

India Consumer Scam Report 2026: Permission Granted, Cases Still Open





The GSMA is a global organisation that unifies the mobile ecosystem to discover, develop, and deliver innovations 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 and follow the GSMA on X ([@GSMA](https://twitter.com/GSMA))

Author

Leslie Falvey is a senior executive and board member with a career spanning strategy consulting and the leadership of telecommunications and technology companies. Co-Founder of Armidale and a founding member of CROSEC, he brings this depth of executive and industry experience to fraud prevention, growth and strategy work across operators, financial services and digital platforms.

Acknowledgements

Our thanks to Julian Gorman, Head of Asia Pacific at GSMA, and to Jeanette Whyte, Head of Public Policy & External Affairs at GSMA, whose guidance shaped this year's report. We are grateful to the GSMA APAC team for taking the work to a wider audience, and to Milieu Insight for conducting the fieldwork. Our greatest debt is to the five hundred consumers in India who answered, many of them recounting difficult experiences.

Data sources: This report draws on Armidale's 2026 consumer fraud survey in India (n≈500), compared with the 2026 survey across six ASEAN markets (n≈500 per market), and associated qualitative insights gathered during analysis and industry consultations. References to India's reporting arrangements draw on the Ministry of Home Affairs, "Indian Cyber Coordination Centre", Press Information Bureau, 17 March 2026, covering the Citizen Financial Cyber Fraud Reporting and Management System operated by the Indian Cyber Crime Coordination Centre, the 1930 helpline and the amounts saved through reported complaints, and on the Department of Telecommunications, "1000+ banks, TPAPs and financial institutions onboarded on DoT's Digital Intelligence Platform", Press Information Bureau, 22 December 2025.

Contact the author: contact@armidale.co

Contents

Foreword	2
Executive Summary	3
1 Scams and the Indian Consumer	5
2 What Actually Happens to a Scam Case	9
3 Trust and the Room to Act	13
4 What the Ecosystem Can Do Next	18
Consumer survey methodology	21

Foreword

India's digital economy has transformed how people communicate, bank, shop, work and access services. Mobile connectivity sits at the heart of that transformation. As digital participation has grown, however, so too has the challenge of protecting consumers from increasingly sophisticated scams.

This report offers reasons both for confidence and for continued action. Consumers surveyed in India are highly likely to report scams, and reported cases are more likely to reach resolution than across the six ASEAN markets covered by our research. Yet too many cases still remain unresolved, and too many consumers who lose money recover nothing.

Perhaps the most striking finding is the level of permission consumers give institutions to help protect them. Some 87% of respondents are comfortable with their bank or financial provider holding and using their data to detect fraud, while 81% say the same of their mobile operator.

This is significant. It suggests that consumers are prepared to support more effective use of data when there is a clear purpose and a tangible benefit in protecting them from fraud.

The opportunity now is to turn that trust and permission into better protection. That means improving what happens when a scam is reported, resolving more cases and recovering more of what is lost. It also means looking beyond individual interventions towards stronger collaboration across the institutions that make India's digital economy work.

Mobile operators have an important role to play. Their contribution goes beyond connectivity and reporting. Trusted network capabilities can help financial institutions, digital platforms and other service providers strengthen authentication, identify risk and protect consumers. Greater use of common, interoperable capabilities, including those enabled through GSMA Open Gateway, can help strengthen digital trust across the ecosystem, while respecting privacy and avoiding unnecessary friction for consumers.

No single organisation can solve the scam challenge alone. Scams move across networks, platforms, financial services and borders. Effective protection therefore depends on mobile operators, financial institutions, digital platforms, government and law enforcement working together, with each bringing its capabilities and information to a shared objective.

India has strong foundations on which to build. The challenge now is to convert consumer trust into stronger protection, reports into resolution and the capabilities across the ecosystem into better outcomes for people.

I trust this report contributes to that effort and, above all, encourages practical collaboration and action.

Julian Gorman

Head of Asia Pacific, GSMA

Executive Summary

| **86%**

of victims report the scam
to an organisation

| **33%**

of reported cases are
still unresolved

| **87%**

would let their bank
hold their data

When an Indian consumer is scammed, they tell someone. The survey finds that 86% of victims take the case to an organisation, compared with 69% across the six ASEAN markets surveyed (ASEAN-6). An organisation took responsibility for 65% of reported cases, compared with 53%, and 33% of reported cases remain unresolved, compared with 45%. Among victims who lost money, 33% recover some or all of it, compared with 18%.

Real harm remains behind those figures. A third of reported cases end unresolved, and 67% of victims who lost money recover nothing.

Indian consumers also extend institutions an unusual level of permission to use their data. Some 87% are comfortable with their bank or financial provider holding and using their data to detect fraud, 82% with government, 81% with their mobile operator and 73% with digital platforms. Each figure is higher than the corresponding ASEAN-6 result. Operators are rated highly on delivery as well: 65% rate their mobile operator's protection 8 or above out of 10, compared with 49% across ASEAN-6, and the gap between the responsibility consumers assign operators and the protection they rate them on is 9.2 percentage points, compared with 23.9 across ASEAN-6.

Permission is not uniform. Consumers whose case was resolved report higher comfort with institutions using their data than those whose case remains unresolved: 88% compared with 64% for government, and 87% compared with 57% for digital platforms. For banks the difference is small, 87% compared with 85%.

