GSMA

ASEAN Consumer Scam Report 2026: Defences Rising, Cases Unresolved

ARMIDALE

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)

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, 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 three thousand consumers across ASEAN who answered, many of them recounting difficult experiences.

Data sources: This report draws on Armidale's 2024, 2025 and 2026 consumer fraud surveys (n≈500 per market) and associated qualitative insights gathered during analysis and industry consultations.

Contact the author: contact@armidale.co

Contents

Foreword 2

Executive Summary 3

1 What consumers are doing 6

1.1 The Scale of the Problem 7

1.2 Consumers Have Taken Action 10

1.3 Consumers Accept Their Share of Responsibility 14

2 What happens when they report 16

2.1 What Actually Happens to a Scam Case 17

2.2 The Cost of an Unresolved Case 21

3 What it costs the ecosystem 22

3.1 Ecosystem Trust and the Cost of Distrust 23

3.2 The Room for the Industry to Act 27

3.3 Country Snapshots 31

4 What to do next 34

4.1 What the Ecosystem Can Do Next 35

4.2 Conclusion and the Path Forward 38

Consumer survey methodology 39

Foreword

As ASEAN economies become more digital, trust is becoming central to the next phase of digital transformation. Citizens need to trust the digital services they use every day. Businesses need to trust the digital infrastructure on which they operate. Governments need confidence in the resilience, security and integrity of the systems on which digital economies increasingly depend.

Scams are therefore more than a consumer protection issue. They affect how we communicate, how we transact, how we respond to legitimate organisations and how willing we are to share the data needed to protect them. When trust is damaged, the impact extends well beyond the individual victim.

This report shows that consumers across ASEAN are not passive in the face of growing scam risks. They are aware of the threat, they are taking more steps to protect themselves, and many are changing their behaviour because of their own experience or the experience of people close to them. That progress matters.

But the report also points to a more difficult challenge. Consumer awareness and individual vigilance are necessary, but they are not enough. Too many reported cases remain unresolved, too many victims recover none of the money they lose, and the consequences extend beyond the original scam. When people report a scam and see no clear outcome, trust is weakened. That loss of trust affects communications channels, digital services, data sharing and confidence in the digital economy.

The next phase of anti-scam work must therefore focus not only on prevention, but also on resolution, recovery and coordination. Scams often move across channels, platforms, payment systems and institutions. No single organisation sees the whole case, and no single organisation can address the problem alone.

Mobile networks and services remain central to how people connect, access services and participate in the digital economy. Operators have an important role to play, alongside governments, financial institutions, digital platforms and technology providers. The priority now is to ensure that the ecosystem works together more effectively, with clearer reporting pathways, better information sharing, measurable outcomes and practical safeguards that improve consumer confidence without adding unnecessary friction.

ASEAN has made significant progress in digital transformation. Protecting consumers from scams and rebuilding trust when things go wrong must now be part of that agenda. The findings in this report are intended to support that discussion and help identify where further action is needed.

Julian Gorman

Head of Asia Pacific

GSMA

Executive Summary

82%

of victims who lose money recover none of it

45%

of reported cases are never resolved

41%

of consumers now ignore unknown calls and links

Multiple years of anti-scam campaigns have produced the response they asked for. Every protective behaviour we measure rose this year: more consumers strengthened their account security, more changed or limited their contact details, more installed security tools, and more warned the people around them. Victims are not in denial either: 84% accept at least partial responsibility for what happened to them, and 87% can point to the moment they clicked, shared or paid when they should not have.

What has not moved with them is the system they report into. Sixty-eight percent of scam victims lose money, and of those who do, 82% recover none of it. Only one in ten is made whole. Nearly half of all reported cases, 45%, are never resolved. Whether money comes back depends on where it went rather than who the victim contacted: unauthorised card charges are recovered far more often than any other kind of loss. Where the charge is genuinely unauthorised and the victim raises it with their financial institution, money comes back far more often than through any other route. No other route in the region comes close.

Scammers have moved accordingly, away from taking money and towards persuading consumers to send it, which is the hardest kind of payment to reverse. No single organisation sees a whole case, because scams run across channels and victims report to several organisations in turn. What is missing is a way for a case reported once to reach everyone who needs to act on it.

The cost of leaving these cases unresolved is compounding. This year's analysis shows that unresolved cases do not sit with the individual victim alone. Consumers whose cases remain unresolved report markedly lower willingness to trust communication channels and to share the very data the next generation of scam defences depends on. Victims whose cases were never resolved are far less trusting of SMS, less comfortable with conversational platforms, and less willing to let digital platforms hold their data than victims whose cases were closed. Consumers who have been scammed move accounts or switch providers at more than double the rate of consumers scams have never touched, 25% against 11%, and 41% of all consumers have changed or limited their contact details or now ignore unknown calls and links, putting a substantial share of the region beyond the reach of inbound contact. Every unresolved case quietly taxes the whole ecosystem. That withdrawal does not stay inside the scam economy. A consumer who has decided not to answer unknown numbers applies that decision to every unfamiliar caller, a bank verifying a transaction or a government

service reaching out included, whoever is on the other end and however legitimate the reason.

The path forward follows directly. Awareness and self-protection have taken consumers as far as they can go alone; the next gain comes from coordination of the reporting layer, measuring recovery rather than activity, and protecting the consumer consent that makes shared defences possible. This report sets out where that room to act exists, which actors hold it, and what each should do next.

GSMA ASEAN Consumer Scam Report 2026

Defences Rising, Cases Unresolved

Consumers across ASEAN have done what a decade of awareness campaigns asked of them. The system they report into has not moved with them, and the cost of leaving a case unresolved no longer falls on the victim alone.

Consumers have done what was asked

Every one of the eight protective behaviours measured rose this year. Concern is at its ceiling and there is almost nobody left to convert. Victims are not in denial either.

worry about being scammed or hacked	have changed their behaviour because of scams	have taken no protective action at all	of victims say they did something they should not have
96%	**66%**	**7%**	**87%**

The system has not reciprocated

The burden of escalation falls on the victim. Those whose losses still worry them report to 2.3 organisations against 1.5, and recover at much the same rate, 25% against 24%. The gap is structural, not a shortage of reporting.

of victims lose money	of those recover none of it	take the case to at least one organisation	of reported cases are still unresolved
68%	**82%**	**69%**	**45%**

An unresolved case taxes everyone

Victims whose cases go unresolved withdraw their trust, and the consent that shared fraud defences run on. The penalty lands on every actor, not only the one that failed.

trust SMS, case resolved vs unresolved	changed contact details or ignore unknown calls	switch provider, untouched vs victims	give data to conversational apps, two years ago vs now
52 vs 32	**41%**	**11 vs 25**	**53 vs 40**

The room to act is narrow and unevenly held

Friction

0.7 out of 10

of a point spare between the friction consumers live with, 5.7, and the most they would accept, 6.4

Credibility shortfall, points

Device makers	17
Financial services	18
Internet providers	21
Telcos	24
Digital platforms	24
Government	28

between what is asked of each actor and what it is credited with

Permission to hold data

Financial services	**79**
Mobile operators	69
Government	65
Digital platforms	60

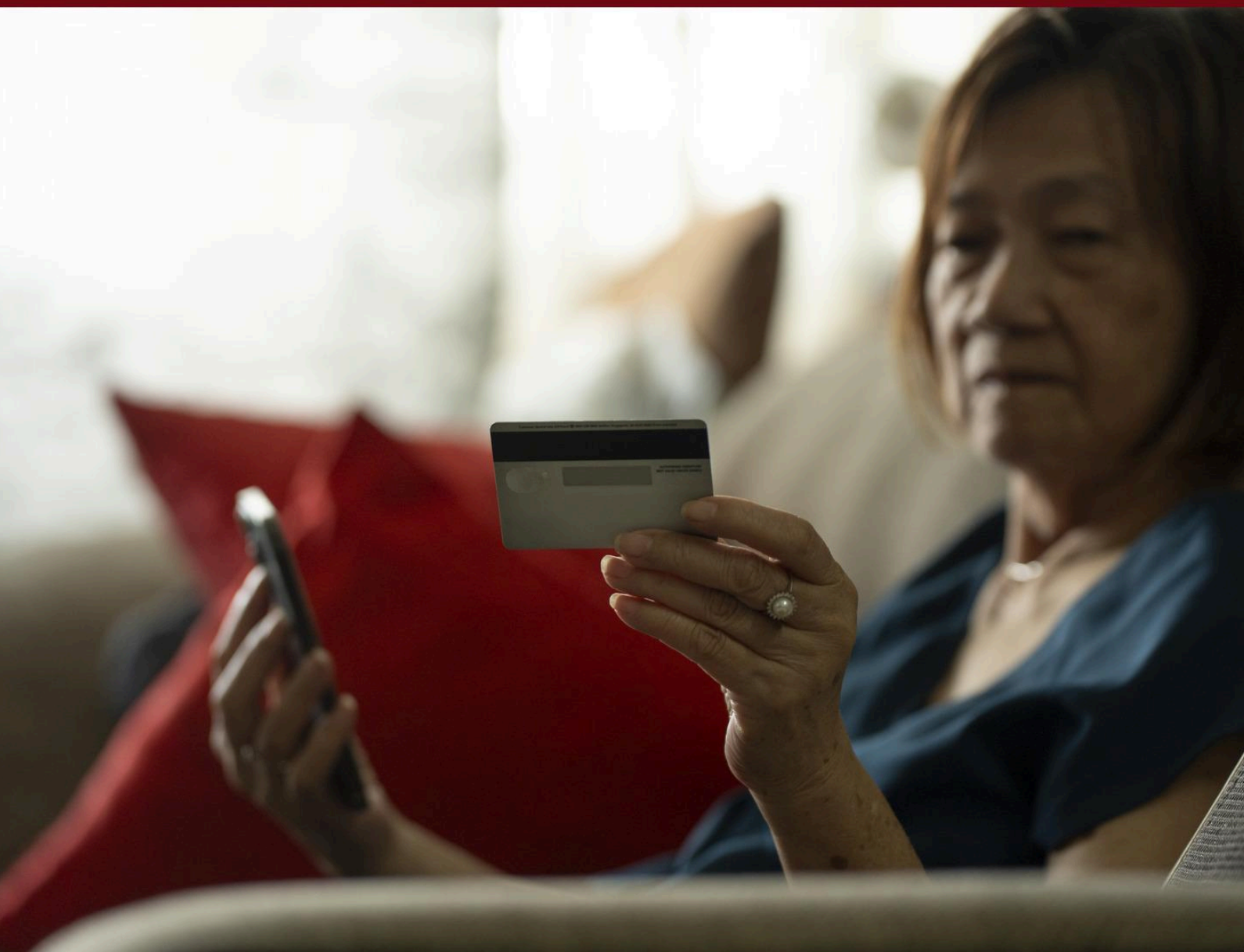
Banks and operators hold it, the state less so. Consent varies 7 points for banks, 32 for government.

