WHO POLICES THE PLATFORMS? REGULATING FINANCIAL FRAUDS THROUGH APP MARKETPLACES IN INDIA

Arya Gupta, Department of Law, Rani Durgavati University, Jabalpur

Aparajita Gupta, Rani Durgavati University, Jabalpur

ABSTRACT

In recent years, India has witnessed a surge in financial frauds perpetrated through mobile applications distributed on major app marketplaces like Google Playstore and Apple Appstore. Despite their central role in approving, ranking, and monetizing these apps, platforms routinely disavow liability for user harms, citing their status as neutral intermediaries under Indian law. This article critically examines the regulatory vacuum that enables such platforms to evade responsibility, highlighting the inadequacies of current Indian statutes and drawing on global models such as the European Union's Digital Services Act. Through case studies and enforcement data, it demonstrates how self-regulation and scattered interventions have failed to protect users from predatory apps. The article argues for a dedicated regulatory authority and a statutory duty of care for app marketplaces, proposing reforms that would impose proactive vetting, real-time oversight and user compensation mechanisms. These measures are essential to safeguard consumer rights and restore trust in India's digital economy.

Keywords: App marketplaces, Fraudulent apps, Mobile applications, User harm, Platform accountability.

Introduction

Since at least 2020, Indian enforcement agencies, including the Enforcement Directorate (ED), have uncovered a sprawling financial scam involving over 300 instant loan mobile applications, many of which were available on the Google Play Store.[1] These apps were often operated by shell companies with foreign, particularly Chinese, funding and targeted low-income and digitally inexperienced users by offering easy access to loans. Once installed, they harvested personal data such as contact lists and social media activity, which was later used for coercion, harassment and reputational harm. Despite mounting complaints and widespread media coverage, many of these apps still remained accessible on app stores.

Between September 2022 and August 2023, Google removed over 2,200 fraudulent loan apps from the Play Store[2]. In the previous year, it had taken down more than 2,500 such apps following a review of nearly 4,000. The sheer volume of removals highlights the scale of the threat and the inability of self-regulation or scattered interventions to contain it. This persistent cycle of abuse and belated enforcement underscores the need for a dedicated regulatory body or framework focused specifically on platform accountability in app marketplaces.

In India's rapidly digitizing economy, app marketplaces like Google Play and Apple App Store serve as the primary gateways for mobile applications, including those offering financial services. These platforms do not merely act as passive intermediaries; they curate content, rank apps, verify developers, and extract commissions from in-app purchases. Yet, when users suffer financial harm from fraudulent third-party apps, platforms routinely disavow liability, citing their intermediary status under Indian law.

This essay examines the regulatory vacuum surrounding platform responsibility for financial frauds perpetrated via hosted apps. It argues that existing legal protections, are insufficient in the face of curated marketplaces that actively shape user experience and profit from app distribution. Furthermore, this essay argues for the creation of a dedicated governmental regulatory authority responsible for verifying, licensing, and auditing mobile applications that

[1] Hemant Kashyap, *ED Summons Senior Google Executives on Probe Into App-Based Micro-Lending Fraud*, Inc42 (Apr. 6, 2022), https://inc42.com/buzz/ed-summons-senior-google-executives-on-probe-into-app-based-micro-lending-fraud/.

[2] Google Removes 2,200 Fraudulent Loan Apps from Play Store: MoS Finance, *Press Trust of India* (Feb. 6, 2024), https://www.ptinews.com/story/business/google-removes-2-200-fraudulent-loan-apps-from-play-store-mos-finance/1270485.

offer financial services or access sensitive user data. It also proposes a legal framework that assigns a duty of care to app marketplaces, including liability in cases where users suffer harm due to failures in the vetting process.

The App Marketplace as a Digital Gatekeeper

Smartphone applications have become the primary interface for Indian users accessing finance, health, education, and government services. App marketplaces like Google Playstore and Apple Appstore dominate this ecosystem[3], acting as powerful gatekeepers that approve, distribute and rank nearly every app on Android and iOS devices. This centralization gives these platforms immense influence over developers and users alike. Most users trust that apps available on these stores have been properly vetted. Platforms reinforce this belief by branding themselves as safe and curated environments.

