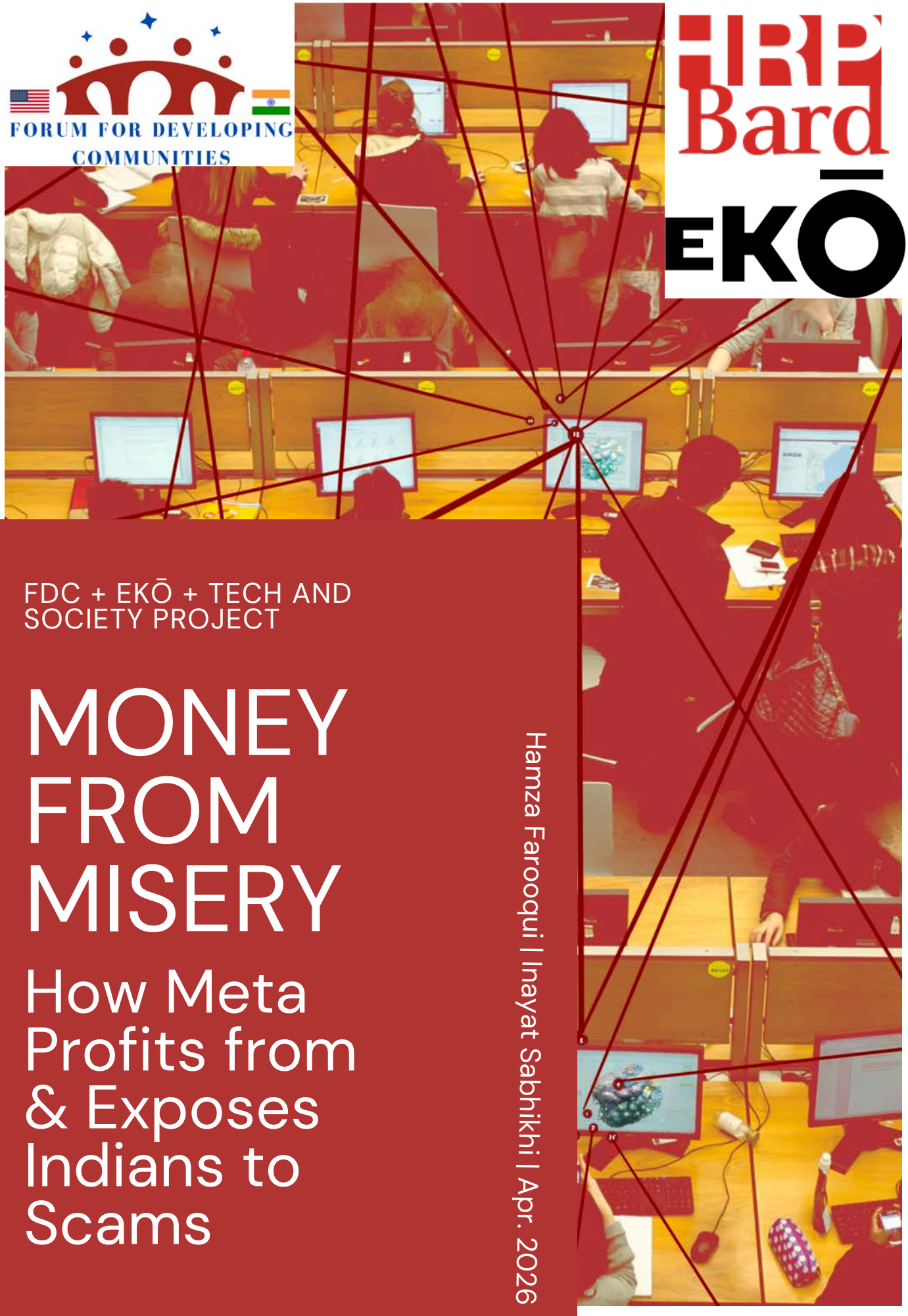
FORUM FOR DEVELOPING COMMUNITIES

IRP Bard

EKŌ



FDC + EKŌ + TECH AND SOCIETY PROJECT

MONEY FROM MISERY

How Meta Profits from & Exposes Indians to Scams

Hamza Farooqui | Inayat Sabhikhi | Apr. 2026

Report Authors

Hamza Farooqui, independent researcher

Inayat Sabhikhi, associate director, Human Rights Project, Bard College

Ekō is 23,528,130 people stopping big corporations from behaving badly.
https://www.eko.org/

Bard Human Rights Project
Examining human rights through teaching, research, and public programs.
https://hrp.bard.edu/

Forum for Developing Communities
Bridging India and the Diaspora.
https://forumdc.org

Table of Contents

Executive Summary

Online scams are everywhere in India—spanning news reports, policy discussions, and private conversations with victimized friends and family. This is compounded by the ceaseless bombardment of scam calls, e-mails, and advertisements targeting Indians daily. This report sheds light on a critical but underreported reason for the steep rise in scams: social media platforms that host fraudulent advertisements and profit from them.

Through paid advertising systems, platforms like Facebook and YouTube earn substantial revenue by serving scam ads to potential victims. Internal Meta documents reviewed by Reuters reveal a staggering scale of complicity: Meta projected that approximately 10% of its total 2024 revenue, roughly $16 billion, would come from fraudulent ads and banned goods, while showing users an estimated 15 billion "higher risk" scam advertisements daily (Horwitz 2025a). Even Meta's "trusted" advertising agencies openly sold services to bypass platform checks (Horwitz 2025b), and reports detail an internal playbook that sought to prevent policymakers from addressing this crisis (Horwitz 2025c).

Indian regulatory authorities have attempted to address these trends. This report tests a significant measure by the Securities and Exchange Board of India (SEBI), the apex body regulating India's securities markets, akin to the U.S. SEC. SEBI issued an advisory in 2025 requiring platforms to ensure that all advertisers required to be registered with SEBI must verify their registration with platforms (SEBI 2025a). Our research found that more than six months after the registration deadline, a whopping 97% of financial advertisers on Meta are unregistered entities. This report shows how easy it is to advertise without registration.

Immense Toll of Scams

The financial toll of scams is immense. According to the Global Anti-Scam Alliance, an estimated $1.03 trillion was lost globally to scams in a year between 2023–24 (GASA 2025). Three-fourths of Indian adults reported encountering a scam in the past 12 months, with more than one-quarter experiencing financial loss (GASA 2025). The crisis has intensified in India: losses tripled in 2024 compared to the previous year, reaching

Rs. 22,845 crore (~2.5 billion USD) according to the Ministry of Home Affairs (PTI 2025). Beyond financial losses, scams inflict significant emotional, mental, and societal harm. Nearly 60% of victims in India reported that it affected their wellbeing—reduced confidence, increased distrust of digital tools, or family tensions—and over two-thirds suffer impacts to their mental well-being (GASA 2025). Impacts are exacerbated by prevalent victim-blaming, which leads individuals to feel personally responsible for having been deceived. This emotional burden disproportionately affects victims in developing nations.

Social Media Platforms Accelerate the Crisis

Social media platforms have emerged as potent accelerants of this crisis. In the U.S., one in four people who reported specific contact by fraudsters said it started on social media, with reported losses reaching $2.7 billion—far higher than with any other method of contact (Fletcher 2023). Among Indians, Meta platforms dominated as sources of scams, with 80 percent encountering scams on WhatsApp and half reporting Instagram as the source (GASA 2025).

Targeting mechanisms that make social media ads effective also make scams precise. Algorithms identify when users are more likely to engage with specific content based on their circumstances, such as targeting financially distressed individuals with fraudulent loan offers. This compounds the tragedy: those desperately seeking financial solutions, job opportunities, or investment advice are precisely the "high-value targets" algorithms identify for scam ads.

Platforms have the Power to Prevent Scam Ads...

While comprehensive solutions require user education, as well as action from law enforcement and financial institutions, social media platforms are uniquely positioned to prevent scams at their source. Unlike random instances of fraud that occur in hard-to-detect peer-to-peer interactions, purchasing a scam ad targets many victims in one fell swoop. Moreover, it involves a transaction with the platform itself. This creates a clear point of intervention: platforms have the technical capability and financial records to verify identities, validate business credentials, and detect fraudulent patterns before scams reach potential victims. If platforms rigorously verified advertisers, scammers would find it exponentially harder to reach victims at scale.