The opportunity is to turn that trust and permission into stronger protection. Indian consumers report only a narrow gap between the friction they already experience in online transactions, at 6.4 out of 10, and the most they say they would accept for stronger protection, at 6.9. That points towards better resolution, better recovery and closer coordination between institutions rather than more checks at the point of payment.

GSMA India Consumer Scam Report 2026

Permission granted, cases still open

Indian consumers report their scams, hand the case to institutions and extend them more trust than consumers in any of the six ASEAN markets. More of those cases close, and victims whose case is resolved give institutions the most permission.

Scams reach most Indian consumers

Twelve percent were scammed in the last year. Indian consumers hold themselves responsible, yet fewer have enhanced their account security than in any of the six ASEAN markets.

were scammed within the last 12 months

12%

have changed their behaviour because of scams

72%

have enhanced their account security

49%

Victims report, and cases close

Reporting, ownership and recovery are higher than in any of the six ASEAN markets. A third of reported cases still end unresolved.

of victims take the case to an organisation

86%

of reported cases have an organisation take responsibility

65%

of victims who lost money recover some or all of it

33%

Permission is lower where cases stay open

Indian consumers grant institutions wide permission. Victims whose case is unresolved are less comfortable with government and digital platforms holding their data, and there is little room to add friction.

are comfortable with their bank holding data to detect fraud

87%

of victims with an unresolved case are comfortable with government holding data, 88% if resolved

64%

point more friction consumers will accept, out of 10: 6.9 at most, against 6.4 today

0.5

What the ecosystem can do next

1 Improve what happens after the report

Extend coordination to the cases it does not yet close.

2 Turn resolution into digital trust

Permission is lower where cases stay open.

3 Banks and financial providers

Move from holding funds to returning them.

4 Digital platforms

Bring platform reports into the shared coordination.

5 Government and police

Publish cases resolved and money returned.

6 Mobile operators

Interoperable network capabilities, including Open Gateway.

01

Scams and the Indian Consumer



1

Scams and the Indian Consumer

Twelve percent of Indian consumers were scammed within the last twelve months, compared with 8% across ASEAN-6. Thirty-nine percent have not been scammed themselves but have watched someone close to them be scammed, similar to the 40% across ASEAN-6. Through their own experience or someone else's, 72% of Indian consumers have changed their behaviour because of scams, compared with 66% across ASEAN-6.

Indian consumers expect the problem to grow. Forty-two percent say the risks from scams and hacking are increasing rapidly, compared with 32% across ASEAN-6, and 75% are very concerned about the privacy of their personal data online, compared with 48% across ASEAN-6.

Fifty-two percent say they are absolutely worried about being scammed or hacked, compared with 59% across ASEAN-6. Ninety-one percent worry at least sometimes about being scammed or hacked, compared with 96% across ASEAN-6.

Online shopping scams are the most common type in India, at 33%, compared with 32% across ASEAN-6, followed by prize, lottery and inheritance scams at 31%, compared with 25%, and job or income scams at 30%, compared with 32%. Scams using a QR code or payment link stand at 27% in India, compared with 18% across ASEAN-6 and 23% in Thailand, the highest ASEAN market.

Messaging apps are the most common route in, involved in 42% of Indian victims' scams, similar to the 41% across ASEAN-6, followed by social media at 37%. Email is higher involved in 33% of Indian cases, compared with 17% across ASEAN-6 and 20% in Malaysia, the highest ASEAN market. Offline QR codes and payment links reach 21%, compared with 10% across ASEAN-6 and 13% in Malaysia and Indonesia, and sponsored search results 16%, compared with 9% across ASEAN-6 and 13% in Indonesia.