However, this trust is increasingly misplaced. Despite claims of strict vetting, numerous fraudulent apps, often in high-risk sectors like finance, evade scrutiny and remain on the platform for extended periods. These failures are not isolated. In March 2025, cybersecurity firm Bitdefender exposed 331 malicious apps on the Google Play Store, disguised as QR scanners and health trackers, and wallpaper tools which later evolved into phishing tools[4]. They accumulated over 60 million downloads before being flagged. Similarly, the Tria Stealer malware targeted Indian users via sideloaded APKs, harvesting emails, messages, and OTPs to hijack accounts and solicit fraudulent transfers. While Google stated the malware was not on the Play Store, its emergence reflects the limits of existing safeguards.

Google's own 2024 report revealed it blocked over 2.36 million policy-violating apps and banned 158,000 malicious developer accounts[5]. In 2024 alone, Apple blocked nearly 2 million fraudulent or risky app submissions, underscoring the scale of abuse even on tightly controlled

[3] Cowls, Josh and Morley, Jessica and Floridi, Luciano, App store governance: implications, limitations, and regulatory responses (April 29, 2022). Available at SSRN: https://ssrn.com/abstract=4096933 or http://dx.doi.org/10.2139/ssrn.4096933.

[4] Alecsandru Cătălin Daj et al., *Hundreds of Malicious Google Play-Hosted Apps Bypassed Android 13 Security With Ease*, Bitdefender (Mar. 18, 2025), https://www.bitdefender.com/en-us/blog/labs/malicious-google-play-apps-bypassed-android-security/.

[5] Ravie Lakshmanan, Google Bans 158,000 Malicious Android App Developer Accounts in 2024, Hacker News (Jan. 31, 2025), https://thehackernews.com/2025/01/google-bans-158000-malicious-android.html.

platforms like the App Store[6]. These numbers, while impressive, indicate the scale of the threat. Although features like Play Protect and app verification exist, enforcement remains opaque and inconsistent. Approval criteria are not clearly communicated, and the moderation process lacks transparency.

India currently has no law specifically holding app marketplaces accountable for financial fraud. The Information Technology Act, 2000[7] and the Consumer Protection Act, 2019[8] offer only limited and reactive protections. As a result, platforms operate in a regulatory vacuum, benefitting from legal immunity while shaping the digital economy. Without a proactive framework to govern high-risk apps and impose liability on platforms for lapses in oversight, user safety will remain compromised.

Platform Inaction and the Consequences for Users

The absence of effective regulatory oversight for app marketplaces has resulted in severe consequences for end users. Individuals have lost personal data, suffered financial fraud, and faced psychological trauma from predatory apps that were readily available on trusted platforms. In the loan app scams, users are lured by promises of easy credit, only to be harassed with threats and extortion tactics once they have granted data permissions to the app. The applications involved are downloaded from the Google Play Store and had remained live for extended periods, even after complaints were raised. In most cases, users have no clear channel for redress, and platforms are legally insulated from liability.

This pattern is not limited to India. In *Diep v. Apple Inc.*[9], a United States federal court dismissed a class action suit against Apple filed by users who had downloaded a fake cryptocurrency wallet from the App Store. The app had harvested private keys and drained digital assets. The court held that Apple was protected under Section 230[10] of the Communications Decency Act and by the terms of its user agreement, which limited its liability

[6] Apple Inc., *The App Store Prevented More Than $9 Billion in Fraudulent Transactions Over the Last Five Years*, Apple Newsroom (May 28, 2025), https://www.apple.com/in/newsroom/2025/05/the-app-store-prevented-more-than-9-billion-usd-in-fraudulent-transactions/.
[7] Information Technology Act, No. 21 of 2000, India Code (2000).
[8] Consumer Protection Act, No. 35 of 2019, India Code (2019).
[9] Hadona Diep, et al. v. Apple, Inc., No. 22-16514, 9th Cir. (Mar. 27, 2024).
[10] 47 U.S.C. § 230

for third-party apps. The case demonstrated that existing legal frameworks often favour platforms over users, even when platforms market themselves as secure and trustworthy.