What the ecosystem can do next

1. **Coordinate reporting**
   One case, one reference, visible to whoever must act.
2. **Certify outcomes**
   Certification earned on cases actually resolved, not programmes described.
3. **Financial services**
   Extend recovery beyond the card reversal, while money is traceable.
4. **Operators**
   Attack impersonation on voice and SMS; share scam signals with banks.
5. **Platforms**
   Most exposure, least permission. Verification, takedown, shared cases.
6. **Government**
   Measure and publish resolution. Anchor data sharing commercially.

01

What consumers are doing



1.1

The Scale of the Problem

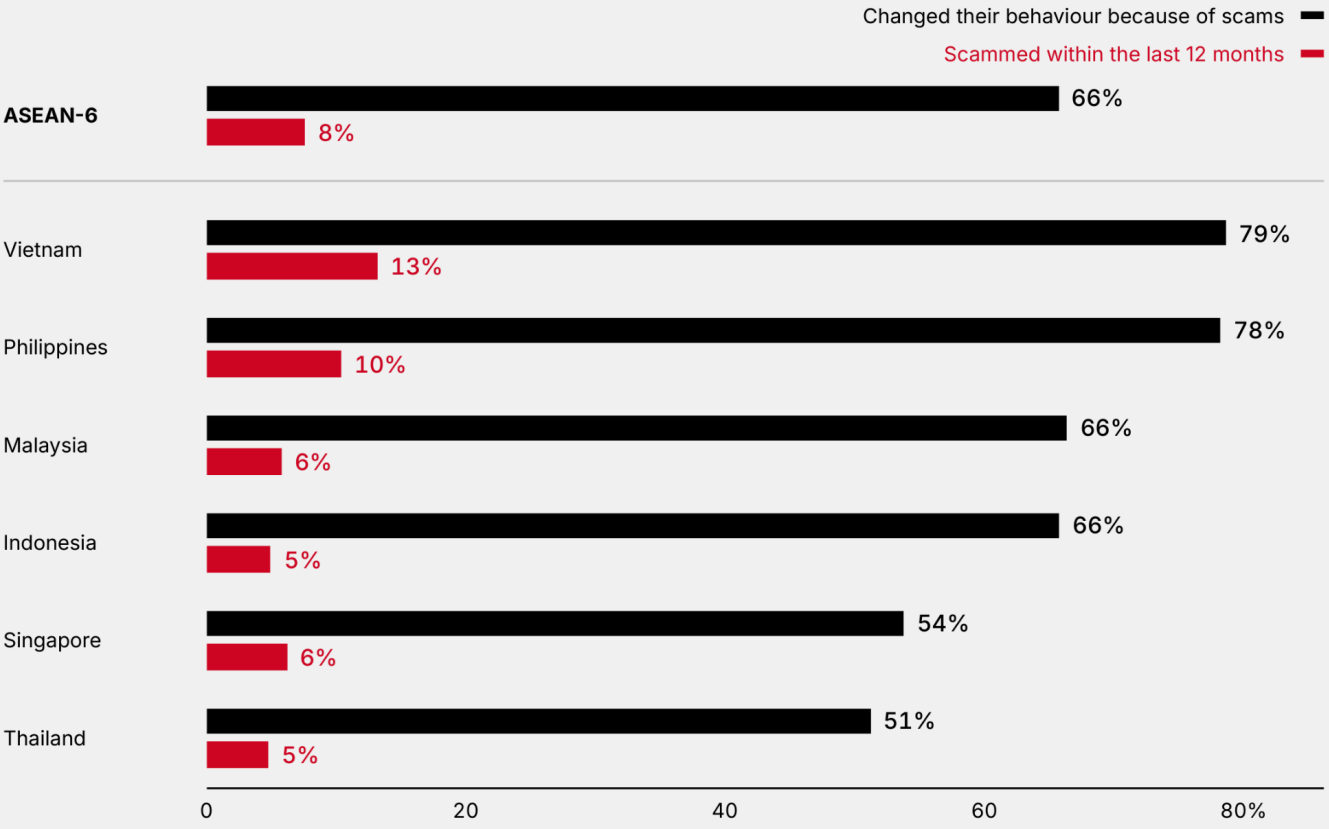
Recent victimisation remains steady. Eight percent of ASEAN consumers report being scammed within the last twelve months, unchanged from 2025. This year, however, the regional range has widened: 5% in Thailand (down from 8% in 2025) and Indonesia (down from 7%) rising to 13% in Vietnam (up from 11%), where recent victimisation runs at well over one and a half times the regional rate.

The footprint of scams, however, extends far beyond the people directly defrauded. Forty percent of consumers have not been scammed themselves but have watched someone close to them, a family member, friend or colleague, be scammed, and say it changed how they behave. Sixty-six percent of ASEAN consumers have changed their behaviour because of scams, through their own experience or someone else's. Two-thirds of the region's consumers now carry the behavioural cost of fraud, a market-wide effect no victim count captures.

Figure 1

How scams touch ASEAN consumers

Percentage of consumers



Source: GSMA Consumer Scam Survey 2026

Concern has nowhere left to rise. Ninety-six percent of consumers worry about being scammed or hacked, flat on 2025; 59% say they absolutely worry; and 82% believe the risks are increasing. Anxiety is effectively at its ceiling. Consumers have heard the messages and are aware of the problem, so there is little room left to move by raising concern further. Worry is not evenly spread. Sixty-two percent of women say they absolutely worry about being scammed, against 55% of men, and that gap was the same size last year. It does not track exposure: women and men are scammed at almost the same rate, 8% and 7% within the last twelve months.

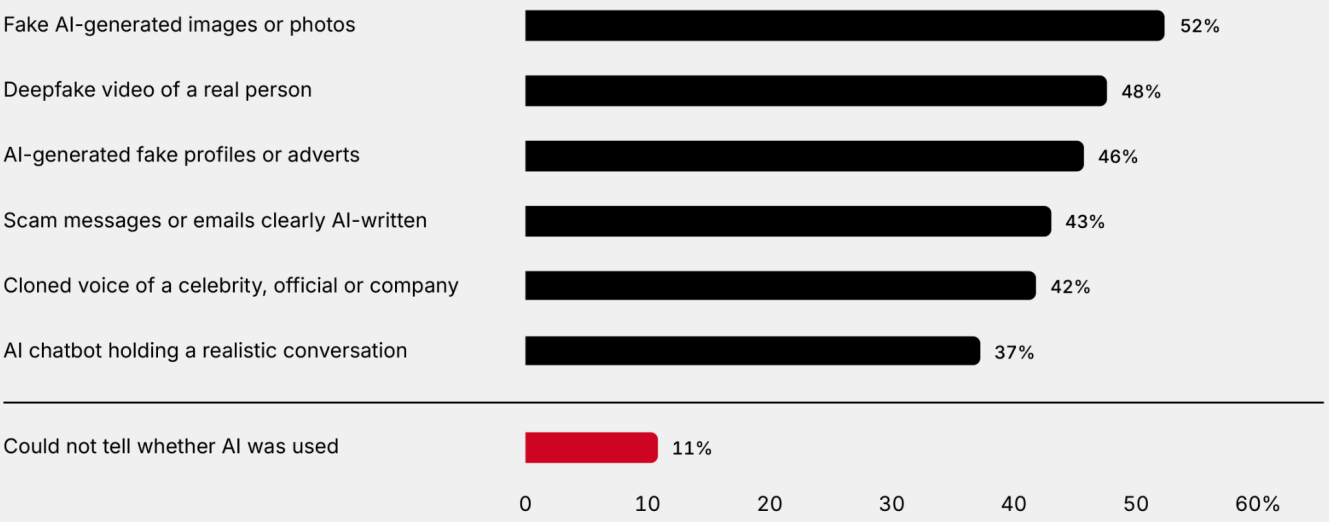
Artificial intelligence is now the operating environment rather than an emerging threat. Eighty-nine percent of respondents say that they have seen AI used in scams. The remaining 11% could not tell whether AI was involved in the scams they met. Fake AI-generated images were recognised by 52%, deepfake video by 48%, fake AI profiles and adverts by 46%, AI-written messaging by 43%, cloned voices of celebrities or officials by 42%, and AI chatbots holding a realistic conversation by 37%. Recognition runs highest in Vietnam, at 95%, the same market carrying the region's highest recent victimisation. No single technique dominates. All six run between 37% and

52%, which shows how far AI has saturated the market. AI is not a specialist trick confined to one kind of scam; it runs through every format consumers meet.

Figure 2

The AI tactics consumers recognise

Percentage of consumers



Source: GSMA Consumer Scam Survey 2026

1.2

Consumers Have Taken Action

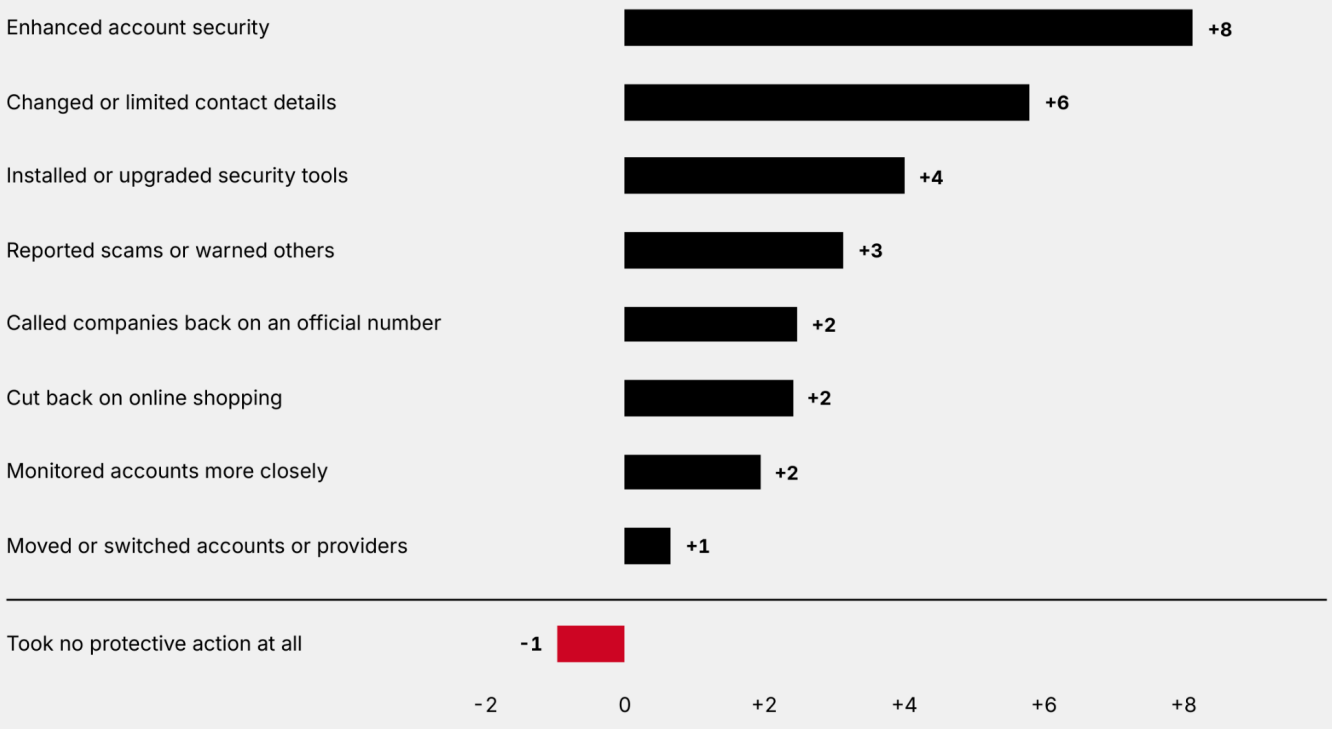
Consumers have not waited for the system to improve and have changed their own behaviours to increase personal defence against scams.