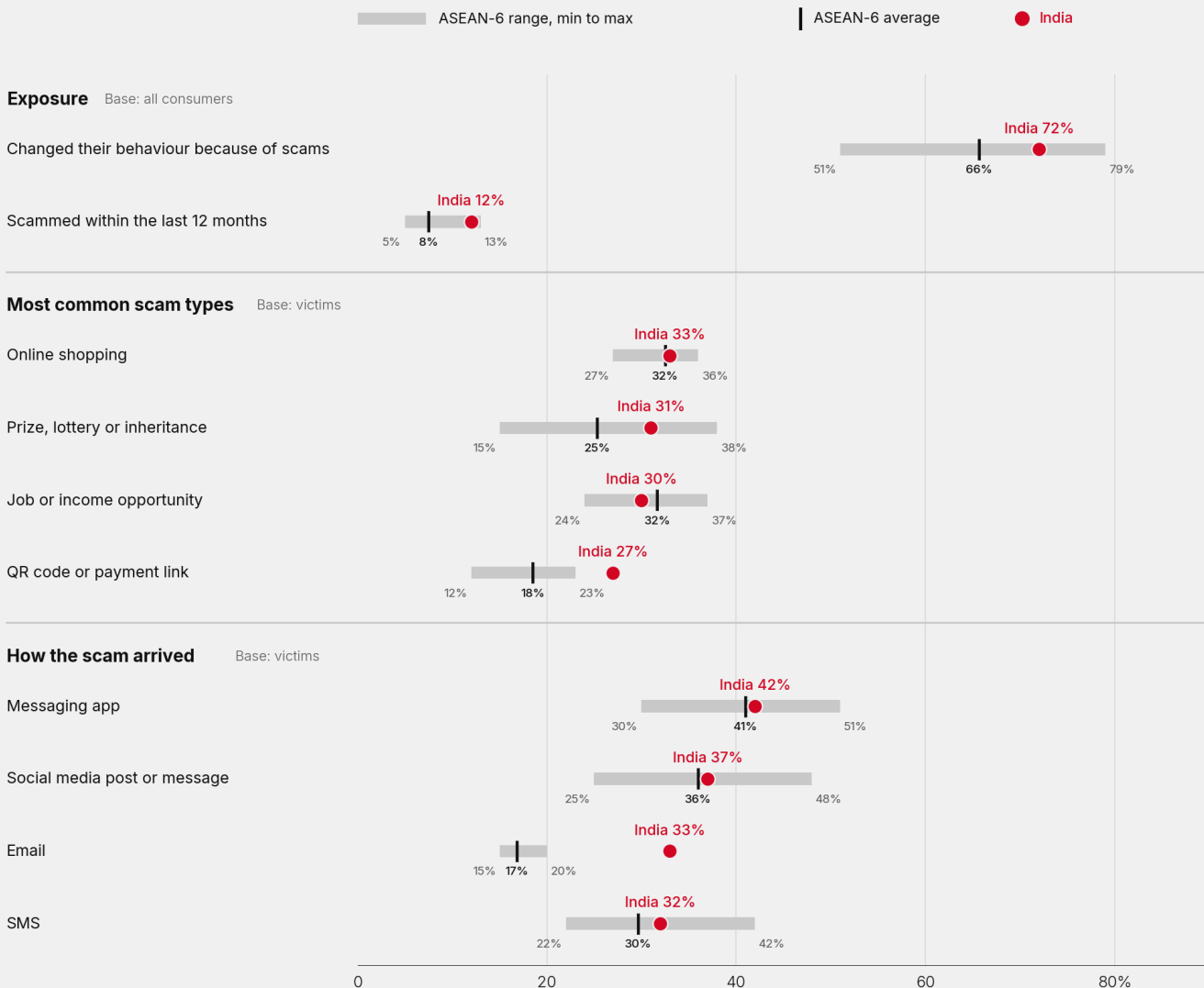
Urgency is the pressure scammers use most, at 39% in India, similar to 40% across ASEAN-6. In India secrecy or confidentiality comes next, at 33% compared with 22% across ASEAN-6 and 30% in Vietnam, the highest ASEAN market. Across ASEAN-6 the next are reciprocity, a free gift, reward or bonus, and fear of loss, each at 34%. In India reciprocity is the least used, at 24%, compared with 26% in Singapore, the lowest of the six ASEAN markets, and authority, posing as police, a bank or a government official, stands at 25% compared with 33% across ASEAN-6.

Eighty-nine percent of Indian consumers have seen AI used in scams, level with the region, and a further 11% saw scams but could not tell whether AI was involved. The most recognised techniques are AI-written messages and fake AI images, each seen by 48%, followed by fake AI profiles or adverts at 47% and deepfake video of a real person at 42%.

Figure 1

How scams reach Indian consumers

Percentage of consumers, and of victims for scam types and channels



Source: GSMA Consumer Scam Survey 2026. ASEAN-6 is the equal-weighted average of Singapore, Malaysia, Thailand, Indonesia, the Philippines and Vietnam.

Almost every Indian consumer has done something to protect themselves. Only 5% have taken no protective step at all, compared with 7% across ASEAN-6, and 37% have installed or upgraded security tools, compared with 31% across ASEAN-6 and 36% in Thailand, the highest ASEAN market. The gap is in hardening their own accounts. Forty-nine percent have enhanced their account security, compared with 58% across ASEAN-6 and 54% in Singapore and Thailand, the lowest of the

six ASEAN markets, and 42% monitor their accounts more closely, compared with 46%.

Where Indian consumers do act, they change how they deal with the organisations that contact them. Twenty-seven percent now call companies back on an official number rather than trust an inbound call or message, compared with 19% across ASEAN-6 and 23% in Malaysia, the highest ASEAN market, and 26% have cut back on or changed how they shop online, up from 20% in 2025 and compared

with 23% across ASEAN-6.

They also know what is being done on their behalf. Seventy-two percent are aware of scam education or protection programmes run by four or more of the six actor groups in the study, compared with 62% across ASEAN-6.

Indian victims take responsibility for what happened to them. Ninety-three percent agree that, looking back, they did something they should not have done, compared with 87% across ASEAN-6 and level with Indonesia, the highest ASEAN market. Eighty-six percent feel at least partly responsible, compared with 84% across ASEAN-6. They rate themselves capable, with 91% confident they could spot a similar scam now, compared with 86%, and 77% rating their own protection 8 or above out of 10, compared with 75%. Seventy-eight percent accept that a newer or more convincing scam could still catch them out, compared with 76%.

Indian consumers hold themselves accountable, rate themselves capable, and expect the institutions around them to carry as much of the load.