...but Fail to Do the Bare Minimum Required

Accordingly, Indian regulator SEBI consulted with social media platforms and mandated “advertiser verification of SEBI Registered Intermediaries” before they are permitted to “upload / publish advertisements on these platforms” (SEBI 2025a). This was a bare minimum expectation. In response, Meta modified its ad-buying process but introduced a loophole: the verification process is only triggered when advertisers “self-declare” as financial advertisers. As our research shows, 97% of financial advertisers avoided all verification steps by simply failing to make the declaration.

This failure compounds prior failures. Our research also shows that despite a media outcry over specific scams in news reports, Meta failed to take action against them. We found over 400 scam ads still active on Meta platforms months if not years after they had been reported in the media.

More Research Is Required

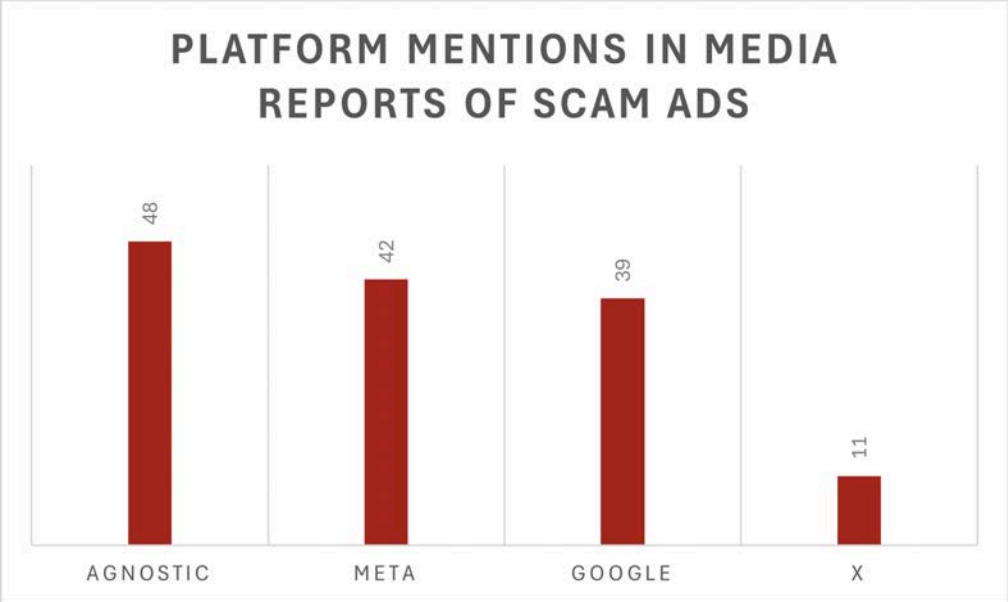
While this report focuses primarily on Meta's advertising ecosystem, all social media platforms are vulnerable to exploitation by scammers, and the dynamics we document are not unique to any single platform. A more systematic study of scam advertising across all major platforms—including YouTube, TikTok, X (formerly Twitter), and others—remains urgently needed to understand the full scope of platform-enabled fraud.

Context

Prevalence of Social Media Ad Scams

To better understand the prevalence of scams and their effects, we started by systematically cataloguing publicly reported digital-scam media reports between January 2024 and May 2025, using keyword-based searches across major platforms. This process yielded a database of 149 distinct scam stories, which served as the foundation for identifying common patterns and nuisances.

Ad scams emerged as the dominant topic in media coverage, accounting for 67 of the 149 stories (45%). This significant proportion suggests that advertising-based scams represent either a particularly prevalent threat, substantial media attention, or both. The platform distribution revealed that Meta-related scams (including Facebook, Instagram, and WhatsApp) featured in 42 stories (28%), while Google-related scams appeared in 39 stories (26%). Twitter/X was mentioned in 11 stories (7%), and 48 stories (32%) were platform-agnostic, discussing scams that either operated across multiple platforms or were not tied to a specific digital platform.



Following our preliminary research, we chose to focus on advertisement scams and Meta for two substantive and one methodological reason: first, ad scams made up almost half of all the media reporting on scams. Second, since ads require a transaction with the platforms, it is possible for the platforms to create verification mechanisms to control scams. Methodologically, Meta's Ad Library has an Application Programming Interface (API) which allows users to query and retrieve data on all active and inactive ads, enabling systematic, large-scale analysis that is not possible on most other platforms.

This last limitation is an indictment of other major platforms that do not provide the level of transparency around avertising that Meta provides.

Meta and Ad Scams

Reuters Expose Reveals Meta's Playbook

Internal company documents reviewed by Reuters reveal that Meta is aware of the scale of ad scams running on its platforms. Despite this, Meta's enforcement approach reveals a troubling tolerance threshold: the company bans advertisers only when its automated systems predict that they are at least 95% certain to commit fraud (Horwitz 2025a). For advertisers that fall below this certainty threshold but are still suspected of fraudulent activity, Meta implements "penalty bids"—charging higher advertising rates as a deterrent rather than removing them entirely. This creates a perverse incentive structure where Meta continues to profit from likely scammers.

The documents further show that Meta's platforms were involved in approximately one-third of all successful scams in the United States as of May 2025. Perhaps most tellingly, Meta's own internal review concluded in April 2025 that "it is easier to advertise scams on Meta platforms than Google", acknowledging that some of its main competitors were doing a better job at weeding out fraud (Horwitz 2025a).

Meta's 2024 Scam Revenues

$16 bn

The company's strategic documents illuminate a calculated balancing act between enforcement and revenue. Internal projections show that while the company anticipates regulatory fines of up to $1 billion for scam advertising, this figure remains significantly smaller than the revenue generated from such ads. A November 2024 document notes that every six months, Meta earns $3.5 billion from scam ads that "present higher legal

risk—a figure that "almost certainly exceeds the cost of any regulatory settlement involving scam ads" (Horwitz 2025a).

This creates a strong financial disincentive for Meta to act against fraudulent advertisements. In early 2025, Meta stopped the team vetting suspicious advertisers from acting as it was projected to cost the company more than $130 million. Additionally, the documents revealed that Meta failed to take action against user-reported suspect advertisements as well. According to their estimates, users filed approximately 100,000 valid reports of fraudsters messaging them each week. However, Meta ignored or incorrectly rejected 96% of such reports (Horwitz 2025a).

Even in cases where there is evidence of financial fraud, the process for removing such advertisements and pages is far from straightforward. According to Reuters reports, depending on the money spent by the advertiser, it would take from eight to 500 strikes before Meta takes action (Horwitz 2025a).

Taken together, all of these facts indicate a pattern of Meta seeing a trade-off between controlling scams on its platform and advertising revenue. Much like polluting industries treat their impact on ecology as an “externality” that should not be relevant to profit calculations, Meta has accepted the “polluting” of our online environment with scams in lieu of higher revenues.

Meta’s Fear of Advertiser Verificiation

Meta’s internal assessment shows that verification of advertisers would reduce fraudulent activities– 70% of the scams, illicit services, and “low quality” products came from unverified and newly active advertisers (Horwitz 2025c). However, given the cost and effort involved in verification, plus the potential loss of revenue from such unverified accounts, Meta described globally required verification as a “black swan”: a low probability event that would be catastrophic to the corporation. Instead, Meta developed a “playbook”’ to placate regulators and delay or offset significant regulations (Horwitz 2025c).

This playbook, first developed and deployed in response to potential verification requirements from Japanese regulators, hinged on “prevalence perception” management through sanitizing the Ad Library (Horwitz 2025c). They repeatedly identified the top keywords that regulators could potentially use to find fraudulent ads and deleted ads that appeared suspicious (Horowitz 2025a). Scrubbing the Ad Library did reduce the kind of scam ads that regulation would target; however, it also made the situation appear cleaner than it was, with Meta’s team suggesting such efforts should make problematic ads “not findable” for “regulators,

investigators and journalists" (Horowitz 2025c). These efforts had the desired effect: Japanese regulators were convinced of Meta's efforts and put off verification requirements. However, it is important to note that these efforts were a cosmetic fix rather than a systematic one.