These examples highlight a troubling pattern. App stores allow harmful applications to pass through their review systems, remain online for extended durations, and often act only after third-party researchers or law enforcement agencies raise alarms. This reactive model places the burden of security on users, who are frequently unaware that they are being targeted. In practice, this means that platforms benefit from the trust of consumers without accepting any meaningful responsibility for the harms that result from their failure to screen high-risk apps effectively.

Additionally, the user agreements of platforms such as the Play Store and App Store typically contain limitation of liability clauses. These terms significantly reduce the platform's accountability even when users suffer harm dure to apps that were made available through their services. Courts have frequently upheld such clauses, reinforcing the idea that platforms are not liable for third-party content even when the apps in question have passed through internal review mechanisms, which further prevent users from seeking compensation[11]. These clauses, although contractually valid, are often dense and difficult to comprehend, making it unlikely that users fully grasp the extent to which they are waiving their rights. The result is a system in which platforms can continue to profit from user trust while facing minimal consequences for failing to screen harmful applications.

Legal and Regulatory Framework: Gaps in Indian Law and Global Comparisons

A. Intermediary Liability under the Information Technology Act, 2000

Under Indian law, digital platforms are classified as intermediaries under Section 2(1)(w)[12] of the Information Technology (IT) Act, 2000. Section 79 of the IT Act 2000[13] grants them a conditional "safe harbour" from liability for third-party content, provided they act as neutral conduits and comply with due diligence obligations. The Supreme Court in *Shreya Singhal v.*

[11] Jeffery Neuburger, App Store Protected by CDA Immunity (and Limitation of Liability) for Losses from Fraudulent Crypto Wallet Appellant, *Lexology* (Sept. 16, 2022), https://www.lexology.com/library/detail.aspx?g=3af81835-d52f-46ea-b9c4-732ce766cc38.
[12] Information Technology Act, No. 21 of 2000, § 2(1)(w), India Code (2000).
[13] Information Technology Act, No. 21 of 2000, § 79, India Code (2000).

Union of India[14] held that this immunity is lost when platforms acquire "actual knowledge" of unlawful content and fail to act.

App marketplaces such as Google Play and the App Store frequently invoke this intermediary shield to disclaim responsibility for hosting harmful or fraudulent apps. However, this defense is increasingly untenable. These platforms charge developer fees, curate search results, impose content policies, and extract commissions from in-app transactions. Their extensive control over app distribution and monetization renders them far from passive.

B. Deficiencies in the IT Rules, 2021 and Related Domestic Frameworks

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[15] expand on the due diligence duties under Section 79. They require intermediaries to appoint grievance officers, publish privacy policies, and take down unlawful content within defined timeframes. However, these rules were drafted primarily for social media intermediaries and digital news platforms. They impose no explicit obligation on app stores to pre-screen financial service apps or evaluate developer credibility, leaving wide leeway for bad actors.

The Consumer Protection Act, 2019[16] penalizes unfair trade practices, misleading advertisements, and deficient services. In *Amazon Seller Services Private Limited vs. Vishwajit Tapia*[17], the State Consumer Disputes Redressal Commission held that an e-commerce platform could be liable if it actively participates in transactions. The court noted that marketplaces earn revenue from user engagement and have a duty to verify sellers, rejecting the defense of being mere intermediaries.