Every one of the eight protective behaviours tracked rose this year. Enhanced account security, the most common action, climbed from 50% to 58% of all consumers. Changing or limiting contact details rose from 35% to 41%, installing or upgrading security tools from 27% to 31%, and reporting scams or warning others from 31% to 34%. Monitoring accounts, the second most common action at 46%, cutting back on online shopping, and calling companies back on official numbers all edged upward. The share of consumers who took no protective action at all fell slightly from 8% to 7%. These changes clearly show that the population has absorbed the awareness messaging.

Figure 3

How far each protective behaviour moved

Change in percentage points, 2025 to 2026



Source: GSMA Consumer Scam Survey 2026

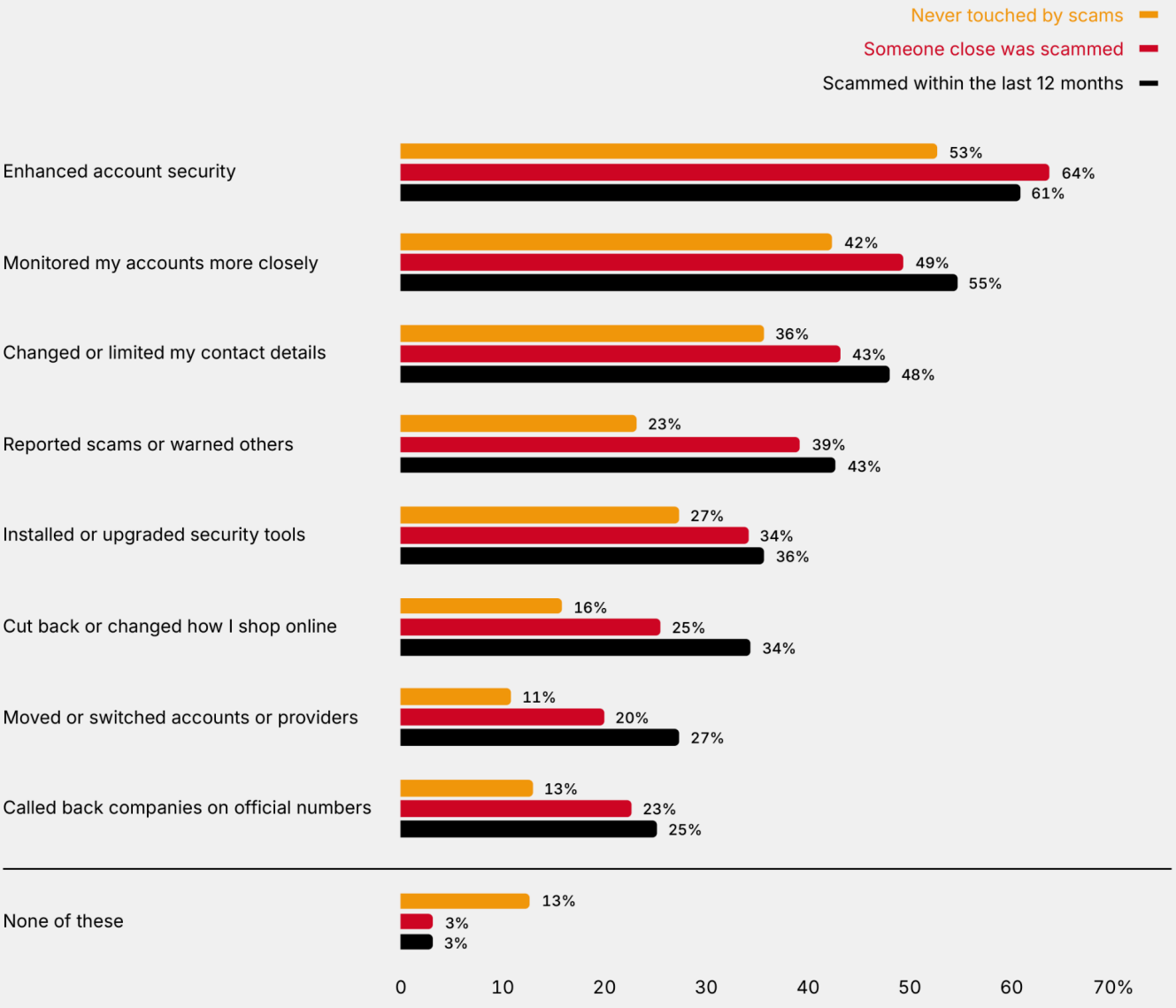
Being scammed changes what a person does. Across the eight protective actions we track, recent victims sit above consumers scams have never touched on every one. The largest shifts are in warning others, up from 23% to 43%, cutting back on online shopping, from 16% to 34%, and moving accounts or switching provider, from 11% to 27%. The share who have taken no protective action at all falls from 13% to 3%. A scam does not only cost a victim money. It changes how they deal with every provider they have.

Most of that change reaches the people they tell. Forty-six percent of victims warn friends, family or a partner, and consumers who have watched someone close to them be scammed pick up about 80% of the victim's shift on warning others, on calling companies back through official numbers, and on installing security tools. They are just as likely to have taken some action at all. Where the transfer weakens is on the responses that cost something: cutting back on online shopping and switching provider both carry across at about half strength. Vigilance travels through a network almost intact, and withdrawal at about half strength. The impact of fraud is amplified to reach two-thirds of the population.

Figure 4

Protective behaviour by experience of scams

Percentage of cohort



Source: GSMA Consumer Scam Survey 2026

What does not spread is the level of organisational distrust. The close-contact group rates institutions almost exactly as the untouched do: they score telco protection at 7.2 out of 10, against 7.3 among the unaffected, while recent victims drop to 6.6.

Being scammed erodes trust in every actor measured, financial services, platforms, telcos, device makers, internet providers and government alike, and no single actor is damaged more than the rest. Victims even mark down their own competence: their self-rating falls alongside their rating of every institution. This data points clearly to the fact that behaviour is contagious; distrust is not. Protective habits travel through families and

workplaces ahead of any campaign. The loss of trust does not travel, but where it does land it lands on the whole ecosystem at once rather than on any single actor within it.

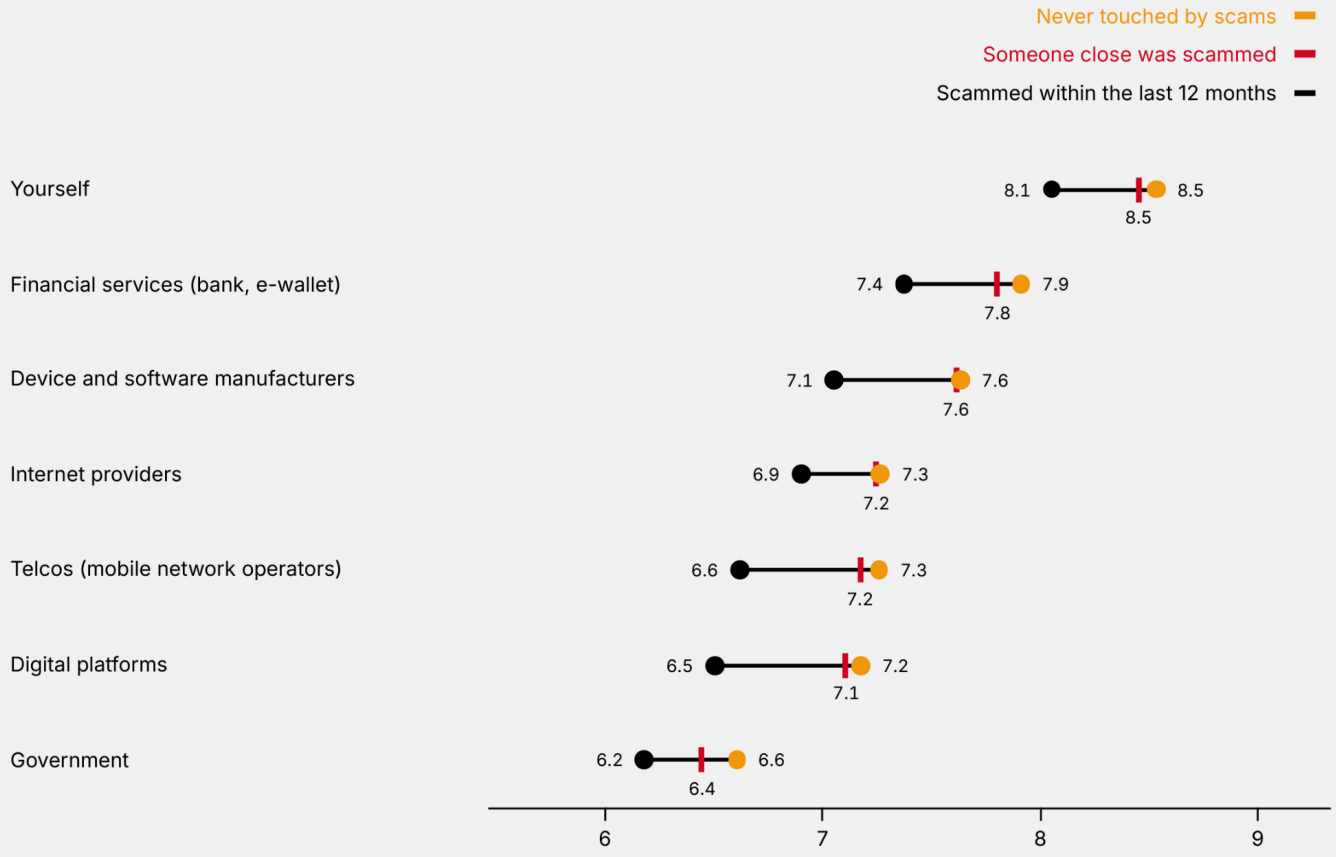
Awareness programmes have wide reach: between 65% and 80% of consumers know that their telco, their financial institutions or their government runs anti-scam education, depending on the actor. Protective behaviour has risen alongside that reach, and it has risen among people the scams never hit. Awareness and self-protection are no longer confined to those who learned the hard way.