A second prong of this playbook involved more perception management efforts by Meta. In Hong Kong, to fend off regulation, requiring verification, the company worked with regulators to draft a voluntary "anti-scam charter" that Google also co-signed (Horwitz 2025c). The initiative was appreciated by officials in Hong Kong, and regulations that would have required verification of financial advertisers were shelved (Horwitz 2025c).

These strategies proved so effective that Meta incorporated them into what internal documents describe as a "general global playbook" for managing regulatory scrutiny across multiple jurisdictions, including the United States, Europe, Australia, Brazil, Thailand, and India (Horwitz 2025c). The playbook outlines Meta's strategy to delay regulators and postpone advertiser verification requirements unless new legislation leaves no alternative. As we show below, in India as well, Meta employed a sophisticated strategy of perception management to fend off verification requirements.

How Meta Played Indian Regulators

SEBI's New Regulatory Requirement

Given the high potential for consumer harm from fraudulent investment schemes and misleading financial promotions, advertisements related to securities and financial services occupy a particularly sensitive regulatory space. The Securities and Exchange Board of India (SEBI) serves as the primary authority overseeing securities markets and financial intermediaries. SEBI is responsible for regulating market participants, protecting investors, and maintaining the integrity of India's financial markets. As a result, SEBI's interventions targeting financial advertisements on social media platforms represent the most concrete attempts by an Indian regulator to address platform-enabled scam advertising.

On 21st March 2025, SEBI issued an advisory, taking note of different kinds of fraudulent advertisements, including "online trading courses, seminars, giving misleading or deceptive testimonials, promise or guarantee of assured or risk-

free return" (SEBI 2025a). The advisory requires financial intermediaries to verify their SEBI registration with social media platforms before publishing advertisements on them. This is achieved by requiring financial intermediaries to register on the social media advertising platform through their SEBI-registered email ID and mobile number for verification. It is only after the platforms have verified the registration details against the SEBI database that the intermediaries will be permitted to upload advertisements. The advisory required intermediaries to complete the process by 30th April 2025.

This order was, crucially, released in consultation with social media platforms, particularly Google and Meta. On 27 June 2025, a month after the registration with social media platforms was due to be completed, Meta released a blog post announcing an update to its requirements for advertisers targeting Indian users with securities, investment, or financial ads (Barua 2025). The blog detailed the steps intermediaries were required to take to register with them before publishing advertisements. Meta informed advertisers that they will have to verify both the person or organization advertising, as well as the payer by providing SEBI registration information. In case an advertiser is exempt from SEBI registration (as in the case of international advertisers), they will have to register alternatively through identity or business verification. Meta also gave a timeline for the registration process: the verification options were to be rolled out from 26th June onwards, with the system expected to be available to 100% of eligible advertisers by 28 July 2025. Intermediaries and advertisers were advised to complete verification as soon as possible, as compliance enforcement would begin as early as 28 July 2025, with the exact deadline varying depending on when each advertiser became eligible.

Toward the end of 2025, there was another flurry of activity as SEBI sought to tackle unmitigated fraudulent activities on social media platforms, summarized in the table below. Following a global call (IOSCO 2025) to action by the International Organization of Securities Commissions (IOSCO)—a global forum that works with world's security regulators to develop and promote internationally consistent standards and practices—SEBI announced in early November its increased efforts to combat investment scams on social media (SEBI 2025b). It "formally communicated" with social media platforms, urging them to expedite the implementation of verification processes to ensure only SEBI-registered entities can advertise regulated products and services. There has been no further update regarding the concrete steps taken by SEBI under these increased efforts or the platforms' responses to SEBI's communication.

Table 1

Steps Taken by Indian Regulators

Title	Type	Date	Main Purpose
Advisory to SEBI Registered Intermediaries (SEBI 2025a)	Advisory	21 Mar 2025	• SEBI Registered Intermediaries are required to register on Social Media Platform Providers (SMPP). • Advertisers are only allowed to publish ads after SMPPs conduct advertiser verification.
SEBI Press Release Calling for Greater Collaboration from Platforms (SEBI 2025b)	Press Release	06 Nov 2025	• Urged SMPPs to prioritize and fast-track mandatory advertiser verifications.
Ministry of Finance Notification (Singh 2025)	Notification	8 Dec 2025	• SEBI was empowered to direct Social Media platforms to remove illegal or fraudulent posts related to regulated products.
SEBI Circular on Ease of Doing Investment—Disclosure of Registered Name and Registration Number by SEBI Regulated Entities (Mahala 2026)	Circular	26 Feb 2026	• Comes into effect May 1, 2026 • Requires disclosure of registration details on entities' social media handles and on every piece of content. • Expands the category of "advertisement" to include non-explicit promotion.

However, a more concrete step was taken on 8th December: the Ministry of Finance authorised SEBI to direct social media platforms to remove illegal or fraudulent posts related to regulated products and services (Singh 2025). Moreover, in a circular released on February 26, 2026, SEBI mandated additional measures to increase transparency and accountability for regulated entities on social media (Mahala 2026). The circular requires all regulated personnel and entities to disclose their registered name and SEBI registration number prominently; specifically, on the page of their social media platform handles and on each post they upload. Additionally, the circular requires this disclaimer on all social media content that relates to securities in any form (Mahala 2026). The circular will come into force on May 1, 2026.

Evaluation of SEBI Framework

The measures outlined above reflect a broader recognition that the existing regulatory architecture was not equipped for the scale and speed at which financial fraud operates on social media. Digital advertising tools have dramatically lowered the cost and effort required to reach large, precisely targeted audiences, capabilities that legitimate financial intermediaries and fraudulent actors alike can exploit with equal ease. Platform-level verification, in this context, becomes one of the few mechanisms capable of intervening at the point where fraudulent content is amplified. Whether SEBI's framework is adequate to that challenge is a question that demands closer examination.

The February 26 circular (Mahala 2026) goes the farthest in mandating that all the entities SEBI directly controls, i.e., those that are registered with it, must announce their formal status in every piece of content, whether “organic” content such as educational posts, or advertisements. It even covers pieces of content shared in “closed groups.” However, the framework still contains several limitations.

- First, SEBI is trying to address scam actors by getting legitimate actors to declare their registration with SEBI. This does nothing to restrict bad actors from targeting consumers, especially those vulnerable to manipulation or lacking in sufficient awareness.

- Second, SEBI has not instituted any penalties for failing to follow this policy, nor has it notified any structure to monitor content or ads libraries. It even imposes requirements on content in areas that it cannot oversee, like in private groups.

- Third, in terms of advertisements, it allows entities exempted from SEBI registration, like foreign entities, to only upload a personal ID or business document to be exempt from registration requirements. The policy does not provide standards for how platforms must evaluate these documents (Bansal 2025).

- Fourth, the advertising policy does not address indirect advertising, such as when financial services are promoted through affiliate links, influencer-brand collaborations, or informal partnerships that do not use platform ad tools directly (Bansal 2025).

- Fifth, there is lack of an enforcement and monitoring framework to ensure social media platforms comply with SEBI's advisory.

In particular, methodologies like this report's are easy to replicate to identify potential scam ads and proactively push platforms to take them down.

Finally, Meta's participation in shaping SEBI guidelines aligns with their playbook to offset verification requirements. The company's internal assessment of neutering Hong Kong's regulations that "the finalised language does not introduce new commitments or require additional product development" (Horwitz 2025c)—applies equally to the outcome in India.

Methodology

This report employed a two-tiered mixed-methods approach to assess Meta's handling of ad-based scams and its compliance with regulatory interventions in India. The methodology combined qualitative media analysis, platform investigation, and quantitative data collection to examine both the prevalence of fraudulent ads and the effectiveness of Meta's enforcement mechanisms.

First, following our background research looking at media coverage of scams, we then investigated whether Meta had taken steps to mitigate these publicized scams by searching for similar advertisements in Meta's publicly accessible Ad Library using keywords extracted from media reports.

Second, we assessed Meta's compliance with the Securities and Exchange Board of India (SEBI) advisory requiring registration for advertisers of finance-related content. This involved two measures: creating test advertisements through a dummy Facebook page to identify loopholes in Meta's enforcement mechanisms.

