GSMA

# India Consumer Scam Report 2025: More Reporting, Less Trust in Outcomes

ARMIDALE

**The GSMA** is a global organisation that unifies the mobile ecosystem to discover, develop, and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full potential of connectivity, enabling people, industry, and society to thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at **www.gsma.com**

Follow the GSMA on X: **@GSMA**

# Authors

**Leslie Falvey** & **Tyson Hackwood** are the Founders of Armidale and founding members of CROSEC. Together they bring board-level experience across telecoms, technology, payments and retail, with deep specialisation in fraud prevention, growth, and strategy execution. They translate research into practical playbooks that reduce losses, enhance recovery, and foster trust.

# Acknowledgements

We thank Julian Gorman, Head of Asia Pacific at GSMA, for his input and guidance on this report, as well as the GSMA APAC team for their support in outreach and visibility. We are also grateful to the survey partners, Milieu Insight and respondents across the ASEAN region, whose participation made these insights possible.

Data sources: This report draws on Armidale's 2024 and 2025 ASEAN consumer scam and fraud surveys and an addendum study completed to cover India (n≈500 per market) and associated qualitative insights gathered during analysis and industry consultations.

Contact the authors: **contact@armidale.co**

# Foreword

This annex adds India to the broader 2025 consumer scams work, intending to identify how scams manifest, the harm they cause, where victims report, and what protection people expect from banks, platforms, and mobile/internet providers. The focus is practical: highlight what matters for prevention, incident response, and rebuilding trust.

Findings come from a quota-representative online survey of adults in India (n≈500, 2025). Results are presented for India; occasional ASEAN-6 references are included for context only. When used, the ASEAN-6 benchmark is an equal-weighted average of Indonesia, Malaysia, The Philippines, Singapore, Thailand, and Vietnam from the 2025 study.

Percentages refer to the share of respondents unless noted. Multi-select questions reflect all channels or outcomes involved so that totals may exceed 100%. Values are rounded, and small differences may occur.

# Executive Summary

Scams have become a significant consumer issue in India. 53% of adults report lifetime exposure, and 42% say the risk is increasing rapidly. The journey is overwhelmingly digital and multi-surface: victims most often cite messaging apps (46%), SMS (37%), email (33%), social platforms (33%) and voice (32%), with search ads (19%), QR/payment links (18%) and even dating apps (14%) in the mix. 10% believe they were personally targeted by AI-enabled scams (self-reported, but a strong signal that real-time OTP relays and convincing impersonation are already in play).

Harm is tangible. 65% of victims lost money (14% large losses), and many describe emotional distress (50%), ongoing anxiety (43%), and the time and effort (40%) it takes to put things right. People do act: most tighten account security and monitor more closely, and a growing share default to calling back on official numbers rather than trusting inbound links or calls.

Reporting is active and spread across multiple doors. Only 14% do not report; the rest go to platforms (46%), banks/e-wallets (40%), police (37%), and their mobile/ISP (33%). That breadth is a strength for detection, but it fragments cases and slows recovery when hand-offs aren’t joined up.

Trust in protective outcomes is the gap that needs to be closed. Ratings of “good/very good” protection are consistently low across banks, platforms, telcos/ISPs, merchants/marketplaces, and government, even as people expect all of them to act. The same consumers are willing to support targeted, privacy-preserving fixes: 47% approve of purpose-limited mobile-network signals used at transaction time to prevent fraud, rising to 84% comfort when sharing occurs only in response to suspicious activity. Security also moves market share: a clear majority say they would switch to a more secure financial provider that uses authorised, minimal checks.

The path forward is practical. Make prevention visible where scams actually land (messaging, SMS, email, social, search, QR); bind numbers and devices and check for recent SIM-change/device risk at login, payout changes and high-risk payments; surface

confirmation-of-payee cues before money moves; and turn reporting into resolution with a single case record, clear roles and SLAs across platform to bank/e-wallet to telco to police. Done well, this reduces losses, shortens the time to action, and rebuilds confidence without exposing broad data.

# Prevalence, Perception and Personal Worry

Indians report substantial exposure to scams: 43% have been scammed before, and an additional 10% were a victim within the past year, indicating a problem that is both widespread and still growing.

Perceived risk is accelerating, with 42% saying the threat is increasing rapidly, suggesting significant momentum rather than a static background hazard.

Anxiety is very high and similar to the levels seen around ASEAN. 58% describe themselves as very worried, and an additional 35% register some concern with the situation.

10% say they have been personally targeted by AI-enabled scams; this is self-reported and difficult to verify in practice, but it is a meaningful signal that should be closely monitored.

