of various types of frauds, such as identity theft, investment scam, phishing scams, online shopping scam, lottery scam, job offer scam etc. Online fraud is a pandora's box, if you compare the frauds committed in early 2000's to the present you will realize how the growth of technology was both boon and bane for the society, scams took place on a large scale, ranging from phishing and identity theft to UPI scam, investment scam etc. With the increasing technology like AI driven social media and deepfakes, the number of online crimes have increased by fivefold in India.

Identifying At-Risk Population

Certain group of population are more vulnerable to these frauds than others, elderly, low-income individual, rural women, unemployed and student are prey of these scammers. Elderly citizen are mostly unfamiliar with the growing technology and many senior citizens fall for this trap of scammers who often pretend to be from banks or government institution. Nowadays a new scam called "digital arrests" going on in India where people will receive a call from a person impersonating to be a police officer, judge or government official, they use video call and fake documents to create an illusion, sense of urgency and authority to extort money. Most of the elderly are unaware of such people and they tend to believe that they are true and fall into the trap of these scammers.

After elderly, the target of these scammers are the people belonging to low-income groups of society who are in dire need of money to keep their household running with their limited knowledge and access to education and internet literacy, they lack awareness of safe digital practice. Due their lack of awareness they become an easy target of scammers. Then we have women in conservative or underserved area or women who are often financially dependent on their husband, father or any patriarch of the family. As these women are financially dependent and excluded from decision making, such women are easy target for instant loan and investment scheme. Student and people searching for jobs are lured by the promise of scholarships, internships or part-time job through fake websites and emails. These scammers identifies a particular set of people who will be their target and these are the individual wo use digital service without understanding the proper functions and risks involved.[1]

Barrier to Digital Inclusion

According to National Sample Survey-based Analysis only 38% of households in India are digitally literate compared to 61% of digital literate in urban areas, rural area only 25% people are digitally literate. In this report it was also revealed that Schedule Tribes have the lowest digital literacy at the household level at 21%.[2] Vulnerable groups of society are targeted by these scammers because of their predictability, psychological traits and limited exposure to technology. These group of people are target because they have low awareness and digital literacy because of which many of them are not able to differentiate between legitimate and fraudulent digital platforms. Victims of these crimes often believe in the communications from those posing as government or bank officials. Many victims are unaware about how and where to report these frauds. To increase the credibility the scammers, use regional or local language to gain the trust of people. Finally, the socioeconomic pressure such as unemployment or financial distress make individuals more likely to fall for scams offering quick loans, jobs or investment opportunities that appear too good to be true.

The Instant Loan App Crisis

One of the most alarming cases of Online fraud and digital exploitation that took place in India occurred between 2019 and 2021. A sudden rise of unregulated instant loan apps in Indian market, many were found to be linked with Chinese shell companies. These apps often appeared on platform like Google play store with any registration from RBI or NBFC affiliation. These apps offered unsecured loan with minimal requirement of documentation from the victims. Their main target were individual who were financially distressed and who were in dire need of funds. Once these apps are installed, these apps typically requested access to user’s contact list, gallery, message and location. Granting this permission gave these shell company access to private information, extensive data collection and surveillance.[3] After the

[1] DIGITAL EMPOWERMENT FOUNDATION, https://www.defindia.org/wp-content/uploads/2025/04/ASPEN-HP_Project-Report-Final.pdf (last visited Feb. 1, 2025).

[2] Venugopal Mothkoor and Fatima Mumtaz, *The digital dream: Upskilling India for the future*, IDEAS FOR INDIA (Mar. 23, 2021), https://www.ideasforindia.in/topics/governance/the-digital-dream-upskilling-india-for-the-future; TIMES OF INDIA, https://timesofindia.indiatimes.com/technology/tech-news/digital-literacy-and-the-future-of-work-reflecting-and-preparing-indias-youth-for-the-digital-economy/articleshow/125830356.cms (last visited Feb. 9, 2025).