Third, we conducted large-scale data scraping using Meta's Ad Library API twice: once in September 2025 and again in February 2026. This helped us measure how many financial advertisers had actually registered their SEBI credentials with the platform.

Fourth, we created a basic taxonomy of risk to categorize the ads we scraped into High Risk, Moderate Risk, and Low Risk ads. This involved classifying ads based on six factors: the presence of urgency language in the ad copy; explicit guarantees of returns or risk-free investment outcomes; a low number of page likes; a short average active duration for ads run by the page; the absence of the advertiser's business details in SEBI's intermediary registry; and the presence of an external link in the ad.

Detailed methodology is available in the Annexure.

Findings

Lack of Accountability and Action

A notable finding relates to platform responsiveness to media coverage on scams. Of the 149 stories, 73 were of a nature where platform comment was neither expected nor necessary (such as policy discussions, general trend pieces, or government advisories). However, among the remaining 76 stories where platform response would have been relevant to the reporting, 50 stories (66%) contained no comments from the implicated platforms. This trend suggests a lack of attention on the platform's behalf to media reports and scams.

This lack of attention is all the more troubling when it translates to a lack of action. We followed up on several of the scams reported in our database and found that they were continuing unhindered. Despite widespread media coverage, including in some instances an in-depth explanation of markers that show that the ads were fraudulent, Meta had failed to remove these scams.
We identified five widely reported advertisement scams linked to Meta.

Two of the scams represented here primarily operate through Telegram, the instant messaging platform. However, Meta hosts multiple advertisements promoting these Telegram-based groups or communities linked to fraudulent activities. The other three scams were widely reported across multiple media organizations. In the Aurangabad Bank and Fake Platform Account Verification cases, media reports included statements from police authorities, indicating that law enforcement was aware of and actively working to address these scams. Despite this, nearly a year after these cases were first reported, our findings showed that these scams continue to operate without hindrance.

Table 2 below provides an overview of the findings from the data scraping conducted on the July 15, 2025 that found 413 advertisements still up. We also performed a qualitative check six months later and found ads still functioning in January 2026.

See also the case study on the Al-Khair Baitul Mall Loan Scam below.

Table 2

Platform Inaction on Media Reports of Scams

Media Report	Date of Reporting	Active and Inactive Ads Found in July 2025	Ads still up in Jan 2026?
Hackers Use Fake FAcebook Ads to Distribute Malware of AI Tools: **Fake Software Ads** (Nath 2024)	12 Apr 2024	Total: Active + Inactive: 452 Active: 43	Yes, still active
How Meta Ads Enable Loan Scams that Misuse Aurangabad Bank's Name: **Loan Scam Ads** (Hasan 2024)	11 Jun 2024	Total: Active + Inactive: 107 Active: 38	Yes, still active
Is Telegram Staring at a Ban in India?: **Solicitation Ads, Including Child Sexual Abuse Material** (Shivangini 2024)	27 Aug 2024	Total: Active + Inactive: 107 Active: 38	Yes, still active
Is Telegram Staring at a Ban in India?: **Investment Ads** (Shivangini 2024)	27 Aug 2024	Total: Active + Inactive: 833 Active: 228	Yes, still active
Verified or Duped?: **Platform Account Verification Scam Ads** (Vatyam 2024)	02 Dec 2024	Total: Active + Inactive: 103 Active: 19	Yes, still active

Examples of Active Solicitation Ads

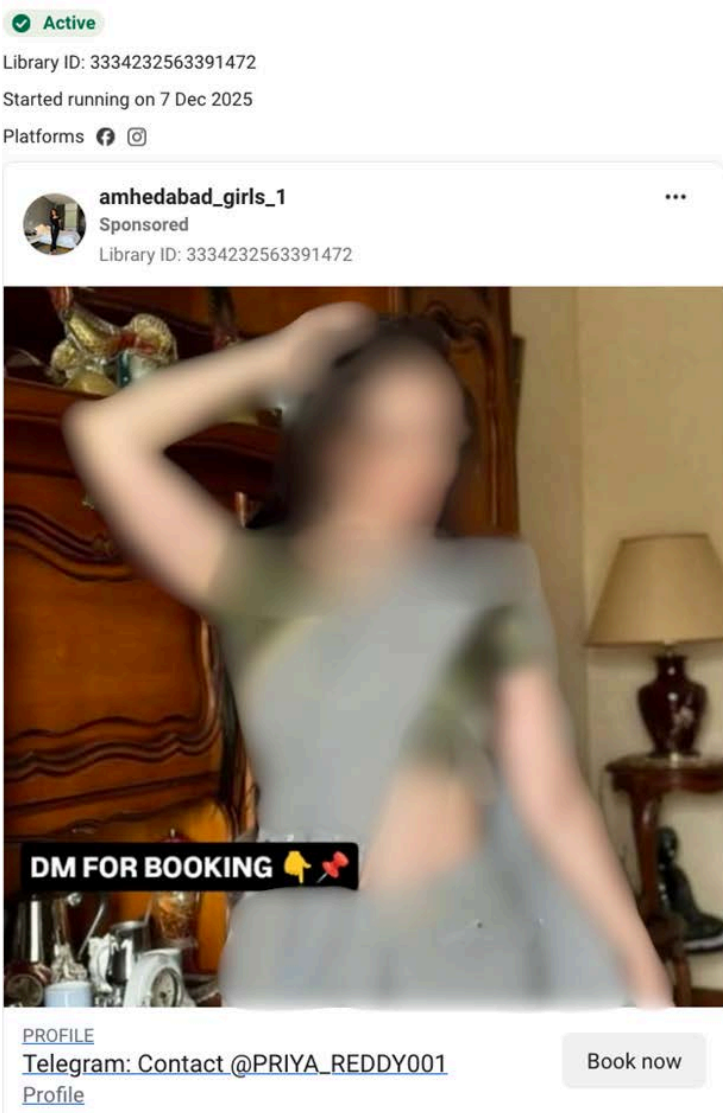


Fig. 1: These solicitation ads have been seen in the past to lead to "sextortion" scams where the person clicking on these ads is subjected to blackmail

Fig. 2: Note the targeting based on cities

Case Study: Al-Khair Loan Scam

In June 2024, BoomLive Decode reported on a loan scam that had been operating for at least six months, misusing the name of Al-Khair Baitul Maal, a legitimate urban co-operative society in Aurangabad, Maharashtra (Hasan 2024).

The scam operated through numerous fake Facebook and Instagram pages that ran advertisements promising interest-free loans using an eight-year-old Zee News report about the legitimate bank. These fraudulent ads received millions of views, reactions, shares and comments across dozens of fake pages and accounts.

The deception was fundamental: Al-Khair Baitul Maal provides interest-free loans only to residents of Aurangabad, offering loans up to 50,000 rupees on the condition of mortgaging gold, with all services provided in person at the bank office, and no online services. Yet, all the scam advertisements claimed to offer online loans with no geographic restrictions.

The scale of victimization was substantial. Bank officials estimated that around 2 crore rupees had been swindled through the scam, with the bank receiving nearly 150 calls daily either enquiring about the loan or reporting the fraud. Individual victims lost significant sums—one victim reported losing 40,000 rupees after being asked to pay successive "processing fees," while another lost over 2 lakh rupees.

What makes this case particularly relevant to our analysis of platform accountability is the documented failure of Meta to act despite clear violations of its own advertising policies and repeated complaints. Bank authorities stated they had filed a complaint with Facebook when the scam started and had been continuously reporting the ads and pages, yet no action was taken. This occurred despite Meta's advertising policy explicitly prohibiting ads promoting schemes using deceptive practices meant to scam people out of money. When Decode reached out to Meta for comment on the story, no response was provided.

When we followed up on this case on 15th July 2025, we found 107 similar ads with 38 active ads that, on qualitative assessment, had all the markers of the scam that Decode had identified (see figs. 3 and 4). This suggests that the scam identified in June 2024 remains active despite the detailed media exposure and documented complaints to both the platform and law enforcement authorities.