02

What Actually Happens to a Scam Case



2

What Actually Happens to a Scam Case

When an Indian consumer is scammed, they go looking for help. Eighty-six percent take the case to at least one organisation, compared with 69% across ASEAN-6 and 79% in Singapore, the highest ASEAN market, and those who report reach 1.99 organisations on average, compared with 1.87 across ASEAN-6. Forty-nine percent go to the police, up from 37% in 2025, compared with 36% across ASEAN-6. Forty-one percent go to their bank or e-wallet provider, compared with 36%, and 40% to the platform where the scam happened, compared with 32%. Thirty-six percent go to their mobile or internet provider, compared with 19% across ASEAN-6 and 27% in Thailand, the highest ASEAN market.

Fourteen percent of Indian victims do not take the case to any organisation, and 7% tell no one at all, compared with 17% across ASEAN-6 and 11% in Singapore, the lowest of the six ASEAN markets.

Most of those reports find an owner. An organisation took primary responsibility for resolving 65% of reported cases, compared with 53% across ASEAN-6 and 63% in Malaysia, the highest ASEAN market. This measures what the victim experienced, whether an organisation picked the case up and carried it, rather than whether a formal investigation followed.

Government or the police resolved 32% of the cases taken to them, compared with 30% across

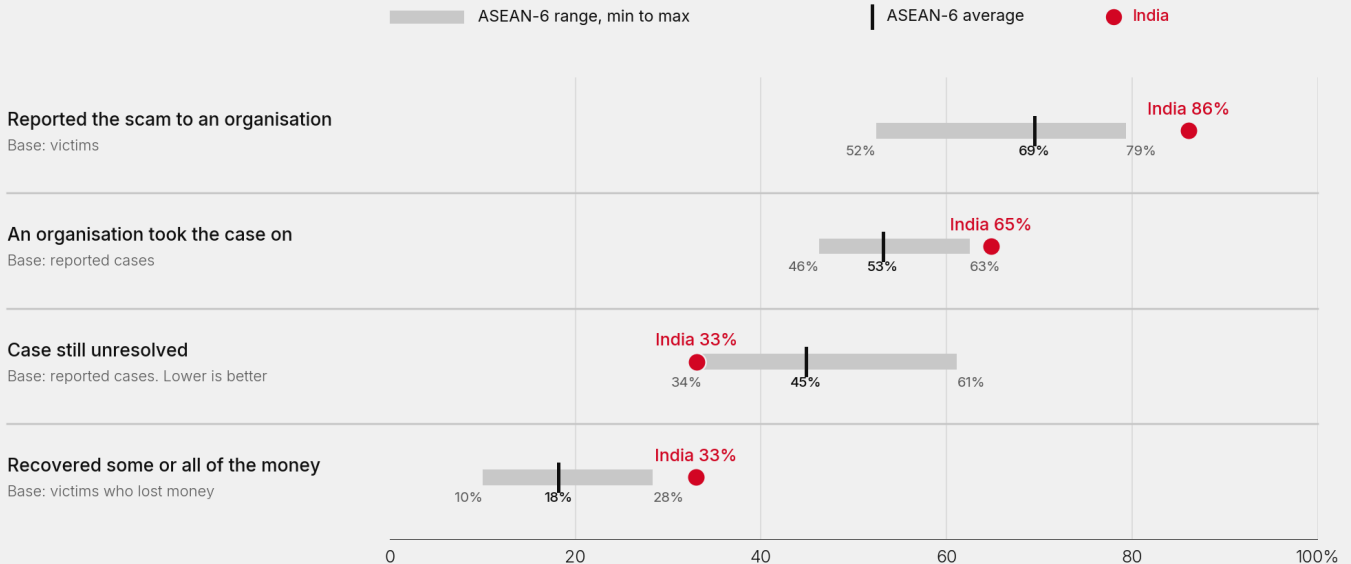
ASEAN-6. Banks and financial providers resolved 25% of the cases they received, compared with 19%, platforms 17%, compared with 19%, and operators 10%, compared with 16%. No organisation took responsibility for 35% of reported cases, compared with 47% across ASEAN-6 and 38% in Malaysia, the lowest of the six ASEAN markets.

Cases close more often and money comes back more often. Thirty-three percent of reported cases remain unresolved, compared with 45% across ASEAN-6 and 34% in Vietnam, the lowest of the six ASEAN markets. Twenty-two percent were fully resolved with the money returned, compared with 14% across ASEAN-6 and 21% in Singapore, the highest ASEAN market, and a further 17% were partly resolved with some money returned, compared with 11% across ASEAN-6 and 16% in Malaysia. Sixty-four percent of Indian victims lost money, compared with 68% across ASEAN-6, and 33% of those recovered some or all of it, compared with 18% across ASEAN-6 and 28% in Singapore.

Figure 2

What happens to a scam case

Percentage at each stage, on that stage's own base



Source: GSMA Consumer Scam Survey 2026. ASEAN-6 is the equal-weighted average of Singapore, Malaysia, Thailand, Indonesia, the Philippines and Vietnam.

That still leaves much of the harm unaddressed. Thirty-three percent of reported cases end unresolved, and 67% of those who lost money recover nothing. The harm is personal as well as financial. Asked which part of the scam had the biggest negative impact on them, 43% of Indian victims name ongoing anxiety or a loss of confidence, compared with 38% across ASEAN-6, 35% the time and effort of trying to resolve the case, compared with 39%, and 29% losing enough that it still worries them today, compared with 35%. Emotional distress is named as the biggest impact by 42%, compared with 50% across ASEAN-6 and 46% in Singapore and Indonesia, the lowest of the six ASEAN markets.