Concern is already at its ceiling, and only 7% of consumers have taken no protective action at all. Awareness has reached most of the people it can reach on its own. What this wave adds is a measure of what happens after the consumer has acted.

Figure 5

Trust by experience of scams

Mean protection rating



Source: GSMA Consumer Scam Survey 2026

1.3

Consumers Accept Their Share of Responsibility

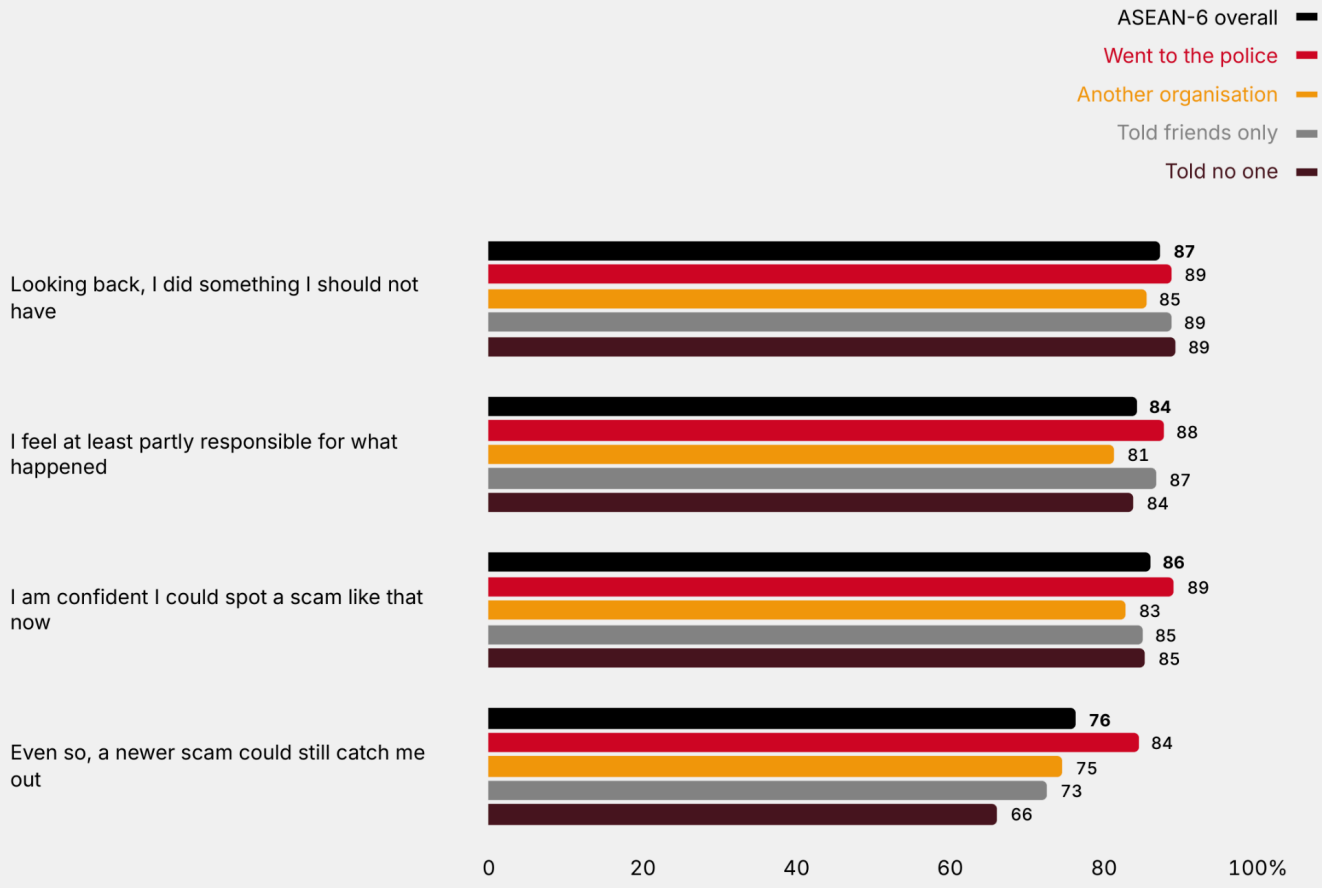
Consumers are clearly taking responsibility and accountability for their own actions when it comes to scams.

Eighty-seven percent of victims agree they did something they should not have, clicking, sharing or paying when they should not, and 84% feel at least partly responsible for what happened. The respondents also report learning and continued vigilance with 86% confident they could spot a similar scam now, and 76% accepting that a newer or more convincing scam could still catch them out. Victims hold a clear-eyed view of their own role.

Figure 6

Victims on their own role

Percentage of victims who agree



Source: GSMA Consumer Scam Survey 2026

The flip side of that self-reliance is overconfidence. Consumers rate their own protection higher than any institution's: 77% score themselves 8 or above out of 10, against 49% for telcos and 43% for government, and they assign themselves as much responsibility for staying safe as they assign their financial institution. That confidence is precisely what social engineering exploits. One further pattern sharpens the point: the victims who never reported their scam to anyone are the least likely to accept that a newer scam could catch them out, while those who went to the police are the most likely. Silence travels with overconfidence. The survey cannot settle which way that runs. Reporting may temper confidence, or the less confident may simply be more likely to report. The same gap appears at the point of reporting. Sixty-seven percent of women who are scammed take the case to an organisation, against 73% of men, and 18% of women tell no one at all against 15% of men. Once a case is reported the difference disappears: recovery is identical at 25% for both. The gap is in getting into the system, not in what happens inside it.

02

What happens when they report

2.1

What Actually Happens to a Scam Case

Despite consumers' awareness and efforts having increased, reporting effectiveness and resolution have not.

Sixty-eight percent of victims lose money when scammed, and most then go looking for help. Sixty-nine percent report their case to an organisation, and the victims who do report take it to nearly two organisations on average. Where they go is spread across the chain rather than concentrated with any one channel: 36% to a financial institution, 36% to the police, 32% to a digital platform, and 19% to their telco. With seven in ten victims reporting scams, the bottleneck is no longer in the consumer's hands.

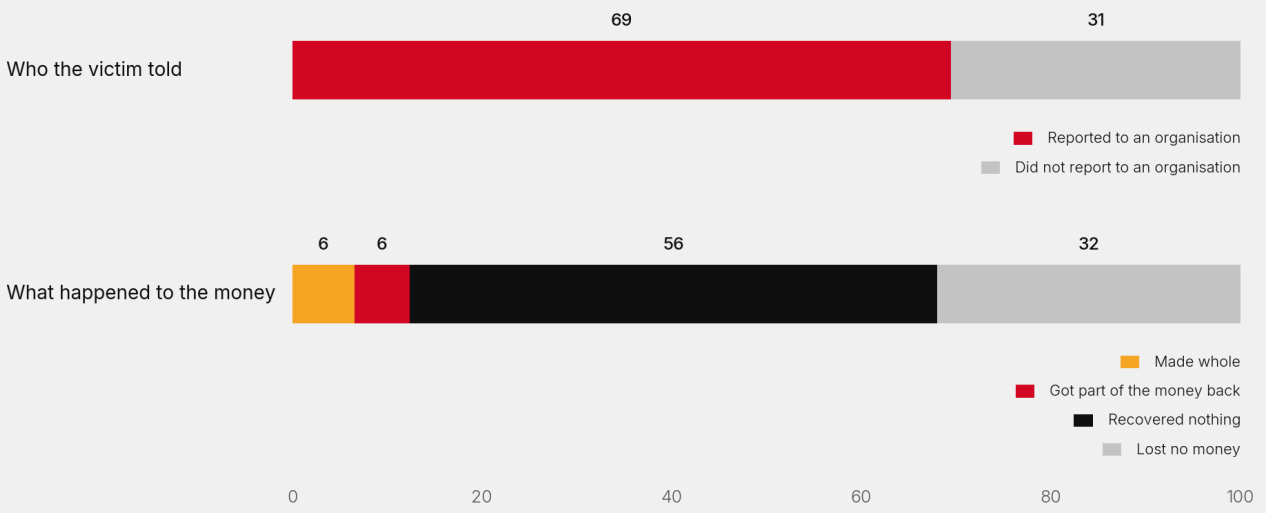
Financial recovery is, however, most often unsuccessful. Among victims who lost money, 82% recovered none of it. Ten percent were made whole and a further 8% got part of their money back.

Money is not the only unresolved harm: half of victims cite emotional distress as a major impact of the scam, 39% cite the time and effort of trying to resolve it, and 38% carry ongoing anxiety or a loss of confidence. An unresolved case keeps impacting its victims long after the scammer has moved on.