Screenshots of Al Khair Scam Ads

Fig. 3: Note the language of "guaranteed returns"

Fig. 4: Note how a different page is advertising a similar offer

These cases illustrate Meta's lack of accountability and action. These are ongoing scams that have been widely reported, including key identifiers. Using only the publicly available Ad Library, we were able to identify large volumes of illegal and fraudulent advertisements. This raises serious questions about Meta's enforcement efforts: if we could identify these scams using publicly available data alone, Meta has no credible justification for its failure to act given its extensive technological capabilities, internal data access, and direct engagement with government authorities.

Moreover, in the five examples that we explored, the most significant ones seem to be financial services or investment-related scams, such as the Al-Khair Baitul Maal Loan Scam detailed above. Notably, such scams fall under the purview of the new regulations introduced by SEBI. The Loan Scam is a particularly illustrative example where advertiser verification could have mitigated the scam. The lack of verification is demonstrative of the shoddy and half-hearted implementation of SEBI's advisory by Meta. In the next section, we take a deeper look at Meta's compliance with SEBI's regulations.

Meta Fails to Comply with SEBI Advisory

Our detailed study of Meta's advertiser verification systems presented stark findings: the verification mechanism is effectively voluntary and trivially easy to circumvent. Advertisers can run financial ads without declaring them as such, with no automated detection or enforcement by Meta's systems. This glut of unverified advertisers is reflected in the data scraping results: more than six months after the enforcement deadline, 97% of financial advertisers on Meta had either not had SEBI registration, or had failed to verify it. Furthermore, more than one-third of the ads were high-risk according to our categorisation.

In this section, we start with the findings of the dummy ad test, followed by the scraping results, and finally the risk-categorisation of the ads.

Meta's Flawed Verification System

Our testing of Meta's advertiser verification system revealed a fundamental flaw in the company's implementation of SEBI's advisory: the verification process is so easy to bypass that it might as well not exist. The lack of automated detection or enforcement by Meta's systems further creates this laissez-faire situation. Even when advertisers do declare their ads as finance-related, selecting the "Not registered with SEBI" exemption pathway requires only minimal verification—a single photograph of any government-issued ID for individuals, with no phone number verification or authenticity checks. There is no clear incentive pushing advertisers to register with SEBI.

Paradoxically, the most robust verification protocols apply only to SEBI-registered entities, creating a perverse incentive structure in which malicious actors can simply claim an exemption from SEBI registration rather than undergo meaningful scrutiny. This design effectively renders Meta's compliance mechanism meaningless, as bad-faith actors have no incentive to go through the verification process. There are, in effect, no checks in place to prevent scam and fraudulent advertisers from posting advertisements.

1. Posting a Financial Ad without Declaring It

When we created a financial ad using keywords from the scam ads we identified above, the Ad Centre displayed a prompt asking, "Is this ad about securities and investments with audiences in India?" along with a note stating that financial advertisements must be declared for audiences in India. A checkbox was provided to indicate the ad as a financial advertisement (see fig. 5). However, there was no mechanism to verify this declaration. We simply did not check the box, even though the ad featured the words "financial services" and "investment advice." The ad was allowed to run and accumulated 24,541 users and generated 11 leads. The 11 leads were despite the ad clearly stating it was "NOT REAL" and for research purposes (see figs. 6 and 7).

This is the most crucial gap in the mechanism. There is no incentive for malicious actors to go through the process and no checks or monitoring to ensure that they do. The advertisement, despite clearly being a security and investments advertisement, was allowed to go live without any corrections from Meta. This, along with Meta's inability to filter for non-declared paid advertisements, such as reels or posts, significantly dilutes Meta's compliance with SEBI directives.

“Self-Declaration” Loophole in Advertiser Verification

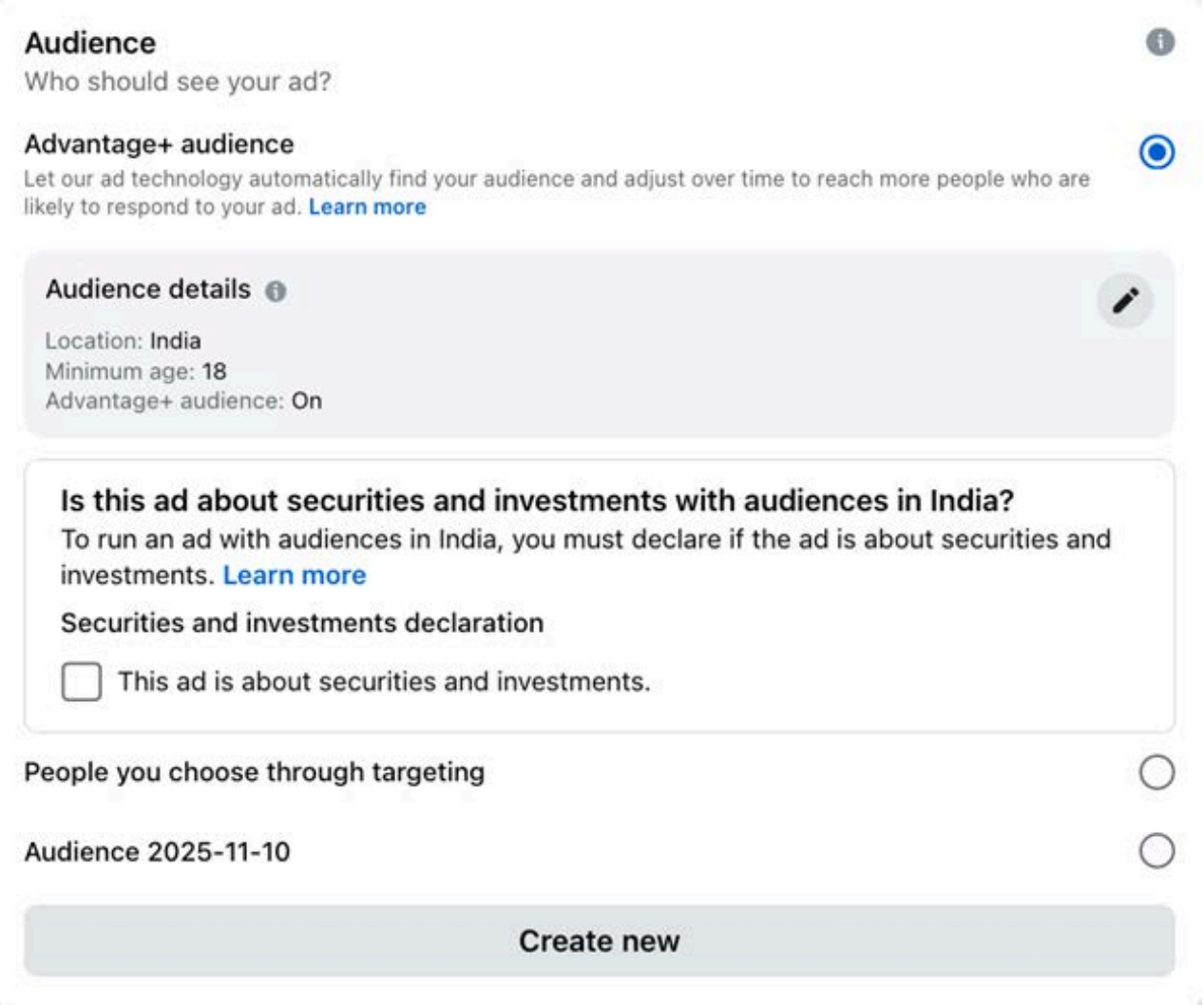


Fig. 5: Simply refusing to select “This ad is about securities and investments” bypasses verification procedures