Victims whose case was resolved report higher comfort with institutions using their data to detect fraud than victims whose case remains unresolved.

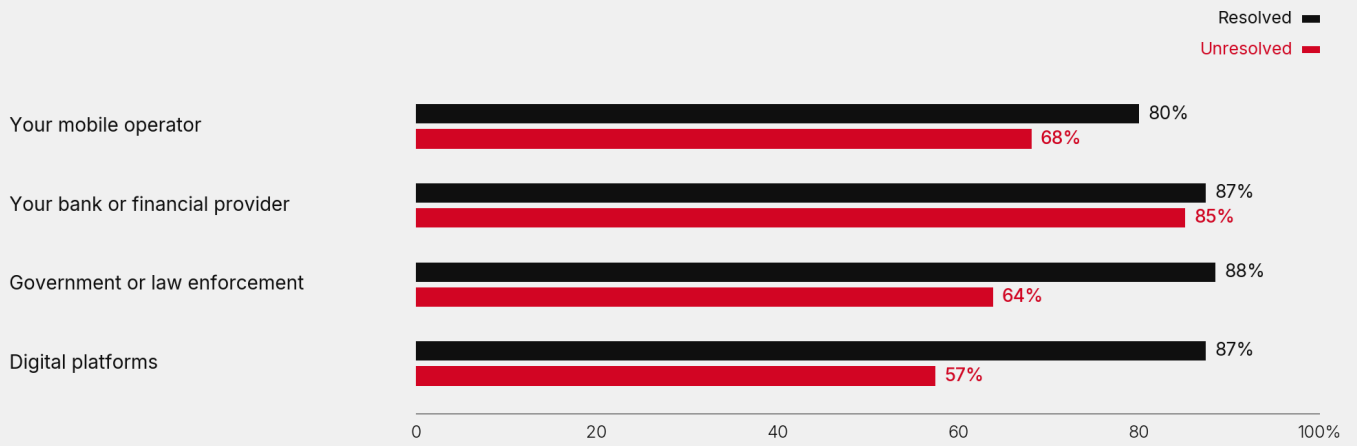
Among Indian victims whose case was resolved, 88% are comfortable with government holding their data, 87% with digital platforms, 87% with their bank and 80% with their mobile operator. Among victims whose case is unresolved, the figures are 64% for government, 57% for digital platforms, 85% for banks and 68% for mobile operators. These comparisons rest on 95 victims whose case was resolved and 47 whose case is unresolved.

Across ASEAN-6, comfort is similarly lower among unresolved victims for all four: government from 72% to 59%, digital platforms from 67% to 56%, banks from 85% to 70% and mobile operators from 74% to 62%. In India the gaps for government and digital platforms are larger than across ASEAN-6, the gap for banks is small, and the gap for mobile operators, 80% compared with 68%, is in line with ASEAN-6.

Figure 3

Permission to hold data, by case outcome

Percentage of Indian victims who reported a scam comfortable with each actor holding and using their data to detect fraud



Comfortable: 7 or above out of 10. Base: Indian victims who reported a scam, resolved n=95, unresolved n=47.

Source: GSMA Consumer Scam Survey 2026

03

Trust and the Room to Act



3

Trust and the Room to Act

Indian consumers place a high level of trust in the very channels scams arrive through. They rate SMS at 7.3 out of 10 for trustworthiness, compared with 5.7 across ASEAN-6 and 6.6 in Vietnam, the highest ASEAN market, and voice calls at 7.4, compared with 5.9 across ASEAN-6 and 6.5 in Thailand. They rate six of the seven channels in the study higher than any of the six ASEAN markets, and online shopping level with the Philippines at 7.4. Email scores 7.8, compared with 6.7 across ASEAN-6 and 7.2 in the Philippines, and messaging apps 7.5, compared with 6.1 across ASEAN-6 and 6.5 in Thailand.

Sixty-six percent are comfortable sharing personal data such as name, address and payment details with conversational apps, compared with 40% across ASEAN-6 and 50% in Indonesia, the highest ASEAN market. Thirty-three percent are very comfortable, compared with 7% across ASEAN-6 and 10% in Vietnam, and only 9% say they would never do it, compared with 15% across ASEAN-6 and 9% in Thailand, the lowest of the six ASEAN markets.

One of the strongest findings from the India survey is the level of consumer permission for institutions to use data for fraud prevention. Eighty-seven percent of respondents are comfortable with their bank or financial provider holding and using their data to detect fraud, compared with 79% across ASEAN-6 and 82% in Indonesia, the highest ASEAN market. Eighty-one percent say the same of their

mobile operator, compared with 69% across ASEAN-6 and 76% in Vietnam, 73% of digital platforms, compared with 60% across ASEAN-6 and 66% in Indonesia, and 82% of government, compared with 65% across ASEAN-6 and level with Vietnam, the highest ASEAN market.

Indian consumers do less to harden their own accounts and extend more permission to institutions.