Figure 7

The outcomes funnel

Per 100 victims



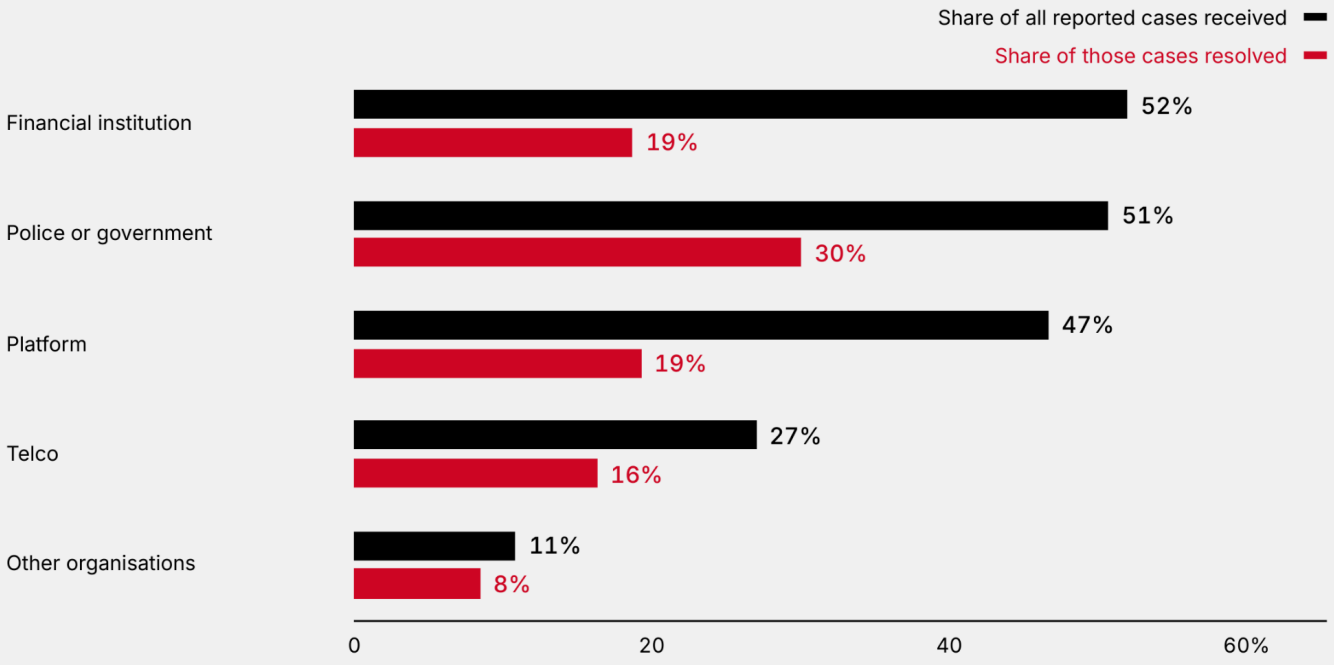
Source: GSMA Consumer Scam Survey 2026

Forty-five percent of reported cases are never resolved, and the shortfall runs across every actor. Thirty percent of victims who go to the police credit the police with resolving their case, against 19% each for financial institutions and platforms, and 16% for telcos. Half of all reported cases reach a financial institution, level with the police, and fewer than one in five of those victims credit the institution with resolving it. According to consumers, no organisation is credited with resolving even a third of what reaches it.

Figure 8

Cases received and cases resolved, by organisation

Percentage



Source: GSMA Consumer Scam Survey 2026

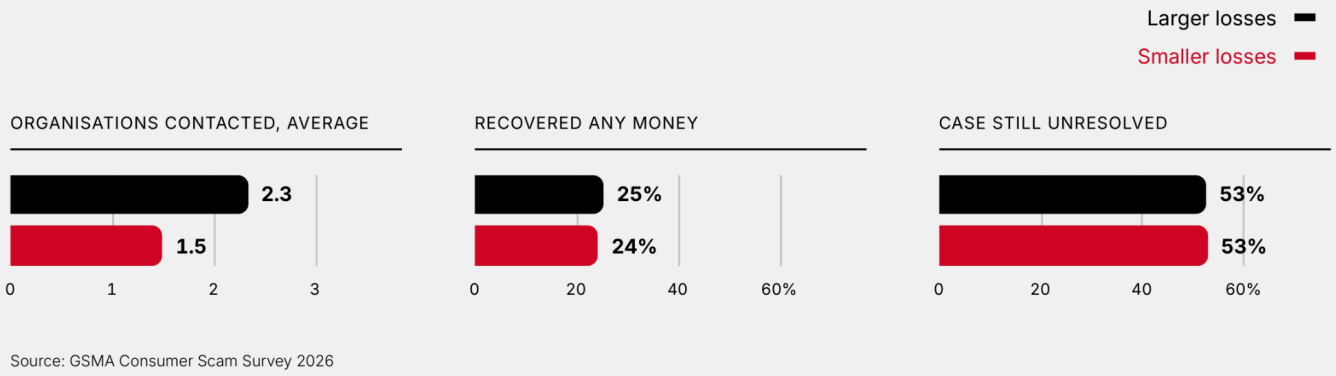
The burden of escalation falls on the victim. Victims whose losses still worry them today report to 2.3 organisations on average, against 1.5 for those whose losses do not, and among those who reported, recovery differs little, 25% against 24%.

Reaching the organisation that can act is left to the victim's own persistence, which points to a structural gap rather than a problem of under-reporting.

Figure 9

Escalation without recovery

Percentage and count



Source: GSMA Consumer Scam Survey 2026

One part of the system reliably works. Where a charge is genuinely unauthorised and the victim raises it with their financial institution, money comes back far more often than through any other route. Card is the only route in the region that delivers that. The advantage is widest on smaller losses and narrows as the amounts grow.

What limits it is reach, not the mechanism. More than a third of card-charge victims never take the case to their financial institution. Most describe a scam that also involved another type, where the payment was authorised and no reversal right applies. The card system does what it was built to do. The region's problem is how few of its losses now arrive as unauthorised charges.

Scams are moving away from card channels. The fastest-growing types are the ones where the victim is persuaded to send the money: investment and crypto, online shopping, and job scams each rose three to four points. The types where money is taken rather than given fell, including account takeover and QR or payment-link scams. Consumers have made themselves harder to steal from, so scammers have shifted to persuading them to pay. An authorised payment is the hardest of all to reverse, and a system built to reverse small unauthorised charges is aimed at where the harm used to be. Thirty-five percent of victims lose enough money that it still worries them today.

2.2

The Cost of an Unresolved Case

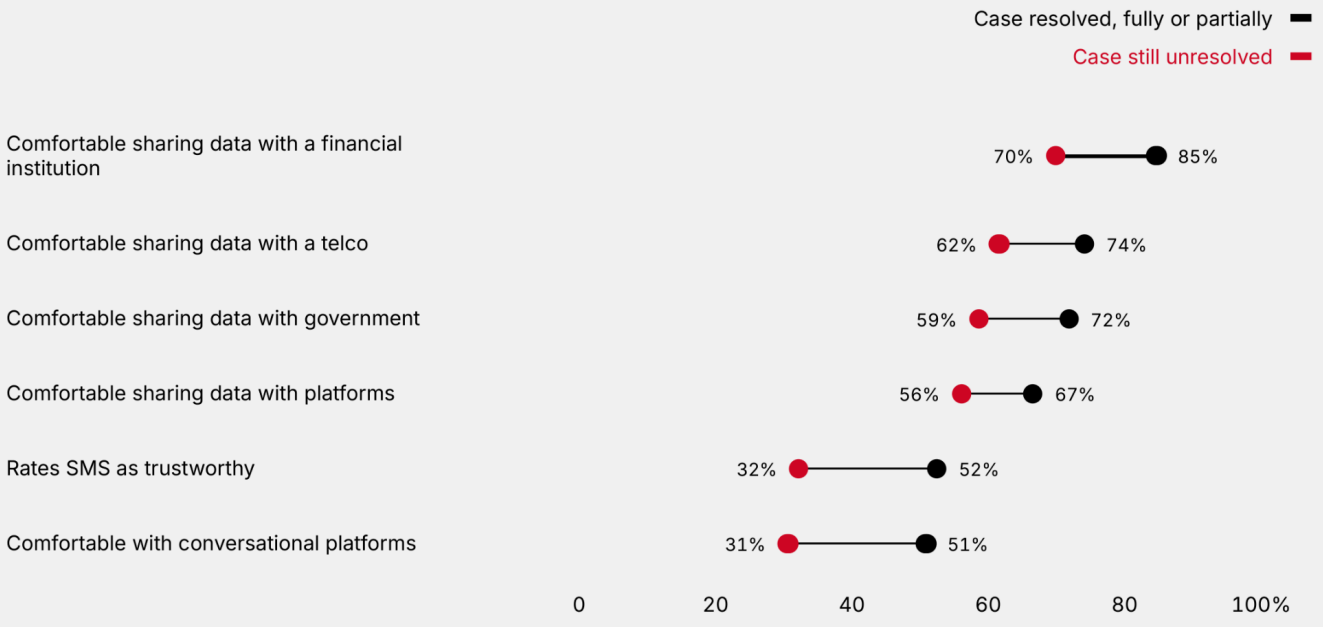
An unresolved case does not end when the victim gives up. Consumers left without a resolution differ, measurably, in what they are willing to do next.

Among victims who reported their case, those left unresolved trust less and are less willing to share. Fifty-two percent of victims whose case was resolved rate SMS as trustworthy, against 32% of those whose case is still open. The gap repeats on comfort giving personal data to conversational platforms, and again on willingness to let digital platforms hold data to detect fraud. The pattern is consistent across every measure. Where cases go unresolved, trust in the channel and consent to share data are both lower, and those are the two things shared fraud defences depend on.

Figure 10

What an unresolved case costs next

Percentage of victims who reported



Source: GSMA Consumer Scam Survey 2026

Across all ASEAN consumers, comfort giving personal data to conversational platforms sits at 40%, where it fell from 53% two years ago and has stayed. Two years on, it has not recovered.

03

What it costs the ecosystem

3.1

Ecosystem Trust and the Cost of Distrust

Fraud imposes an additional cost, one that falls on business rather than on victims. Consumers have defended themselves in part by becoming harder to reach.

Forty-one percent of ASEAN consumers have changed or limited their contact details, which includes ignoring unknown calls and links. Nineteen percent will re-engage only through a number they have dialled themselves. Counting those alongside consumers who have cut back on online transactions, and netting off the overlap, 56% avoid inbound contact or transactions because of scam concerns. A substantial share of ASEAN consumers can no longer be reached by inbound contact, no matter who is calling and however legitimate the reason.

That withdrawal rises with each additional AI technique a consumer recognises. Among consumers who recognised one technique in the scams they met, 28% ignore unknown calls and links. At two it is 34%, at three 44%, at four 51%, and at five or more, 58%. It is also worth noting that it is not victims who are driving this pattern. Among consumers who have never been scammed the numbers are almost identical, matching the full population to within a point at every step and identical at the first.

Recognition of more AI techniques and greater wariness towards inbound contact travel together. That wariness is paid for by the legitimate caller rather than by the scammer. In a market saturated with AI, consumers increasingly trust only what they initiate themselves.

The cost falls hardest on the channels operators own, and it is getting worse. SMS fell from second place to last of the seven channels consumers rate, in a single year.

Online commerce carries its own share, and it is growing. Twenty-three percent of consumers have cut back or changed how they shop online because of scam concerns, up from 20% last year. The pullback is heaviest where the harm landed: 44% of victims of an online-shopping scam have cut back, against 22% of victims of every other scam type. Most of the loss does not come from victims at all, though. Two-thirds of those who have pulled back have never been scammed themselves. They are reacting to what happened to someone else.