Our Test Ad Sails Through Verification and Reaches 24k+ Users

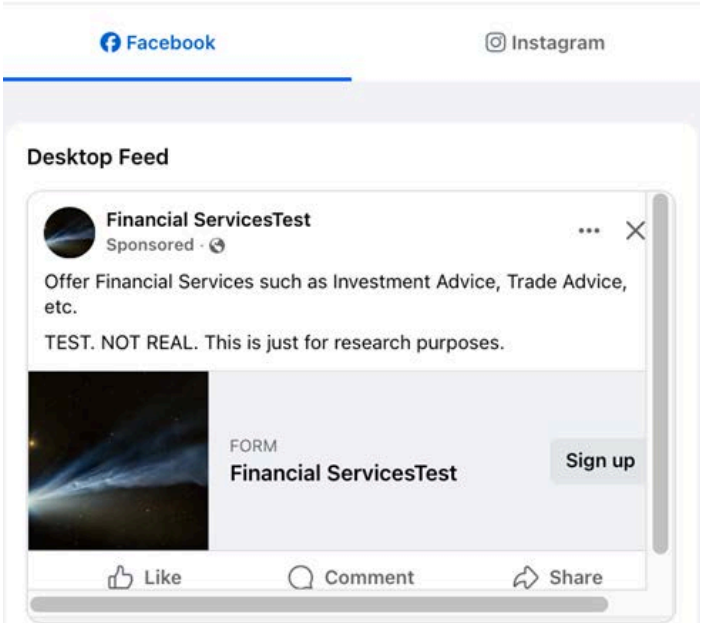


Fig. 6: Even though we did not declare as a financial ad, our ad was accepted by Meta without any checks

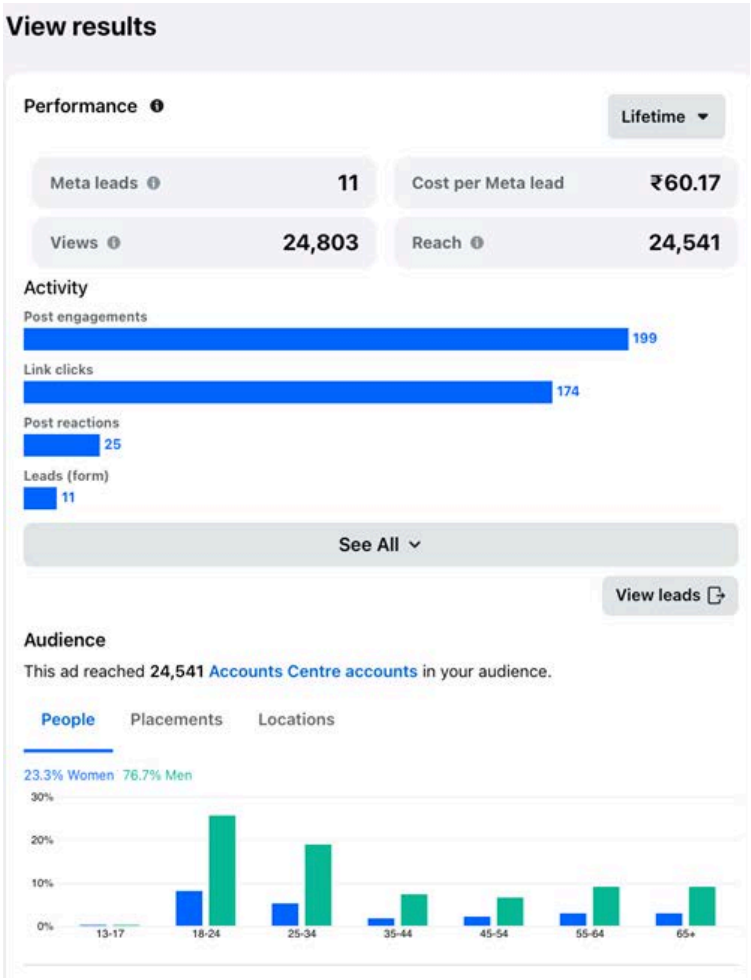


Fig. 7: Our ad clearly stated it was just a test. In a short period for a spend of a few hundred rupees, it reached 24,541 users.

2. Investment Ad Exempted from SEBI Registration

If we ticked the checkbox, we were directed to an "Authorisation and Verification" page. The pop-up box prompted us to clarify whether the advertiser is registered with SEBI. On clicking "Not registered with SEBI," the advertiser was directed to either verify as an organization or as an individual. This appears to be the mechanism described in the aforementioned Meta blog for the "Exempted from SEBI Registration" option. The details of the verification mechanisms are available in the Annexure.

Even if the advertiser self-declares an ad as a financial ad, they only need to opt for the "Not Registered with SEBI" option. There are no additional checks to ensure whether the advertiser is actually exempted from SEBI registration.

In short, non-SEBI-registered intermediaries can still create financial advertisements. Moreover, this option lacks the required checks to authenticate the identity of the person or organization. It requires a photo of a government ID to authenticate a person; there is no OTP verification for phone numbers. Unfortunately, such documents are easily obtainable; Aadhaar card copies are available through a simple Google search. This makes the SEBI-exempted option to run financial ads exceedingly simple.

In order to verify organisations, there are a few more documents required, along with phone number verification. In the absence of SEBI registration, these checks are very easy to bypass. As a result, an entire universe of advertisers who have no reason or incentive to register with SEBI can continue advertising with, to a large extent, anonymity, which then makes holding fraudsters accountable difficult.

3. Posting a Financial Ad as a SEBI-registered entity

There are more robust verification protocols for entities registered with SEBI. We tried to stress-test this mechanism in several ways. The SEBI Intermediary Portal makes the database of registered intermediaries, along with their key details, publicly accessible.

When we attempted to register an organisation that is not listed with SEBI, the process could not proceed. Next, we intentionally entered mismatched details (registration number, phone number, and email ID). The Meta registration interface detected all incorrect combinations—even when the details belonged to different SEBI-registered intermediaries, or when only one field was incorrect while the others were valid.

Finally, when we entered the correct details of a SEBI-registered intermediary (as listed on the SEBI portal), the system required verification of the individual's

association with that intermediary through one of the SEBI-registered contact channels—email, phone call, text message, or WhatsApp.

The safeguards against spoofing a SEBI registration are much more robust. Paradoxically, this only increases the incentive to not report registration, particularly since not reporting registration does not hinder the ability to engage in financial advertising.

How Many Advertisers are Registered with SEBI?

To quantitatively assess Meta's compliance with SEBI's guidelines, we conducted systematic data collection using Meta's Ad Library API twice, across a five-month interval–on September 25, 2025 and February 18, 2026.

The first scraping pulled a total of 3475 ads associated with 1515 pages. Of these, only 41 or 2.7% were registered with SEBI nearly two months after the compliance deadline on July 28. In other words, 97.3% of the financial advertisers on Meta were unregistered entities. The follow-up scraping had starkly similar results. We pulled 3813 ads associated with 1388 pages, and only 35 pages or 2.5%, were registered with SEBI. In other words, despite SEBI's reminder, there was no discernible difference in financial advertisers registering with SEBI or confirming their registration details.

This highlights the crucial gap in the compliance mechanism we identified above: the linking of SEBI-registered details to Meta is entirely voluntary. By simply not declaring the ad as a financial ad, even if the content clearly distinguishes it as such, anyone can circumvent the SEBI directive.

Financial Ads Registered with SEBI

~2.7%

Estimating Risk of an Ad Being a Scam Ad

To further estimate the risk associated with the advertisements we collected, we developed a simple risk assessment framework. We identified six factors that, individually or in combination, may prima facie indicate fraudulent intent. These included the presence of urgency language in the ad copy, such as phrases implying time-limited offers; explicit guarantees of returns or risk-free investment outcomes; a low number of page likes, which may indicate a recently

created or low-credibility page; a short average active duration for ads run by the page, which may suggest the page cycles through ads quickly to evade detection; the absence of the advertiser's business details in SEBI's intermediary registry; and the presence of an external link in the advertisement.

Each ad was assessed against these six factors on a simple binary basis. Ads matching four or more indicators were classified as high risk, those matching two or three were categorized as medium risk, and those matching zero or one were considered low risk. The results were concerning: more than one-third of the advertisements in our sample qualified as either medium or high risk. Examples of high-risk ads can be seen in Figs. 8 and 9. While this framework is deliberately conservative and does not constitute a definitive identification of fraud, it suggests that a significant share of financial advertisements on Meta exhibit patterns that warrant scrutiny.

That such a straightforward assessment flags so many advertisements also makes a broader point: if a basic rule-based screen can surface this volume of potentially problematic content, platforms can easily create sophisticated rules to identify and address these ads.