# Attack Surface: Channels of Contact

India's victim journey is distinctly digital and multi-surface.

Among those scammed, people most often cite messaging apps (46%), SMS (37%), email (33%), social platforms (33%), and voice calls (32%), with search ads/sponsored links (19%), QR codes/payment links (18%), and dating apps (14%) also prominent. Incidents typically involve more than one channel, and the mix skews away from pure voice toward link-led and app-embedded touchpoints.

The pattern suggests credential capture, ad- or message-driven redirections, and embedded payment flows that include QR "quishing" and real-time OTP relay (AiTM)-style takeovers. In combination, these routes create a broad, fast-moving attack surface across inboxes, chat, social commerce, and offline-to-online QR entry points, consistent with later findings on payment-link scams and account compromise.

# What Works for Scammers in India: Types and Triggers

Indian victims most often point to transaction-led and access-seeking scams. The leading categories encountered are online shopping non-delivery/quality disputes (32%), job/income-opportunity pitches (30%), QR/payment-link scams (30%), and tech intercept/account takeover via SIM-swap/OTP/password theft (30%). Password-disclosure phishing is also common (26%). By contrast, government/law-enforcement impostors are reported less frequently (17%). Investment/trading sits in the mid-range (25%).

The psychology that moves people in India is consistent with those scam types. Urgency/time-pressure is cited most often (40%), followed by secrecy/confidentiality (33%) and scarcity/limited-offer cues (28%), with authority/impersonation also present (30%). Reciprocity/freebies land less often (21%). The combination of urgency and privacy follows the theme of link-driven and app-embedded flows (e.g. QR “quishing”, sponsored-link redirects, and real-time OTP relay) that rush a payment or reset before people can verify.

Taken together, India’s profile is less about scripted phone tricks and more about pushing a fast transaction, harvesting a factor, and/or seizing the account; this pattern aligns with the country’s heavier use of messaging, SMS, email, search ads, and QR in the victim journey.

# Victim impact and severity

Scams in India leave a mark that is both financial and personal. 61% of victims name financial loss among the biggest impacts, and many also describe emotional distress (50%) and ongoing anxiety (43%). The practical burden is real, with 40% pointing to the time and effort required to sort things out. In total, 65% say they lost money (spread across small (26%), moderate (25%), and large (14%) amounts) while 35% lost no money but still experienced harm.

People do speak up, but they don’t all go to the same place. Only 14% choose not to report; the rest are split across platforms (46%), banks and e-wallets (40%), the police (37%), and their mobile or internet service provider (33%).

That fragmentation makes it hard for any single organisation to see the full case quickly. A shared handoff with a single case ID and clear roles would reduce duplication, expedite the first response, and increase the likelihood of recovering funds.

The severity profile indicates a significant issue. Of people who have been scammed 14% report large losses of amounts that still concern them today, while at the other end 35% lose no money but still feel shaken.

# Post-incident behaviour change

People do not stand still after a scam. A majority say they tightened account security (by using new passwords and 2FA/passkeys) and monitored their accounts more closely. Many also installed or upgraded security tools, changed contact details, and shifted to “call back via official numbers” rather than trusting inbound links or calls. Only a small minority made no changes.

The overall picture is a population that adapts quickly, which is encouraging, but it also means scammers adjust their scripts in response, keeping the pressure on providers to evolve controls.

# Reporting Behaviour: More Active, to More Endpoints

Indians are more likely to report scams and report them to more than one place. 14% do not report, while the rest spread cases across platforms (46%), banks/e-wallets (40%), police (37%), and their mobile/internet provider (33%).

The pattern points to engaged responders who know where the levers are, platforms to take down content, financial institutions to flag transactions, law enforcement to log offences, and ISPs/MNOs to address network abuse. Compared to ASEAN-6, each route is used more frequently, with ISPs/MNOs notably higher, underscoring India's broader use of every available reporting channel.

# Perceived Quality of Protection: India's Trust Gap

India stands out for a sharp confidence deficit in how well the ecosystem protects consumers. Across every actor tested (i.e. banks and e-wallets, mobile/ISPs, device and platform providers, merchants/marketplaces, and government), the share rating protection as "very good/good" is much lower than elsewhere, and the share rating "poor/very poor" is much higher.

This gap is most pronounced for banks and e-wallets, as well as device/OS platforms, with mobile ISPs and marketplaces also scoring significantly below regional norms. In short, Indians report incidents, but they don't believe the system prevents harm or resolves cases effectively for them.