Two things separate this from the other costs of distrust. It does not track resolution: 34% of victims whose case was closed have cut back, against 32% whose case is still open. And it is not a judgement about the channel. Consumers who have cut back still rate online shopping 6.9 out of 10 for trustworthiness, against 7.1 among those who have not. They have not decided online shopping is untrustworthy. They are using it less anyway.

Churn follows the same pattern. Moving accounts or switching providers because of scam concerns in the past twelve months runs at 11% among

consumers untouched by scams, 20% among those who know a victim, and 25% among consumers who have been scammed at any point. Those close to victims churn at nearly the rate victims do, and at more than double the rate of consumers scams have not touched. Behaviour spreads through personal networks, so the churn cost of fraud reaches far beyond the people actually defrauded.

That distrust is not spread evenly. Consumers hold the entire chain responsible for protecting them but differentiate on who they believe is delivering.

Asked how much responsibility each of seven actors should take, consumers assign high responsibility to all of them: each actor is rated 8 or above by between 71% and 82%. Responsibility does not sit with any single one. Consumers include themselves among those they hold accountable.

Performance is where opinion divides. Across the six institutions, the share rating their protection highly spans 21 points, from 43% for government to 64% for financial services.

That spread widens as consumers see more AI, and it does not widen evenly. Among consumers who recognised one AI technique, 44% rated government protection highly; among those who recognised five or more, 38% did. Telcos fall from 54% to 48% across the same range, internet providers from 54% to 46%, device makers from 62% to 55%, and platforms from 50% to 46%. Financial services barely move, from 65% to 64%. The one actor whose standing survives contact with AI is the one already holding the region's deepest and most uniform permission to act.

Consumers' view of themselves moves the other way. The share rating their own protection highly rises from 76% to 80% across the same range. The movement is selective rather than general: consumers who recognise more AI mark down their protectors and mark up themselves, widening the gap between the two from 32 points to 41. Consumers who recognise more AI do not feel less safe, and overconfidence travels with silence.

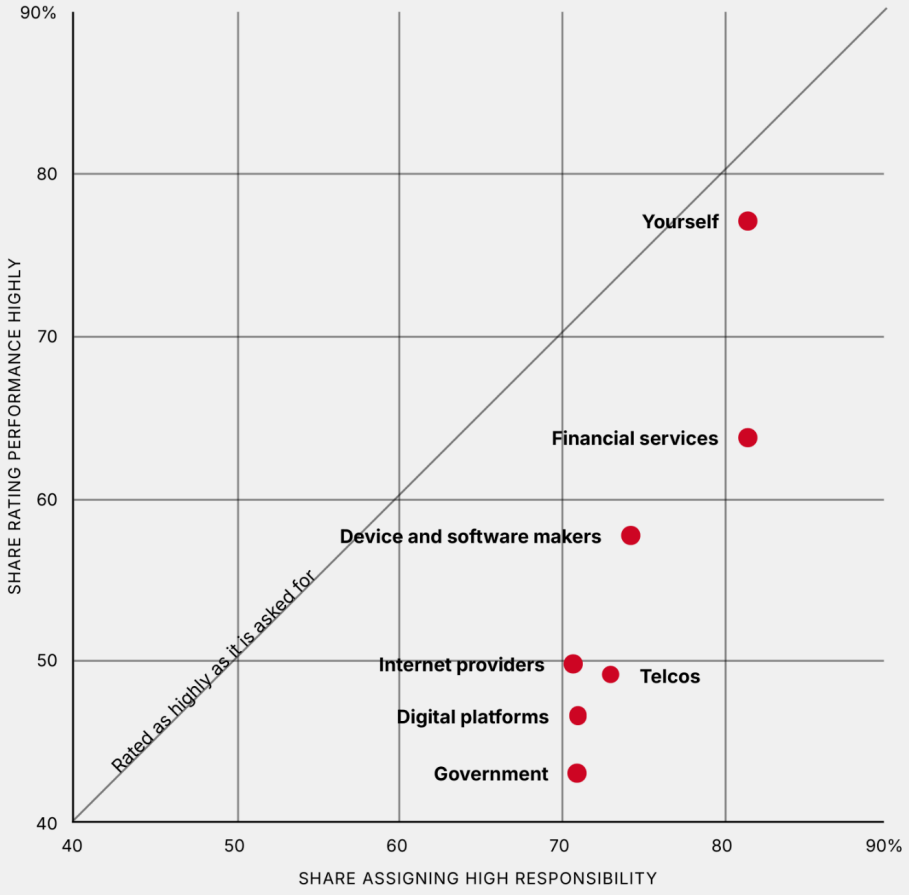
Telcos sit mid-field, alongside platforms and internet providers, neither leaders nor laggards. Government is the outlier at both ends. It carries the widest gap between what is expected of it and how it is rated, at 28 points against 24 for telcos and 18 for financial services. It also draws the widest split of any actor on responsibility: 71% give government high responsibility for stopping scams while 16% place it at the midpoint or below. That split is concentrated in Thailand and Indonesia, where close to 30% place government at the midpoint or below against roughly one in ten elsewhere. A response that leans on the state therefore begins from a contested mandate, and one contested in particular markets rather than across the region.

Consumer expectation of operators has moved. In last year's wave, fewer consumers named telcos as the actor responsible for stopping scams than named financial services, government or platforms. This year telcos sit inside the consensus rather than outside it, carrying high responsibility from 73% of consumers, within nine points of financial services and ahead of platforms and internet providers. The same movement shows on delivery: operators have climbed above platforms on how well consumers think each actor protects them, having sat below them a year ago. Operators are now held close to the standard applied to financial services, on channels that carry less of the scam traffic than messaging apps or social media, and on the one channel that has fallen furthest in standing.

Figure 11

Responsibility versus performance

Percentage



Source: GSMA Consumer Scam Survey 2026

No single channel carries the problem. Messaging apps are involved in 41% of victims' scams, social media in 36%, voice calls in 35% and SMS in 30%, with marketplaces, email and pop-ups behind them. Scams rarely stay on one channel either: 49% of victims report more than one. A scam is a route across channels rather than an event on one of them, which means no single organisation ever sees the whole case.

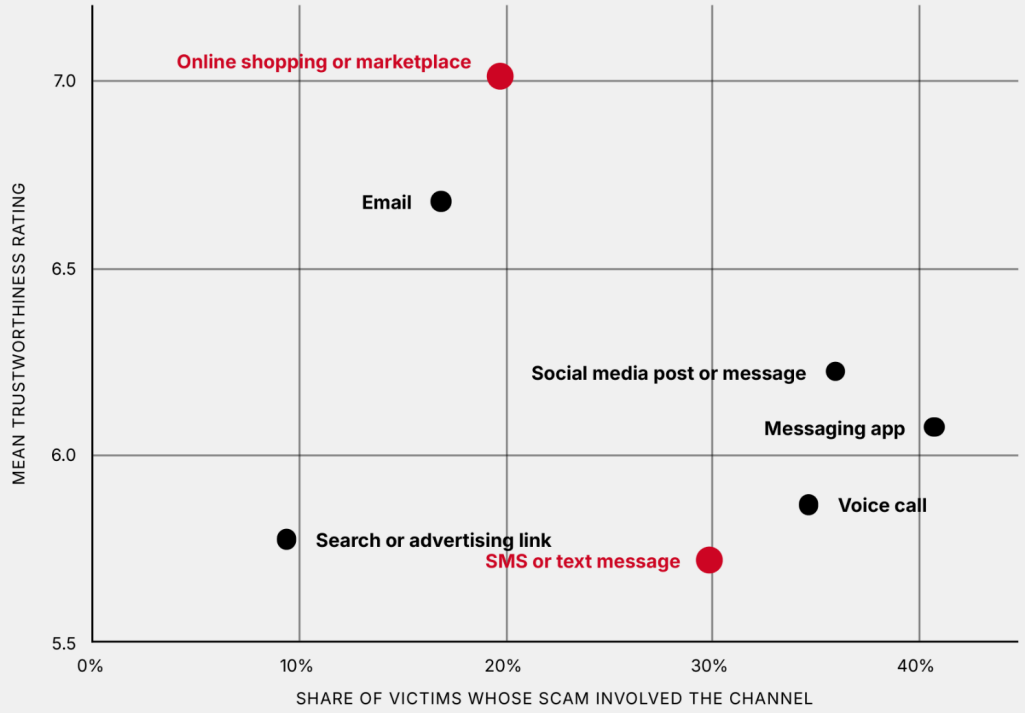
Perception of channels does not track experience. Consumers rate SMS lowest of the seven channels they use at 5.7, search and advertising links next at 5.8, and voice at 5.9, while online shopping is rated the most trustworthy at 7.0. Neither rating follows where scams arrive. Messaging apps are involved in more scams than any other channel, at 41%, and sit mid-table on trust at 6.1, while search and advertising links carry the fewest at 9%. The gap is widening rather than closing: online shopping extended its lead as the most trusted channel over the past year, while SMS fell to last. Channel trust, in short, does not track where scams actually arrive.

Consumer blame of platforms rose across the board this year. Sixty-seven percent now associate Facebook with scams, up from 61%; Telegram rose from 43% to 51%; WhatsApp, TikTok, Instagram and LINE all recorded similar increases. Perception is catching up with where scams travel, but slowly, and unevenly.

Figure 12

Trusted channels versus actual scam routes

Rating and percentage



Source: GSMA Consumer Scam Survey 2026

3.2

The Room for the Industry to Act

Three constraints define what interventions are feasible: friction, credibility and permission.