These findings reveal a significant failure in Meta's enforcement of SEBI's regulatory framework. Despite the mandatory compliance deadline having passed nearly two months prior, the overwhelming majority of financial advertisements continue to operate without proper registration, while a substantial portion exhibit characteristics commonly associated with fraudulent schemes. Moreover, as our analysis demonstrates, identifying non-compliant ads is well within Meta's technical capabilities. This suggests that the enforcement gap stems not from technical limitations but from a deliberate choice to implement only minimal compliance measures. This lack of proactive enforcement is particularly concerning given that SEBI developed this directive in direct consultation with Meta, and that Meta itself established the compliance timeline that has now lapsed.

Ads at High Risk of Being Scam Ads

33%

Examples of High-Risk Ads

Fig. 8: Note the graph suggesting astronomical returns within a single day

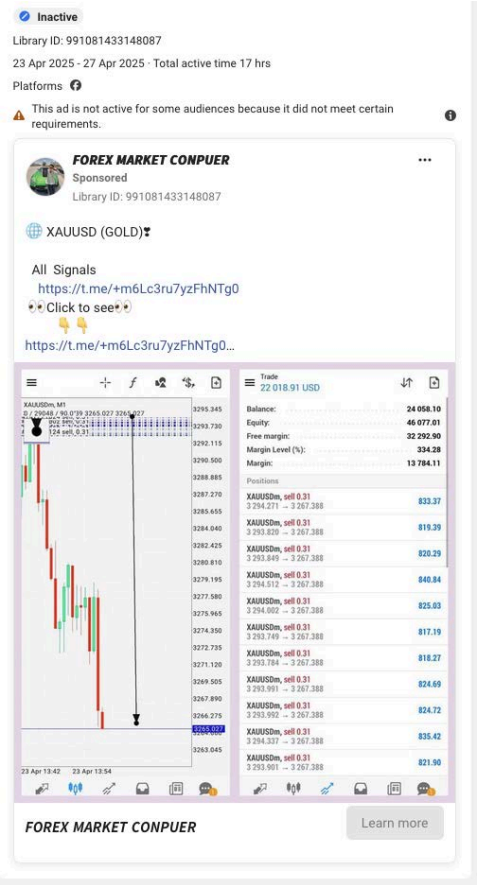


Fig. 9: More hooks to lure unsuspecting investors

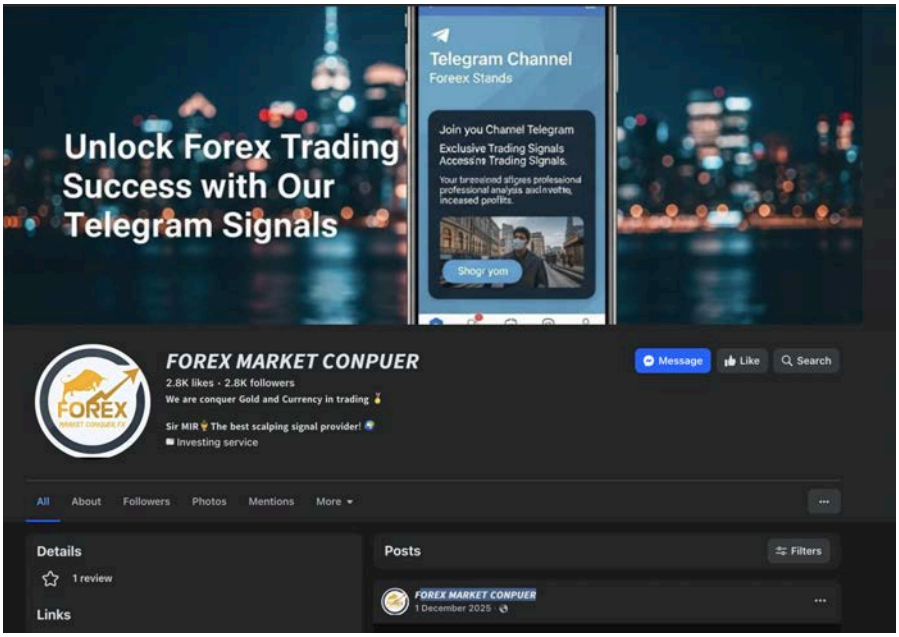


Fig. 10: High-Risk Advertiser Page

Conclusion

This report demonstrates that Meta's platforms play a central and persistent role in India's escalating scam ecosystem. The scale and sophistication of scam advertising on social media, coupled with the emotional, financial, and social harms borne by victims, have made it a very serious threat.

Meta's internal documents reveal that it has prioritized revenue generation over user safety. Even as scams generate massive financial losses globally and exploit individuals across India, Meta continues to profit from dubious advertisements rather than meaningfully restricting them.

As shown by Reuters, its enforcement systems are designed to allow a staggering volume of scam ads daily, rejecting the vast majority of credible user complaints against scammers while only acting against advertisers when automated systems reach near-total certainty of fraud. This business model has effectively normalised scams, despite the harm they cause.

India's regulatory intervention through the SEBI directive represents an important first step, but Meta's deliberately limited compliance mechanisms reveal the inadequacy of relying on platform self-regulation. Our stress tests show that Meta's verification tools are riddled with vulnerabilities—ranging from the ability to run financial ads without declaring them, to exceedingly weak identity checks for "exempted" advertisers, to disclaimers that give unregistered entities an undeserved veneer of legitimacy. Large-scale scraping of advertising data further confirmed that compliance remains overwhelmingly voluntary, with nearly all financial ads bypassing SEBI's intended safeguards. We are confident that Meta has the technical capability to do better.

Ultimately, addressing India's scam crisis requires recognising that platforms like Meta are not neutral intermediaries but profit-driven actors whose incentives currently run counter to public safety. Stronger regulatory oversight—backed by enforceable penalties, independent audits, and mandatory advertiser identity verification—is needed to close the gaps that allow fraudulent actors to operate with impunity. As long as compliance remains optional and enforcement superficial, scam ecosystems will continue to evolve alongside platform design. Protecting users in India's rapidly digitizing

economy, therefore, demands a coordinated regulatory response that treats scam advertising not as an isolated misuse of technology, but as a structural vulnerability engineered and sustained by platforms themselves.

Recommendations

I. Recommendations for SEBI, Central Consumer Protection Authority (CCPA), and Other Government Regulators: Platform Compliance and Enforcement Requirements

1. Strengthen Mandatory Platform Compliance for Financial Advertising

- Require platforms to **automatically detect** financial and investment-related content using keyword and pattern recognition, rather than relying on voluntary advertiser declarations.
- Mandate **pre-publication verification** for all financial promotions—paid ads, reels, posts, stories, influencer content, and affiliate links.
- Impose **strict penalties on platforms** for running undeclared financial ads, including escalating fines based on ad volume and user reach.

2. Establish Legally Enforceable Advertiser Identity Verification Standards

- Require platforms to implement **robust multi-factor verification** (government ID, One Time Password on phone, and live selfie check) for all advertisers to prevent fraudulent advertising.
- Prohibit platforms from accepting **AI-generated IDs, scanned images from search engines, or unverifiable documents**; require machine-readable, cryptographically validated IDs where possible.
- Mandate verification of financial intermediaries like banks, investment advisors, investment educators, etc., through identification mechanisms like Goods and Services Tax Identification Number (GSTIN); Permanent Account Number (PAN); or Udyam Aadhar Verification APIs, preventing impersonation of legitimate organisations.

3. Enable User-Centric Safeguards and Accessible Reporting Channels

- Require platforms to simplify scam-reporting tools and respond within **24–48 hours**, with penalties for failure to act on verified reports.
- Mandate **warning screens** for users who click on suspicious ads, using risk markers such as urgency language or guaranteed returns.
- Fund public awareness campaigns addressing stigma and victim-blaming, which discourage reporting.

4. Establish Participatory Oversight and Policy Development Mechanisms

- Government of India to mandate multi-stakeholder consultations with scam victims, consumer rights groups, digital rights organisations, and civil society representatives in the development and review of platform safety policies and compliance standards.
- Ensure participatory processes are accessible across languages, digital literacy levels, and geographic regions to enable meaningful input from diverse stakeholder groups.
- Government of India to create independent oversight bodies that include representatives from affected communities, victim support groups, and grassroots organizations to monitor platform enforcement and recommend improvements.