Similarly, app stores act as electronic service providers by aggregating users and developers and offering services like developer verification and review filtering. Applying this principle, app stores cannot claim immunity as mere intermediaries and may be liable under COPRA, 1986[18] and 2019 for unfair practices on their platforms. However, courts have yet to clearly

[14] Shreya Singhal, (2015) 5 SCC 1.
[15] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Ministry of Electronics & Information Technology, India, Gazette Notification No. S.O. 1355(E) (Feb. 25, 2021).
[16] The Consumer Protection Act, No. 35 of 2019, Acts of Parliament, 2019 (India).
[17] Amazon Seller Servs. Pvt. Ltd. v. Vishwajit Tapia, First Appeal No. 544 of 2019, State Consumer Disputes Redressal Commission, Punjab. Chandigarh.
[18] The Consumer Protection Act, 1986, No. 68 of 1986, India Code (1986).

apply this to app marketplaces. Users harmed by fraudulent apps also face challenges in pursuing claims, especially when developers are untraceable or overseas.

The Digital Personal Data Protection Act, 2023[19] adds another layer by requiring informed consent for data processing and penalizing misuse. But its scope is primarily limited to data fiduciaries and processors. App stores that merely "enable" data harvesting through hosted apps can escape liability unless directly involved in processing which is a significant loophole, especially when malicious apps exploit platform infrastructure to commit large-scale breaches.

C. Global Models: The EU's DSA and DMA

India's lagging regulatory response stands in contrast to emerging international norms. The European Union's Digital Services Act (DSA)[20] introduces a layered regulatory framework based on the size and impact of online platforms. It requires "very large online platforms" or VLOPs to assess systemic risks, including fraud, consumer harm and data misuse. It also mandates transparency in moderation policies and allows researchers access to platform data (Article 31)[21] which are crucial tools in tackling coordinated financial frauds by malicious apps.

The Digital Markets Act (DMA)[22] complements this approach by targeting gatekeeper platforms, including dominant app stores. It bars anti-competitive conduct, self-preferencing, and exclusive in-app payment systems. While it does not directly address user harm or compensation, the DMA recognizes that app stores exert structural control over market access and must be subject to specific obligations. Importantly, both laws reject the outdated notion of platforms as neutral intermediaries.

These frameworks are not perfect. Scholars have flagged vague definitions, limited jurisdiction over smaller app stores, and insufficient user remedies. However, they mark a significant turn in regulatory philosophy: platforms are no longer invisible infrastructure but central actors in risk governance. India, as one of the world's largest app ecosystems, can no longer afford to

[19] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023.
[20] Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 1.
[21] Digital Services Act, art. 31.
[22] Regulation 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), 2022 O.J. (L 265) 1.

treat app marketplaces as passive. The time is ripe for targeted, enforceable obligations tied to platform power and user vulnerability.

Recommendations and Conclusion

The absence of a preemptive regulatory mechanism allows fraudulent apps to reach users unchecked, resulting in financial loss, identity theft and large-scale privacy violations. The current legal framework in India primarily addresses the processing of personal information once it is shared with a data fiduciary, and focuses on post-incident action such as banning harmful applications after they have already caused harm. This reactive approach fails to provide sufficient consumer protection or prevent recurrence.

To address this gap, India urgently needs a dedicated regulatory framework that acknowledges the gatekeeping role of app marketplaces and tackles the specific risks posed by app-based financial frauds. A meaningful reform agenda should begin with the establishment of a specialized regulatory authority, or by conferring such powers on an existing body like the Indian Computer Emergency Response Team. This body should be responsible for licensing and conducting periodic audits of financial applications and must collaborate closely with app marketplaces by adopting real-time data-sharing protocols to identify and eliminate fraudulent operators early.

In parallel, legislative reform is required to impose a statutory duty of care on app marketplaces, especially for apps that handle sensitive user information such as financial or biometric data. India can draw from global models such as the European Union's Digital Services Act, which introduces a tiered system of obligations based on platform size and societal impact. Moreover, provisions should be introduced to enable compensation for users harmed by such apps, particularly in cases where platform negligence in moderation or vetting is evident.

Regulating app marketplaces is not a roadblock to innovation. On the contrary, it is essential for safeguarding consumer rights, ensuring platform accountability and fostering public confidence in India's digital ecosystem.