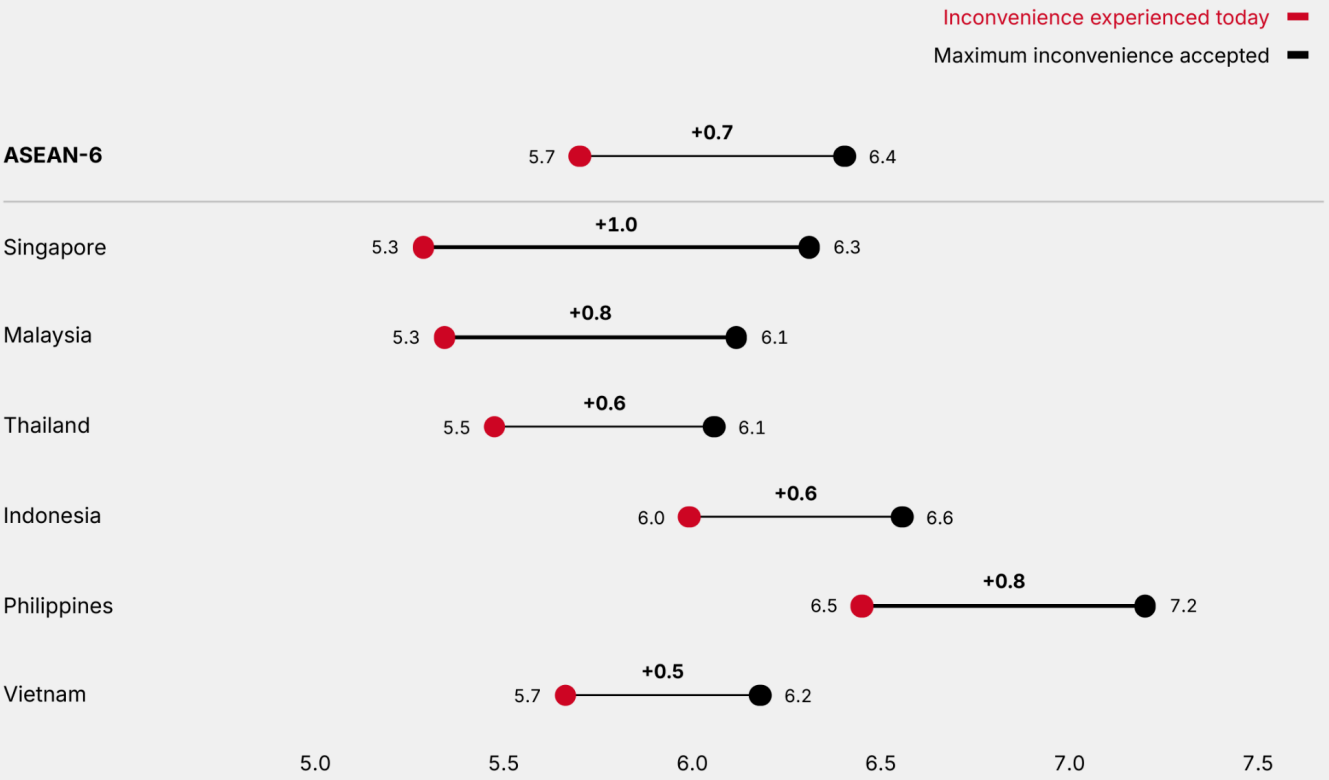
With friction, consumers rate the inconvenience they currently experience in online transactions at 5.7 out of 10, and the maximum they would accept in exchange for stronger protection at 6.4. That leaves 0.7 of a point of room across the region, and the figure is narrow in every market, from a full point in Singapore to half a point in Vietnam.

A security step applied to every transaction uses that room on every customer, including the overwhelming majority whose transactions are legitimate, and friction is increased whether or not the step is effective. Beyond that point, added protection will start to reduce transaction completion, leading to real industry cost. The question for industry and regulators alike is therefore not only whether a measure stops scams, but whether it can be aimed at the transactions that carry risk rather than broadly across all of them.

Figure 13

Friction headroom by market

Mean rating



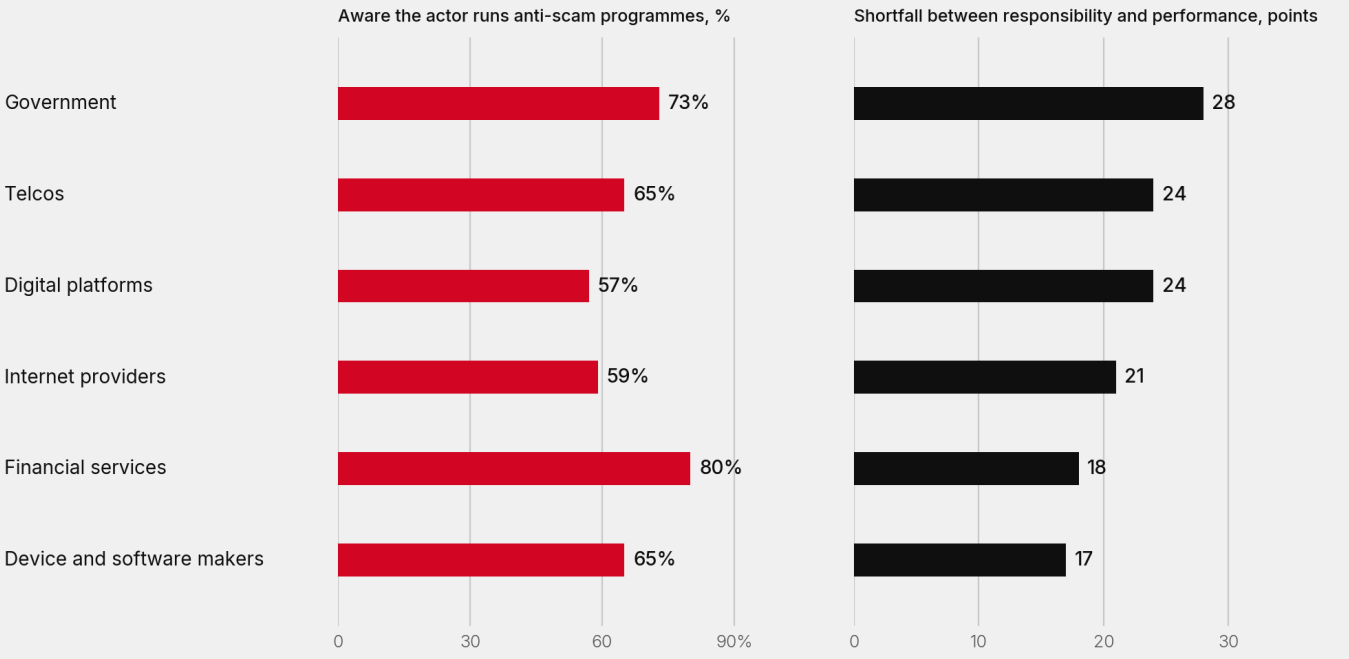
Source: GSMA Consumer Scam Survey 2026

The second factor is credibility. Consumers know these organisations run scam programmes: 80% are aware of programmes from financial services, 73% from government and 65% from telcos. Awareness has not produced confidence. Every actor is rated below the responsibility consumers assign it, by 18 points for financial services, 24 for telcos and 28 for government. Programme visibility is not the constraint.

Figure 14

Programmes known, and the performance shortfall

Percentage and percentage points



Source: GSMA Consumer Scam Survey 2026

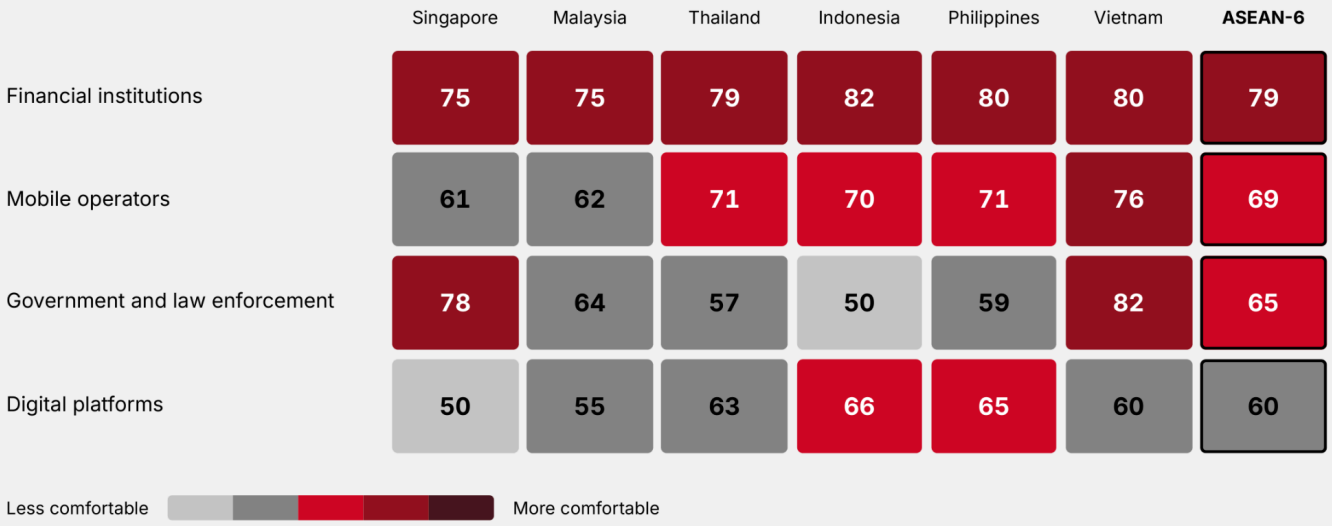
Permission is the third element. Asked how comfortable they are with each actor holding and using their data to detect fraud, consumers rated financial institutions first at 79%, telcos at 69%, government at 65% and digital platforms at 60%. What separates them is geographic consistency rather than the average. Comfort with financial institutions moves only 7 points across the six markets, from 75% to 82%, while comfort with government swings 32 points, from 82% in Vietnam to 50% in Indonesia.

Any arrangement that assumes a single regional answer to who may hold consumer data will therefore fit some markets and not others, and the actor whose licence varies most is the state. Platforms are in the most difficult situation: they hold the least permission of any actor, while the two largest single scam channels in the region, messaging apps and social media, are theirs.

Figure 15

Who consumers permit to hold their data

Percentage comfortable



Source: GSMA Consumer Scam Survey 2026

3.3

Country Snapshots

Figure 16

Where each market sits against the region

Percentage, and distance from the regional figure

	ASEAN-6	Singapore	Malaysia	Thailand	Indonesia	Philippines	Vietnam
Rate their own protection highly	**77**	65	78	80	86	87	68
Absolutely worry about scams	**59**	38	65	48	61	76	64
Aware of government programmes	**73**	82	80	69	50	65	91
Rate government protection highly	**43**	56	46	28	28	38	62
Aware of telco programmes	**65**	35	59	78	65	74	77
Comfortable sharing data with telco	**69**	61	62	71	70	71	76

Bar shows the market's distance from the ASEAN-6 figure, left for below and right for above. Every row uses the same scale, so a flat row is a spread that is genuinely small.

Source: GSMA Consumer Scam Survey 2026

Singapore is where recognition of anti-scam efforts sits almost entirely with the state. Eighty-two percent of Singaporeans know about government anti-scam programmes and 56% rate government protection highly, both near the top of the region. Across the six actors we track, the average Singaporean is aware of programmes from 49% of them, against a regional 66%, the lowest in the region. Every commercial actor sits far below: awareness of telco programmes runs at 35% against a regional 65%, digital platforms at 33% against 57%, internet providers at 34% against 59%, and even financial services at 69% against 80%. Singaporeans also rate their own protection lowest of the six markets, at 65%, are the least worried at 38%, down from 50%, and are the most likely to have taken no protective action at all, at 11%. Concern has fallen without confidence rising and Singapore is both the least worried market and the most likely to do nothing.