II. Policy Recommendations for Ministry of Electronics and Information Technology

1. Shift Liability toward Platforms that Profit from Scam Advertising

- In line with EU regulations, establish a platform liability framework in which platforms bear responsibility for:
  - harm caused by non-compliant financial ads,
  - failure to prevent repeat offenders,
  - using systems that knowingly allow high-risk ads to run, as seen in Meta's clear identification of 15 billion higher risk ads that it showed to users (Horwitz 2025a).
- **Link penalties to ad revenue generated** from fraudulent advertisements to remove incentives for under-enforcement. Government expenditures on cybercrime can be recovered from platforms making money from these advertisements in the form of penalties.

2. Expand SEBI's Regulatory Framework to Cover Organic and Influencer Content

- Broaden SEBI's advisory to cover **organic financial promotions**, including:
  - influencer posts,
  - short videos (reels, shorts),
  - WhatsApp/Telegram funnel promotions and
  - pseudo-educational content linking to investment schemes.
- Require influencers and content creators promoting financial products to display **visible SEBI registration disclosures**, similar to paid ads.

III. Recommendations to Improve Monitoring Mechanisms

1. Require Independent Audits of Platform Ad Safety and Algorithmic Enforcement

- Require platforms to maintain transparent, accessible channels for ongoing engagement with civil society, ensuring that the voices and experiences of vulnerable populations inform policy design and implementation.
- Mandate **annual third-party audits** of Meta, Google, and YouTube's scam-detection systems, with results submitted to SEBI, MeitY, and India's nodal agency for cybersecurity response, the Computer Emergency Response Team (CERT-In). Require transparency reports on:
  - detection accuracy,
  - false-negative rates,
  - volume of high-risk ads removed,
  - advertiser repeat-offender rates, and
  - Revenue generated from suspicious ads.
- Prohibit platforms from using **penalty bids** to monetise likely fraudulent advertisers.

2. Implement Real-Time Enforcement Through a National Digital Ad Registry

- Create a centralised, API-enabled registry where every financial ad must be logged before publication, including:
  - advertiser identity,
  - SEBI registration,
  - ad copy and targeting parameters,
  - payment details.
- Platforms would be permitted to publish ads only if they receive a **unique registry ID.**

IV. Cross-Border Cooperation and Coordination

1. Strengthen Cross-Border Enforcement and Cooperation

- Create a coordinated mechanism between SEBI, CERT-In, INTERPOL, and neighboring jurisdictions to track transnational scam networks.
- Require platforms to share high-risk advertiser information with regulators and law enforcement.

References

Bansal, Aakriti. 2025. "Meta Requires SEBI Registration for India-Specific Investment Ads." MEDIANAMA. July 2025. https://www.medianama.com/2025/07/223-meta-sebi-verification-indian-investment-ads/.

Barua, Joyce. 2025. "Verification and Transparency Requirements for Advertisers Targeting Users in India with Securities and Investments Ads." Facebook.com. June 26, 2025. https://developers.facebook.com/blog/post/2025/06/26/verification-and-transparency-requirements-for-advertisers-targeting-users-in-india-with-securities-and-investments-ads/.

Fletcher, Emma. 2023. "Social Media: A Golden Goose for Scammers." Federal Trade Commission. October 6, 2023. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers#1.

Global Anti-Scam Alliance (GASA). 2025. "Global State of Scams - 2025." Gasa.org. Global Anti-Scam Alliance. December 31, 2025. https://gasa.org/knowledge-base/reports/global-state-of-scams-2025.

Hasan, Waquar. 2024. "How Meta Ads Enable Loan Scam That Misuse Aurangabad Bank's Name | BOOM." Decode. Boomlive.in. June 11, 2024. https://www.boomlive.in/decode/meta-ads-enable-loan-scam-that-misuse-aurangabad-banks-name-25597.

Horwitz, Jeff. 2025a. "Meta Is Earning a Fortune on a Deluge of Fraudulent Ads, Documents Show." Reuters, November 6, 2025. https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/.

Horwitz, Jeff. 2025b. "Meta's 'Trusted Experts' Helped Me Run Scam Ads on Facebook and Instagram." Reuters, December 15, 2025. https://www.reuters.com/investigations/metas-trusted-experts-helped-me-run-scam-ads-facebook-instagram-2025-12-15/.

Horwitz, Jeff. 2025c. "Meta Created 'Playbook' to Fend off Pressure to Crack down on Scammers, Documents Show." Reuters, December 31, 2025. https://www.reuters.com/investigations/meta-created-playbook-fend-off-pressure-crack-down-scammers-documents-show-2025-12-31/.

International Organization of Securities Commissions (IOSCO). 2025. "IOSCO'S Statement on Combating Online Harm and the Role of Platform Providers." IOSCO.org. May 21, 2025. https://www.iosco.org/news/pdf/IOSCONEWS770.pdf.

Mahala, Sanjukta. 2026. "SEBI | Ease of Doing Investment (EoDI)—Disclosure of Registered Name and Registration Number by SEBI Regulated Entities and Their Agents on Social Media Platforms (SMPs)." Sebi.gov.in. February 26, 2026. https://www.sebi.gov.in/legal/circulars/feb-2026/ease-of-doing-investment-eodi-disclosure-of-registered-name-and-registration-number-by-sebi-regulated-entities-and-their-agents-on-social-media-platforms-smps-_100005.html.

Nath, Pratiti. 2024. "Facebook Ads Used to Create Malware of AI Tools like Midjourney." MEDIANAMA. April 12, 2024. https://www.medianama.com/2024/04/223-hackers-fake-facebook-ads-malware/.

Press Trust of India (PTI). 2025. "Citizens Lost over Rs 22,845 Crore to Cyber Criminals in 2024: Govt." The Economic Times. Economic Times. July 22, 2025. https://economictimes.indiatimes.com/news/india/citizens-lost-over-rs-22845-crore-to-cyber-criminals-in-2024-govt/articleshow/122834896.cms.

Securities and Exchange Board of India (SEBI). 2025a. "Advisory to SEBI Registered Intermediaries- Uploading Advertisements on Social Media Platforms (SMPs)." Sebi.gov.in. 2025. https://www.sebi.gov.in/media-and-notifications/press-releases/mar-2025/advisory-to-sebi-registered-intermediaries-uploading-advertisements-on-social-media-platforms-smps-_92866.html.

Securities and Exchange Board of India (SEBI). 2025b. "SEBI Intensifies Efforts to Combat Online Investment Scams, Calls for Greater Collaboration from Social Media Platforms." https://www.medianama.com/wp-content/uploads/2025/11/SEBI-PR.pdf.

Shivangini. 2024. “Is Telegram Staring at a Ban in India? Messaging App Becomes Petri Dish for Financial Frauds and Exam Scams.” Livemint.com. August 27, 2024. https://www.livemint.com/companies/news/telegram-ceos-arrest-did-messaging-platform-become-a-petri-dish-in-india-for-financial-frauds-exam-scams-and-more-11724731138037.html.

Singh, Amit. 2025. “SEBI Can Now Order Takedown of Misleading Stock Content Online.” MEDIANAMA. December 17, 2025. https://www.medianama.com/2025/12/223-sebi-takedown-misleading-stock-content-online/.

Vatyam, Nirupa. 2024. “Verified or Duped? Students Caught in Social Media Scam.” The Times of India. December 2, 2024. https://timesofindia.indiatimes.com/city/hyderabad/students-duped-by-discounted-social-media-verification-scams/articleshow/115875331.cms.

Please share with all who you know are concerned about online scams!

Ekō is 23,528,130 people stopping big corporations from behaving badly.
https://www.eko.org/

Bard Human Rights Project
Examining human rights through teaching, research, and public programs.
https://hrp.bard.edu/

Forum for Developing Communities
Bridging India and the Diaspora.
https://forumdc.org

Acknowledgements

We would like to thank Rewan, Jhanvi, Apar, Sarah, Alex, Snigdha, Ojas, Dhananjay, and Ahan for all your thoughts and inputs.