[3] Anil Kumar, *The Dark World of Illegal Loan Apps in India*, AL JAZEERA (25 December 2023), https://www.aljazeera.com/economy/2023/12/25/the-dark-world-of-illegal-loan-apps-in-india.

loan was given, which usually ranges from ₹1,000 to ₹10,000, the repayment period of this loan was from 7 days to 14 days. The loans were provided on interest rate which varied from 35% to 500% which is unusual. The short period of repayment and high rate of interest was to something that most people ignored while applying for the loan. If someone delayed or defaulted on loan, recovery agents, of using Artificial Interest (AI) to alter the images, often resorted to coercive tactics like persistent calling, threats of police action, public humiliation and altering harmful messages with the contacts taken from the victims' phones.

This shows that when a person is in pressing need of money they forget about checking the rate of interest, period of repayment time and validity of person providing the loan. A 2021 report from Reserve Bank of India highlighted that over 600 such apps were flagged during its examination of digital lending platform.[4] Sadly, suicide was committed by people which was directly linked to the shame and distress caused by these app operators. In one case, 23-year-old tech worker from Hyderabad committed suicide because of the harassment by loan recovery agents. The tech worker was found hanging by a ceiling, he committed suicide after he struggled to repay the loan and facing threats regarding his family's safety and his reputation. This situation prompted an action from state cyber-crime department and central Ministry of Electronics and Information Technology (Meity), which instructed app stores like google play store to remove around 150 illegal lending apps in January 2021. Later, in September 2022, the RBI issued a circular outlining guidelines for digital lending.[5] These guidelines included mandator loan terms disclosures, a ban on user accessing user contacts and media and required registration of lending entities with RBI-approved NBFCs or banks. This scandal not only revealed serious weakness in India's fintech regulation but also highlighted the risk of digital financial inclusion without proper protection. It stressed the need for better consumer education, more rigorous app verification process and legal responsibility for platform intermediaries like google.

Phishing and "Digital Arrest": Targeting the Elderly

In 2022 Delhi police's cyber cell recorded a significant increase in phishing case targeting older

[4] Government of India Ministry of Finance Department of Financial Services, *Illegal Digital Lending App*, Lok Sabha Unstarred Question No. 4113 (Mar. 28, 2022), https://sansad.in/getFile/loksabhaquestions/annex/178/AU4113.pdf?source=pqals.

[5] RESERVE BANK OF INDIA, https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/DIGITALLENDINGF6A90CA76A9B4B3E84AA0EBD24B307F1.PDF (last visited Feb. 1, 2025).

adults mostly above 60-year-old. Elderly are among the most susceptible age group in the age of cyber fraud, mostly because of limited exposure to technology, dependence on other persons when it comes to money matters, and a cultural element of trusting people in authority. These frauds were frequently carried out by individuals impersonating bank employees, police officer or income tax officer. Making unsolicited phone call or sending unsolicited emails that evoked fear or sense of urgency- warning of unpaid taxes are frozen accounts or impending legal action was the scammers modus operandi. The victims were informed that they had to "verify" or "reactivate" their accounts by providing sensitive data, including PAN numbers, Aadhaar information, one-time passwords (OTPs), or net banking passwords. They would gather such data, and before the victims realized what was happening, scammers rapidly carried out unauthorized transfers on UPI platforms or internet banking. A total of over 400 senior citizen cases were reported in the National Capital Region in the year 2022, as per figures made public by the Delhi Police Cyber Crime Unit. The per-victim average financial loss varied between ₹50,000 and ₹2,00,000, while in a few instances, victims lost as much as ₹5 lakhs before realizing they had fallen prey to a scam.1 The Reserve Bank of India has constantly warned consumers against sharing credentials over the phone, but fear of reprisals and limited digital acumen have rendered senior citizens the easiest prey. There was one high-profile case where a retired government servant was tricked into transferring more than ₹1.75 lakhs after being informed that irregularities in his pension account would result in its suspension. Another much-publicized one was that of an 82-year-old widow who lost ₹90,000 after receiving a call allegedly from her "bank manager" informing her of a KYC failure. Even after several campaigns, underreporting is a significant concern since the victims do not want to acknowledge being duped, particularly when large amounts or family savings are involved. It highlights an immediate need for specific digital literacy training for senior citizens, easy-to-use banking interfaces, and effective support systems for cyber fraud victims.