Malaysia pairs maximum expectation with minimum permission. Malaysia has the widest gap in the region between what it asks of its operators and what it allows them to do. Seventy-eight percent of Malaysians assign telcos high responsibility for stopping scams, while only 62% are comfortable letting their operator use their data to detect fraud. That 16-point gap is the largest of the six markets, against 13 points in the Philippines and 9 in Singapore, and it runs the other way in Thailand, Indonesia and Vietnam, where permission sits ahead of expectation. Malaysia demands the most from its operators while granting them the least room to act.

Thailand is one of the region's success stories. The share of Thais who say they absolutely worry fell from 67% to 48%, and recent victimisation is the lowest of the six markets at 5%, coinciding with several years of sustained intervention. Consumers reward the effort unevenly: Thailand shows the best telco perception in the region, with 78% aware of operator programmes, alongside the worst government perception, tied with Indonesia at 28%. The gains did not come from consumers working harder: Thais take the fewest protective actions of any market, 2.4 each, and are the second least worried, yet they are the least likely to be scammed. Two gaps remain open, the network and the state's own identity: voice calls are involved in 50% of Thai victims' scams, and 35% of Thai victims were hit by someone posing as police, tax or the courts.

Indonesia is the market where the state registers least with consumers on every measure we track. Only 50% of Indonesians are aware of any government anti-scam programme, against a regional 73%, government protection scores 5.4 out of 10, the lowest rating any actor receives in any market, and only 50% are comfortable sharing data with government. Consumers have filled the gap themselves: 86% rate their own protection highly against 28% for government, the widest gap between self and state of the six markets, and only 17% of victims go to the police, against a regional 36%. Official statistics built on police reports will therefore capture only a fraction of Indonesia's scam problem.

The Philippines is the market where victims take their cases to platforms rather than the police. Filipinos are the region's most anxious consumers, with 76% saying they absolutely worry, and its most friction-tolerant, carrying 6.5 and willing to bear 7.2. Reporting has moved decisively to platforms: 49% of Filipino victims reported to digital platforms, the highest in the region, while only 16% went to police, against a regional 36%. Filipinos are also the most likely to act on distrust, with 24% switching providers and 62% avoiding contact or transactions. Investment and crypto scams reach 41% of Filipino victims, the highest of the six markets and well above the regional 29%.

Vietnam carries the region's highest exposure alongside its highest trust in institutions. Thirteen percent of Vietnamese consumers were scammed in the last twelve months, well above the regional 8%, and 95% recognise AI techniques in the scams they meet, also the highest in ASEAN. Trust has not eroded alongside it: 91% are aware of government anti-scam programmes, 82% are comfortable sharing data with government and 62% rate government protection highly, all regional highs, while 76% are comfortable sharing data with their mobile operator, again the highest in the region. Vietnam is therefore the market where the need to

act and the permission to act are both at their greatest. That permission is not guaranteed to hold. Victims whose cases go unresolved withdraw exactly this kind of consent, and Vietnam is producing more cases than any other market.

04

What to do next

4.1

What the Ecosystem Can Do Next

1. Coordinate reporting for effective tracking and resolution. Forty-five percent of reported cases go unresolved, and victims are not the reason. They take a case to 1.9 organisations on average. Victims whose losses still worry them today escalate hardest, to 2.3 organisations against 1.5, and recover at much the same rate. Scams also run across channels, with 49% of victims naming more than one, so no single organisation ever sees the whole case. That points towards a coordinated reporting arrangement in each market: a case reported at any entry point, financial institution, telco, platform or police, is registered once under a single reference and made visible to the organisations that need to act on it, so the victim reports once rather than repeatedly to each in turn. Success is measured on outcomes rather than activity: share of victims recovering funds, time to resolution, share of cases still unresolved. Where cross-sector machinery is out of reach this cycle, the unilateral first step is for each institution to publish its own reporting volumes and outcome figures, creating the baseline a coordinated arrangement needs.

2. Make anti-scam commitments verifiable, not merely visible. Consumers know these organisations run scam programmes, with awareness running from 57% for platforms to 80% for financial services. Knowing has not produced confidence: every actor is rated below the responsibility consumers assign it, by 18 points for financial services, 24 for telcos and 28 for government. The programmes are already known, so the gap is not one of visibility. What consumers have is each institution's own account of what it does, and the report's own finding elsewhere is that higher trust sits with resolved cases rather than with programme awareness. One option, and the one we would test first, is a certification anchored to the same outcome measures as recommendation 1 rather than to a described programme: a published minimum standard, common across institutions, that ties certification to what an institution actually resolves rather than what it claims to run. Its advantage over a communications campaign would be that it is checked against the same numbers a case-tracking system would already be producing.

3. Financial institutions: extend recovery to more transactions. The one recovery mechanism in the region that reliably works is the card charge reversal. Where a charge is genuinely unauthorised and the victim raises it with their financial institution, money comes back far more often than through any other route. It works because the money has not left the system: a financial institution can reverse what it still holds. It stops working the moment the funds move, and the advantage narrows as losses grow. What we propose extends that same principle to funds still in the system: increased flagging or holding of transfers that carry the markers of a scam in progress, and stronger cooperation between financial institutions so a payment can be stopped at the receiving institution

and not only at the sending one. Financial institutions already have the standing to do this. They hold the region's deepest and most uniform consumer permission to use data to detect fraud, at 79% and varying by only 7 points across the six markets, a mandate no other actor holds in every market.

4. Operators: act on the vectors they control and supply identification to those who cannot see them. Voice calls are involved in 35% of victims' scams and SMS in 30%, the third and fourth largest channels in the region and the two that operators run. A quarter of victims were hit by someone posing as police, tax or the courts, and 72% of those scams arrived by voice call or SMS. The work we propose is on the network: challenging calls and messages that impersonate an authority or a brand, verifying sender identity, and filtering scam messages before delivery. Operators also hold signals no other actor can see, and consumers already permit their operator to use data for fraud detection at 69%, second only to financial institutions. On that permission, we propose sharing SIM-change status and number verification with financial services at the moment of a transaction, so the institution holding the money can flag a fraudulent payment before it completes. Both should be aimed narrowly rather than applied across the board, because the region has only 0.7 of a point of friction to work with.

5. Platforms: the largest channels, the least visible response. Messaging apps and social media are the two largest single channels in the region, involved in 41% and 36% of victims' scams, ahead of voice at 35% and SMS at 30%. Exposure of that kind reflects where consumers spend their time as much as how well a channel is policed, and this survey cannot separate the two. What it does measure is visibility and permission. On both, platforms sit last of all the actors: least known for running scam programmes, at 57%, and holding the least permission to use data, at 60%. Their shortfall against the responsibility consumers assign them, at 24 points, matches the operators'. That leaves platforms less room for a data-led response than other actors have, so what we propose is structural: seller and advertiser verification, faster takedown, and co-owned case handling with financial services whenever payment leaves the platform. In the Philippines, 49% of victims report to a platform against 16% to the police; the handover from platform report to financial recovery is the practical gap to close.

6. Governments and regulators: measure resolution, design data sharing for market variation, retarget education. Government carries the region's widest gap between expected and rated performance, and consent for the state to hold data is the region's most uneven, swinging over 30 points between markets. What we propose follows directly from both: mandates that measure and publish case outcomes rather than centralise data, and data-sharing arrangements designed around the level of consent each market actually gives rather than a single regional model. Where public consent for the state to hold data is high, as in Vietnam at 82%, a state-led arrangement has the mandate it needs. Where it is low, as in Indonesia at 50%, the same design will not carry. Education budgets should be split by audience, because general awareness has already reached most of the population and further untargeted spend will add little. Awareness campaigns should be refocused rather than retired, onto the 11% who saw scams but could not tell whether AI was involved. That

group takes no protective action at all at 20%, against 7% of consumers overall, and what they lack is recognition rather than motivation, which is the one thing awareness content is built to supply. New programmes should shift focus to two other groups: victims, who accept responsibility and want to act, and the silent minority whose overconfidence keeps them from reporting at all.

For both, the emphasis moves from awareness towards the actions that follow it: reporting the case, and taking it to an organisation that can act on it. Neither group needs telling that scams exist. Both, though, are meeting a class of scam that works by persuasion rather than theft, where recognising the approach is the only defence available before the money moves.

4.2

Conclusion and the Path Forward

Consumers have done their part. Every protective behaviour we track rose this year, the share doing nothing at all fell to 7%, and two-thirds of the region has changed how it behaves because of scams. That is a population that has heard the message and acted on it.

What they meet on the other side has not moved. Forty-five percent of reported cases are never resolved. Eighty-two percent of victims who lose money get none of it back. Reaching an organisation that can act is left to the victim's own persistence. None of that is a failure of consumer effort, and none of it will be fixed by more consumer effort.

This wave measures something the earlier ones could not. Where cases go unresolved, the cost shows up well beyond the victim. Victims whose cases were left open trust less and share less than victims whose cases were closed, across every actor measured. The damage does not stay with the organisation that failed. It spreads, through the ecosystem and through personal networks, because behaviour travels between people even when the scam does not.

Some of that cost cannot be bought back. A consumer who has pulled out of online shopping does not return when the case is finally settled. That is the argument for prevention rather than remediation.

The region also has less room to act than it assumes. Consumers will accept less than one further point of friction, and they grant more permission to their banks and mobile operators than to the state. Any measure applied across every transaction spends that room on everybody, whether or not it works.

What would change the picture is narrow and specific. A case reported once that reaches everyone who needs to act on it. Recovery measured and published rather than activity. Commitments a consumer can check rather than take on trust. None of it requires another campaign, and all of it is within reach of the actors named in this report.

Get that right and the sequence runs the other way. Cases that close sustain consent, consent enables the data sharing that shared defences depend on, and those defences stop the next case before it starts.

Consumer survey methodology

The insights in this report are based on cross-sectional online surveys of adults (18 and above) in six ASEAN markets: Singapore, Malaysia, Thailand, Indonesia, the Philippines and Vietnam. Wave 3 (2026) fieldwork was conducted by Milieu Insight via self-administered online interviewing in local languages, with approximately 500 respondents per market (n=3,000) and non-interlocking quotas on age by gender, region, and socio-economic class. Respondents gave informed consent and data were anonymised and handled in line with GDPR and PDPA principles. ASEAN figures are equal-weighted across the six markets; cohort comparisons use the combined six-market base. Victim impact, reporting and recovery metrics are calculated on the experiences of victims only. 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

Report author
Armidale