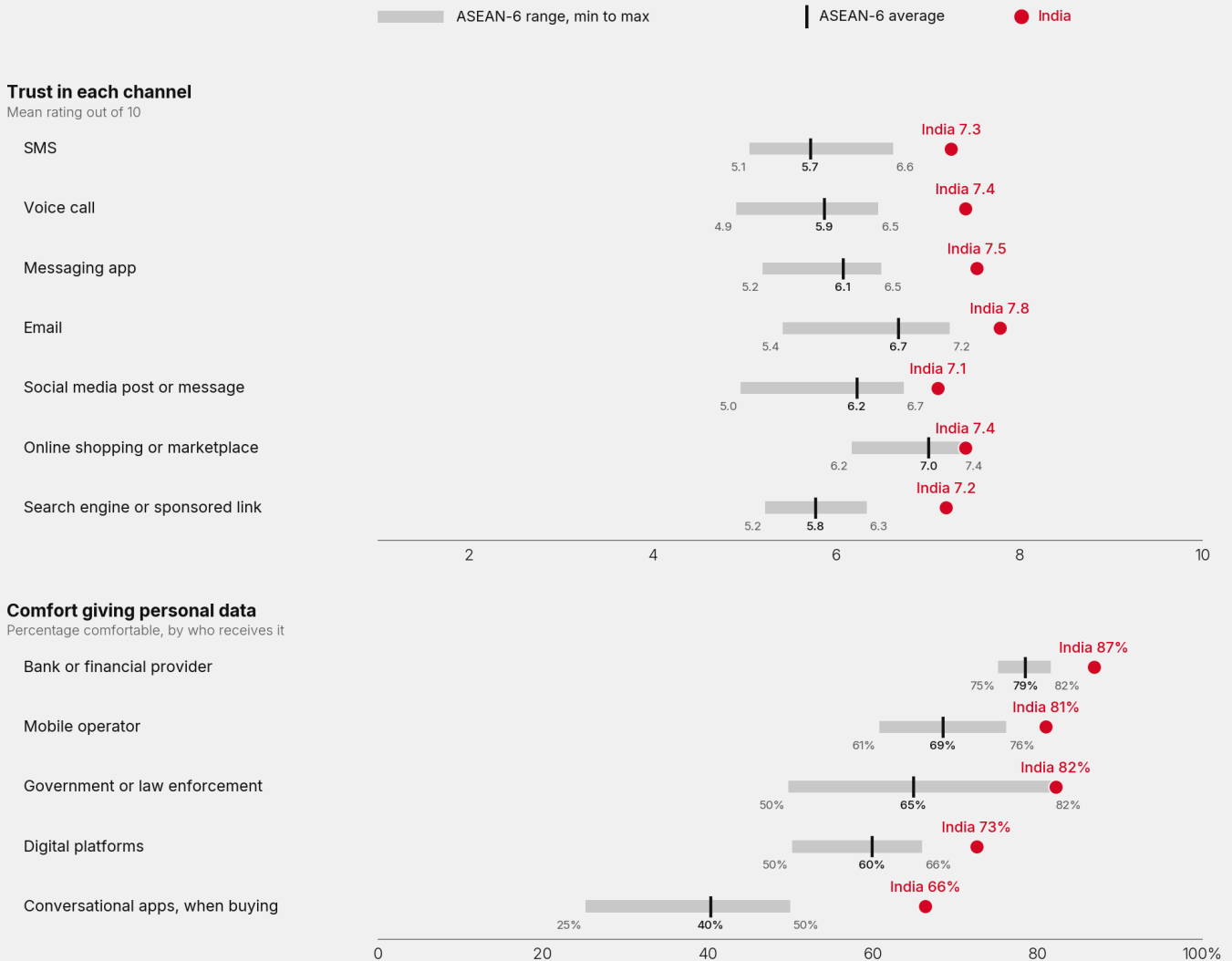
Some withdrawal is already visible. Sixty-one percent of Indian consumers avoid some form of inbound contact or online transaction because of scam concerns, compared with 56% across ASEAN-6, and 35% have changed or limited their contact details, including ignoring unknown calls and links, compared with 41%.

Consumer association of platforms with scams rose this year. Sixty percent of Indian consumers now associate Facebook with scams, up from 51% in 2025, and Instagram rose from 50% to 57%, with Telegram and WhatsApp close behind.

Figure 4

Trust and permission

All consumers, India against the ASEAN-6 range and average



Comfortable: bank, operator, government and platforms rated 7 or above out of 10 for holding and using data to detect fraud; conversational apps very or quite comfortable sharing personal data when buying.

Base: all consumers, n=500 per market. ASEAN-6 average is the equal-weighted average of Singapore, Malaysia, Thailand, Indonesia, the Philippines and Vietnam.

Source: GSMA Consumer Scam Survey 2026

Indian consumers also rate protection delivered highly. Sixty-five percent rate their mobile operator's protection 8 or above out of 10, compared with 49% across ASEAN-6 and 52% in Thailand, Indonesia and the Philippines, the highest of the six ASEAN markets. Financial services score 73%, compared with 64% across ASEAN-6 and 69% in the Philippines, device and software makers

70%, compared with 58% and 65% in Indonesia and the Philippines, internet providers 62%, compared with 50% and 56% in the Philippines, and digital platforms 56%, compared with 47% and 55% in the Philippines. Government scores 62%, compared with 43% across ASEAN-6 and level with Vietnam, the highest ASEAN market.