The Human Cost: Socio-Psychological Impact

According to data which is presented in Lok Sabha India lost ₹107.21 crore to online fraud in first three quarters of ongoing financial year (FY25), with 13,384 cases. National Crime Record Bureau published data stating the number of cases registered under Fraud for cyber-crime during the year 2020, 2021 and 2022 are 10395, 14007 and 17470 respectively.[6] The impact of

[6] Team Angel One, *India Reports Over Rs 107 Crore in Cyber Fraud Losses in First Three Quarters of FY25*, ANGEL ONE (Mar. 11, 2025, 2:37pm IST),

financial fraud committed through the internet is extensive, stretching much beyond immediate monetary harm and casting profound impact on socio-psychological well-being of victims. For many victims, especially prisoners, working women who are day to day wage earner and homemakers, a small financial loss can be crippling.[7] In a number of reported cases, victims have lost all their life's savings, with no institutional relief to soften the blow. Additionally, fraud committed through predatory loan apps often lands victims in a vicious loop of sky-high repayments, harassment, and extortion. In addition to monetary loss, victims usually suffer from psychological trauma characterized by shame, guilt, and humiliation. The psychological impact is always underestimated—victims self-blame for being "naive" or "careless", and such self-stigmatization may lead to extreme anxiety and depression. No less disconcerting is the erosion of confidence of people in online system. The majority of victims particularly older people, chose to avoid online monetary transaction entirely once they have been cheated. This reluctance not only deprive them of essential financial services but also slows nation's larger aspiration toward digital inclusion initiatives like Digital India. Women also have peculiar post-fraud challenges; societal perceptions tend to blame them personally, labelling them irresponsible or reckless. This blame is often initiated in their own family environments, isolating them further. In extreme situations, this results in victims digitally becoming invisible—avoiding any kind of online banking or payments lest they be scammed again. More importantly the process of getting justice itself becomes a kind of exercise in secondary victimization. Victim suffers police apathy, jurisdictional ambiguity and procedural delay, which further fuel their feeling of helplessness and frustration. The shame of being cheated along with the of lethargy of institution denies recourse to many victims.

Online fraud is essentially not much of a technical and criminal problem- it is very much a serious human right and social injustice issue. Its impact reverberates through economic marginalization, emotional breakdown and virtual isolation. Therefore, an effective response must extend beyond repressive law and computer protection. It should include victim centred practices, including psychological counselling, legal aid, efficient redressal mechanisms and extensive public education drives. It is only b reducing the long-term damages of online exploitation and offering all a safer digital environment through such integrated engagement,

https://www.angelone.in/news/market-updates/india-reports-over-rs-107-crore-in-cyber-fraud-losses-first-three-quarters-fy25.

[7] Danish Sufi, Prof. Jagrati Patel and Dr. Geetha Sarasan, *Beyond Monetary Loss: Mental Health Impacts of Online Financial Fraud in India*, 8 IJFMR, 8 (2026), https://www.ijfmr.com/papers/2026/1/67268.pdf.

especially its most vulnerable members.

The Indian Legislative Shield: IT Act and RBI Mandates

In order to combat online frauds, India has a proper legal and regulatory framework that combines legislation, institutional apparatus and statute law. The IT Act of 2000[8] serves as the turning point from the legislative point of view and is used as a primary legal instrument to punish the people committing fraud online and establishing the validity of online business. Section 66C[9] under this Act criminalizes identity theft by punishing the dishonest or fraudulent use of another person's digital signature, password, or distinct identification feature with a penalty of up to three years' imprisonment and/or fine. Section 66D[10] also addresses cheating by personation by electronic means by laying down the same period of punishment. These provisions are complemented by archaic criminal law mechanisms incorporated within the Indian Penal Code (IPC). Section 419 criminalizes cheating by personation, and Section 420 addresses broader cases of cheating and dishonestly inducing the transfer of property—provisions commonly called upon during digital fraud investigations.