The pattern aligns with India's attack surface: scams arrive through links, apps, ads, and QR codes, rather than just voice, so people expect fast takedowns, swift fund freezes, clear status updates, and visible outcomes.

# Who consumers expect to lead

Indians spread primary responsibility across government policymakers, banks and e-wallets, police, and mobile/ISPs), with telcos/ISPs being named by an unusually large share compared with other markets.

That pattern mirrors India's reporting habits (people use multiple doors) and its channel mix (heavy messaging/SMS/email/QR/search). The message is straightforward: protection is a shared mandate, and telcos are expected to be at the forefront alongside banks and platforms.

# Social Commerce and Platform Landscape

Buying through social and conversational apps is mainstream in India. WhatsApp serves as a primary transaction channel for many consumers, and Instagram and Facebook also facilitate frequent purchasing.

Perceptions of platform risk track that activity. Indians commonly associate Telegram and WhatsApp with scams, with Instagram, X, and Snapchat also flagged. Facebook is also widely associated with scams, despite being a significant platform for shopping.

A notable paradox ~~emerges in risk scoring: despite heavier use and stronger scam~~ associations on chat and social media platforms, people are less likely to label these channels as "very high/high risk." Two factors may be at play: everyday exposure that normalises risk (users develop coping habits) and scale compression (respondents reserve top-end ratings for only the most extreme threats).

# Attitudes to Data-Sharing for Fraud Prevention

Support for data sharing in the interest of protecting consumers is strong and decisive. 47% say they approve of providers using minimal, purpose-limited signals at transaction time to stop fraud, and another 34% approve when this is limited to suspect transactions only; just 19% are uncomfortable with data sharing for this purpose.

The centre of gravity sits at the “fully supportive” end, even more so than in most markets, and acceptance strengthens further when sharing is triggered only on suspicious activity. The message is clear: Indians will permit tightly scoped, outcome-based checks when they can see how it prevents fraud without broad or ongoing data use.

# Willingness to switch for security (India)

Security moves market share. Well over half of Indian consumers say they would switch to a more secure financial provider. The combination of strong support for data sharing and high switching intent is a clear signal: make protection visible and effective, and consumers will reward it.

# Conclusion

India’s story is clear: scams are common, the attack surface is broad and digital, and people want protection that actually works. 53% report at least one lifetime impact, channels are link- and app-led (messaging, SMS, email, search, QR), and the playbook that moves people is speed and privacy which lend themselves to online link-oriented scam types.

Self-reported AI-enabled lures are visible at 10% and should be watched closely, and QR/payment-link routes are already part of common scam journeys. This is a rapidly evolving ecosystem that will quickly incorporate new tactics.

People do their part. 86% of victims report somewhere, and they often use multiple doors (platforms, banks/e-wallets, police, and their mobile provider/ISP). They are also changing their behaviour: increasing security on accounts, closer monitoring, and calling back on official numbers. The missing piece is what happens next. Fragmented reporting means that no one can see the whole case quickly, and this erodes confidence.

The fix is practical and measurable. Make hand-offs seamless: one case record, one case ID, clear roles, and SLAs across the platform to bank/e-wallet, telco, and police. Put time-to-first-action, funds-recovery attempts, and status updates on a clock that consumers can see. Tie prevention to the real routes: confirmation-of-payee before money moves; friction and takedown on social and marketplaces; number-binding plus recent SIM-change/device checks at login, payout changes and high-risk payments; safe call-back as the default habit.

Data use can be part of the solution when applied in a tight and transparent manner. 47% are fully supportive with purpose-limited, transaction-time signals and support rises further when sharing triggers only on suspicious activity. That opens the door for Open-Gateway-style checks, SIM swap, device/number match, call-forwarding state, and location checks, all without invasive data exposure. Explain sharing in plain language, keep retention brief, and make outcomes visible; support will be sustained.

Trust is the gap to close. Ratings of protective quality are low across banks, platforms,

~~telecom companies,~~ and the government, even as India expects all of them to act. Delivering faster resolutions, clearer communications and fewer “dead-ends” will reverse that.

Security also moves market share: a majority say they would switch to providers that make protection obvious. The organisations that operationalise the playbook channel by channel, with joined-up response and minimal, authorised signals, will cut losses, rebuild confidence and win customers.

# Other related reports and information:

ASEAN Consumer Scam Report 2025: Victims Rising, Defences Under Strain

Consumer Attitudes Toward Fraud and Opportunities for Mobile Network Operators in SEA

Unlocking Innovation: The Role of MNO APIs