Consumers assign each actor a level of

responsibility for protecting them and separately rate how well it performs. The gap between the two is the shortfall that actor carries. Indian consumers do not expect less of operators: 74% assign them high responsibility, compared with 73% across ASEAN-6. The shortfall is narrow because delivery is rated higher. For Indian operators it is 9.2 percentage points, compared with 23.9 across ASEAN-6 and 15.0 in Thailand, the narrowest ASEAN market. For government it is 13.2 percentage points, compared with 28.0 across ASEAN-6.

What limits the next step is friction. Indian consumers rate the inconvenience and delay they

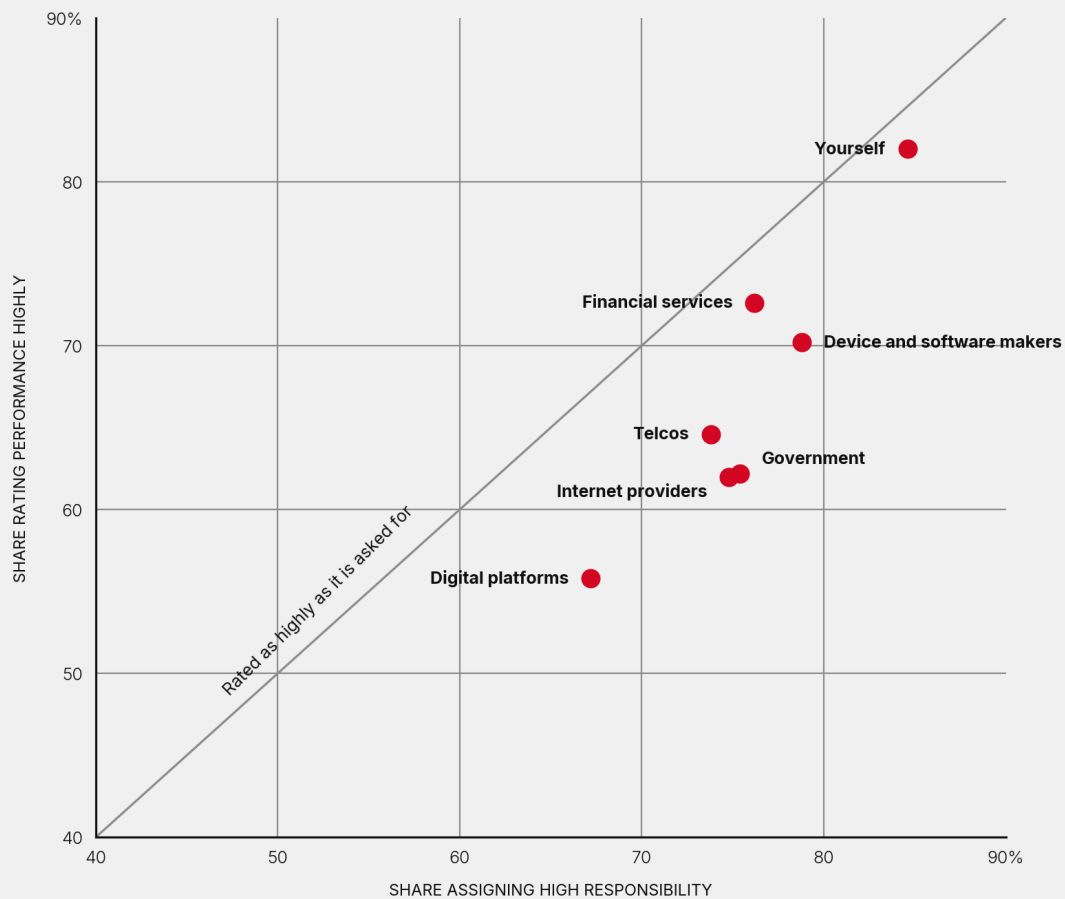
experience in online transactions at 6.4 out of 10, compared with 5.7 across ASEAN-6, and the most they would accept for stronger protection at 6.9, compared with 6.4. The gap between the two is narrow, and narrower than the 0.7 across ASEAN-6, in line with Vietnam, the lowest of the six ASEAN markets. Consumers are also split on where their own limit sits: 36% would accept more inconvenience than they have today, 28% about the same and 36% less. A check, hold or confirmation step applied to every transaction uses that narrow margin on every consumer, whether or not it stops a scam.



Figure 5

Responsibility versus performance

Percentage of Indian consumers rating each actor 8 or above out of 10



Indian consumers, n=500. The distance below the diagonal is the shortfall between responsibility assigned and performance rated.

Source: GSMA Consumer Scam Survey 2026

04

What the Ecosystem Can Do Next



4

What the Ecosystem Can Do Next

1. Improve what happens after the report. Indian consumers report only a narrow gap between the friction they already experience in online transactions and the most they say they would accept for stronger protection, pointing towards prioritising measures that improve resolution and recovery over adding checks or delays for every consumer. A third of reported cases still end unresolved and two thirds of consumers who lost money recover nothing. Sixty-four percent of Indian victims say the scam reached them through more than one channel, compared with 49% across ASEAN-6 and 54% in Vietnam, the highest ASEAN market, and victims already take a case to almost two organisations on average. India already connects police, banks, payment providers and operators around a reported case. Extending it to the cases it does not yet close would mean more reported cases resolved and more lost money returned.