Regulatory framework-wise, the Reserve Bank of India (RBI) is an absolute necessity in issuing binding instructions to financial institutions for anti-fraud purposes. These include compulsory adoption of customer due diligence (CDD) practices, two-factor authentication for online transactions, and grievance redressal mechanisms in banks.[11] Further, the Indian Computer Emergency Response Team (CERT-IN) under the Ministry of Electronics and Information Technology functions as the central agency for the monitoring of cyber threats, putting out advisories, and coordinating responses to cyber security incidents. Another important initiative has been the establishment of the National Cyber Crime Reporting Portal (www.cybercrime.gov.in), a centralized online portal enabling victims to lodge complaints online with a view to making the grievance redressal and law enforcement response system more streamlined.

[8] Information Technology Act, No. 21, Acts of Parliament, 2000 (India).
[9] Information Technology Act, § 66C, No. 21, Acts of Parliament, 2000 (India).
[10] Information Technology Act, § 66D, No. 21, Acts of Parliament, 2000 (India).
[11] RESERVE BANK OF INDIA, https://www.rbi.org.in/commonman/Upload/English/Notification/PDFs/MD18KYCF6E92C82E1E1419D87323E3869BC9F13.pdf (last visited Feb. 12, 2026).

Institutional Challenges : The Roadblock to Justice

Even with the existence of these legal and institutional frameworks, enforcement is still plagued by challenges. A glaring issue is that cybercrime units are not available in most police stations of rural and semi-urban areas, the lack of technological infrastructure and the absence of well-trained personnel for sophisticated digital offenses being the reasons. Delayed investigations usually do not prove useful in tracing or recovering fraudulent transactions because such transactions can be easily rerouted or withdrawn within no time. Adding to this is the abysmally low rate of convictions-regularly quoted less than 5%, due to the technical intricacies involved in establishing cyber fraud and the unfamiliarity of the prosecution with digital evidence. These scams are invisible and often go unreported, these are not just a crime against a person but also a threat to society as a whole. Huge reason for underreporting of these crimes among elderly and women is the fear of society, victim-blaming or lack of knowledge regarding how and where to report. Thus, while the current legal system appears in writing to be in order, a systematic reform and grassroot level implementation are required to combat the evolving landscape of online financial crimes.

Conclusion

Online financial fraud is no longer a concern just for computer literate or the sloppy, it has quietly instated itself into every aspect of our society, with greatest impact on those who are already vulnerable. It has reached an all-time low in this scenario where senior citizens are struggling to find their way in digital world they never knew, or women in some traditional families who are told not to get involved in financial decision, families who are too poor to make ends needs or students who are searching for jobs or scholarships, these people become easy target of scammers. Not that they are stupid but the system educated them on inclusion and then left them vulnerable. It's not merely about money stolen. It's about shattered confidence, broken trust, and the enduring fear of reaching for something as ordinary today as a mobile phone or a digital wallet. The harm that these scams cause - particularly when victims are threatened, humiliated, or blamed - is profound and often intangible. And India has laws and institutions available, but often out of reach for the very individuals who need them most. Lack of knowledge, weak enforcement, and illiteracy in the digital age prevent justice from being achieved. To really address this crisis, we require more than stricter laws. We require compassion. We require systems that prioritize victims—providing them with support, guidance, and a path back to reclaim their dignity. We require education to empower every person to use digital tools responsibly, regardless of where they live or how much they earn. And we require accountability, not only from scammers, but also from platforms, policymakers, and society as a whole. Because ultimately, an India that's digitally secure is not merely an India with the most advanced technology, it's an India where even the most vulnerable are safe, respected, and included. And that's not only good policy.