An organisation took responsibility for 65% of reported cases, and taking responsibility for a case is not the same as investigating and closing it. The opportunity is to turn more of those cases into resolved ones, and to reach the 14% of victims who never take their case to any organisation.

2. Sustain digital trust alongside resolution.

Consumers whose case was resolved report higher comfort with institutions using their data than consumers whose case remains unresolved. Comfort with government holding data is 88%

among victims with a resolved case and 64% among those with an unresolved case, and for digital platforms 87% compared with 57%, wider differences than across ASEAN-6. These figures rest on 95 resolved and 47 unresolved cases.

The permission Indian consumers grant is available now. Eighty-seven percent are comfortable with their bank or financial provider holding data to detect fraud, 82% with government, 81% with their mobile operator and 73% with digital platforms. Indian consumers are more comfortable than consumers across ASEAN-6 with institutions holding and using their data to detect fraud, and comfort is highest among victims whose case was resolved.

3. Banks and financial providers: use the

permission they hold. Forty-one percent of Indian victims take their case to their bank or e-wallet provider, compared with 36% across ASEAN-6, and banks and financial providers resolved 25% of the cases they received, compared with 19%.

Eighty-seven percent of Indian consumers are comfortable with their bank holding and using their data to detect fraud, compared with 79% across ASEAN-6 and 82% in Indonesia, the highest ASEAN market, and that comfort is similar among victims whose case was resolved and victims whose case is unresolved, 87% compared with 85%. Reported fraud is routed to Indian banks so funds can be frozen. The next step is from holding funds to returning them, so more of the cases banks receive

end with money back.

4. Digital platforms: bring reports into the shared

coordination. Forty percent of Indian victims take their case to the platform where the scam happened, compared with 32% across ASEAN-6, and platforms resolved 17% of the cases they received, compared with 19%. Comfort with digital platforms holding data to detect fraud is 73%, the lowest of the four actors asked about in India, compared with 60% across ASEAN-6 and 66% in Indonesia, the highest ASEAN market. Among victims whose case is unresolved it is 57%, compared with 87% where the case was resolved. Platforms take part in India's fraud information sharing. Bringing the reports consumers make to a platform into that coordination would carry a case that starts on the platform through to the bank or payment provider holding the funds.

5. Government and police: measure and publish

outcomes. Forty-nine percent of Indian victims go to the police, compared with 36% across ASEAN-6, and government or the police resolved 32% of the cases taken to them, more than any other organisation. Eighty-two percent of Indian consumers are comfortable with government holding data to detect fraud, compared with 65% across ASEAN-6 and level with Vietnam, the highest ASEAN market. Among victims whose case is unresolved that comfort is 64%, compared with 88% where the case was resolved. Government publishes the money saved through reported complaints. Adding the share of reported cases resolved and of money returned would let the

resolution rate recorded here be tracked over time.

6. Mobile operators: build the digital trust layer.

Eighty-one percent of Indian consumers are comfortable with their mobile operator holding and using their data to detect fraud, compared with 69% across ASEAN-6. Operator protection is rated 8 or above out of 10 by 65%, compared with 49% across ASEAN-6, and 74% assign operators high responsibility for protecting them. Operators resolved 10% of the cases they received, compared with 16% across ASEAN-6, the one measure in this study where India sits below the region. Operators do not hold the funds, so closing that gap runs through the handover to the institution that does. Operators' contribution also goes beyond connectivity and reporting. Common, interoperable network capabilities, including those enabled through GSMA Open Gateway, can support stronger authentication and risk identification for financial institutions, digital platforms and other service providers. Greater coordination between operators, financial institutions, platforms and government could turn that permission into protection across digital services, while respecting privacy and avoiding unnecessary friction for consumers.

Indian consumers report, hand the case over and trust institutions to act, and more often than not institutions do. The opportunity is to keep that true: resolve more of what is reported, recover more of what is lost, and do it without adding friction consumers will not accept.

Consumer survey methodology

The insights in this annex are based on a cross-sectional online survey of adults (18 and above) in India, conducted alongside the six ASEAN markets in the GSMA Consumer Scam Study 2026. Fieldwork was conducted by Milieu Insight through self-administered online interviews in English between 29 July and 3 August 2026, with approximately 500 respondents in India. Respondents gave informed consent, and data were anonymised and handled in line with applicable data protection requirements. ASEAN-6 figures are equal-weighted across Singapore, Malaysia, Thailand, Indonesia, the Philippines and Vietnam (n=3,000) and exclude India. Comparisons between victims whose case was resolved and victims whose case is unresolved, the share of victims reached through more than one channel, and the share of cases each organisation received and resolved use the combined six-market base, as in the ASEAN report. The India figures on those measures are calculated on the Indian sample, 95 resolved and 47 unresolved cases. Where the highest or lowest ASEAN market is named, it is the ASEAN market or markets with the highest or lowest result on that measure. Victim impact, reporting and recovery metrics are calculated on victims only, respondents who have been scammed at any point: 165 in India, of whom 142 reported a case, 95 resolved and 47 unresolved. Comfort and trust measures on 1-to-10 scales report the share scoring 7 or above unless otherwise noted. Responsibility and performance ratings report the share scoring 8 or above. Percentages are rounded to whole numbers, so components may not sum precisely to their totals. Full technical details are available on request.

GSMA Head Office
1 Angel Lane
London
EC4R 3AB
United Kingdom