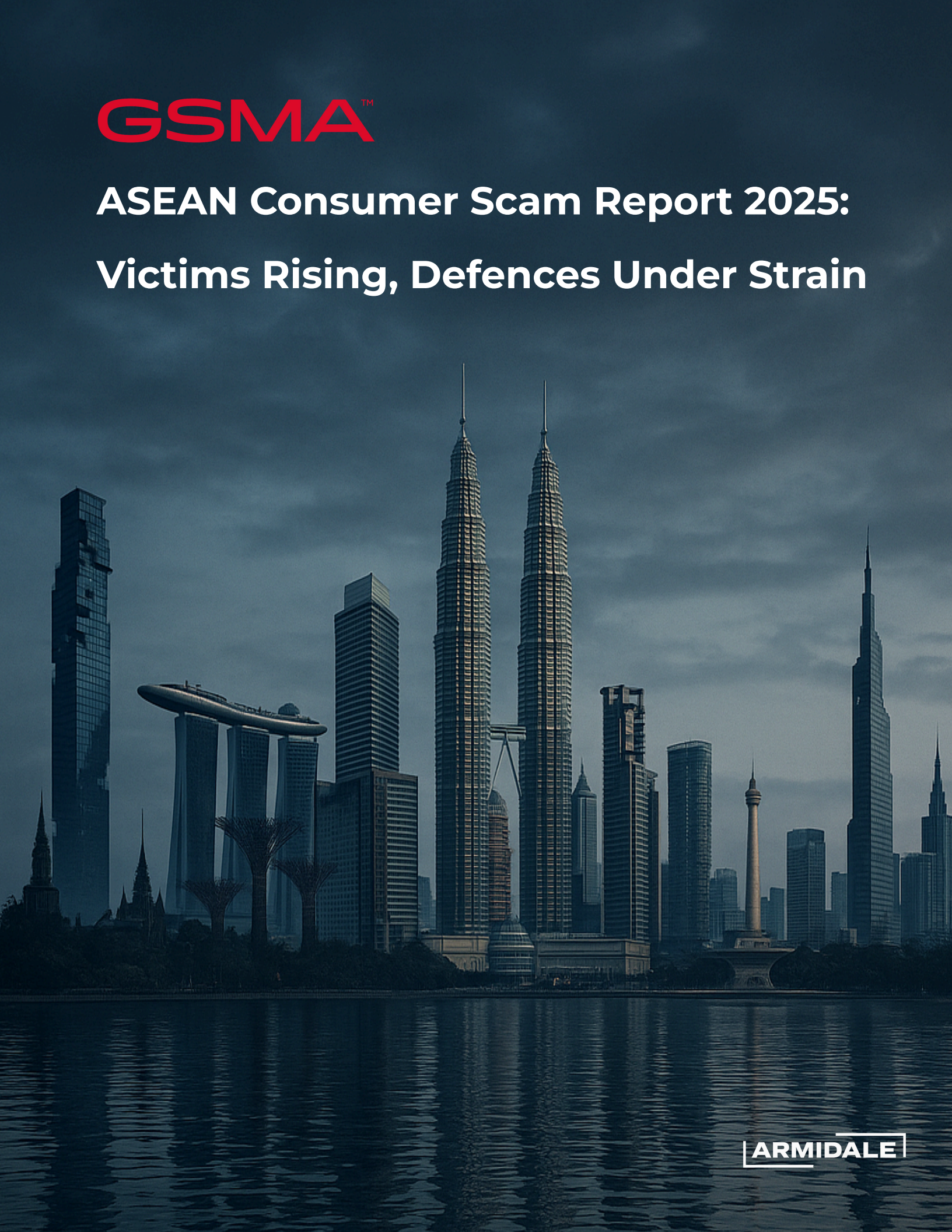
GSMA™

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



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**

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 platform visibility. We are also grateful to the survey partners, Milieu Insight and respondents across ASEAN, whose participation made these insights possible.

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

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

Executive Summary

Scams are on the rise across ASEAN, and they are increasingly targeting people's everyday channels. The equal-weighted share of consumers who report having ever been scammed increased from 31% to 45%. Involvement is overwhelmingly mobile and multi-channel, with victims most often citing OTT messaging, voice calls, and social platforms, while SMS and email remain present. The mix differs by country (for example, social/SMS are more prominent in the Philippines, while voice/OTT is more prevalent in Thailand, Singapore, and Indonesia), which means countermeasures must be tailored to where scams actually originate.

The harm is real, and people are reporting it. In 2025, 68% of victims reported losing money, with 11% stating they had lost a large sum, and ~76% reported the incident to the authorities. Reporting is split across banks/fintechs, police, and platforms, so no single institution sees the whole case, which slows recovery and weakens deterrence.

Privacy concerns remain near-universal at ~97%, and demands for broad disclosures have increased (the share saying it is important that companies disclose what they share moved 95% to 98%). The signal from consumers is consistent: keep data use tight, transparent and tied to specific outcomes.

Acceptance of protective mobile-network signals is strong. 72% are comfortable with limited, purpose-bound checks, and support rises further when sharing is exception-based; this creates a practical path for GSMA Open Gateway–style APIs (e.g., SIM swap, number verification, device status, coarse location confidence) to harden logins and payments while minimising data point use. In contrast, comfort with conversational-app data sharing has dropped from 53% to 40%, mirroring concerns about impersonation and phishing on those platforms.

Consumers will reward better protection. 81% say they would switch financial providers for stronger security, favouring products that bring verification to the front, confirmation-of-payee, safer payment instruments, and simple “official call-back only” habits.

The way forward is clear: prioritise the hot routes (voice/OTT first; strengthen social and SMS where elevated), make safe behaviours the default, use targeted, transparent, authorised data sharing to verify transactions, and close the reporting loop so every report turns into fast, visible remediation.

Consumer Experience & Attitudes Toward Scams

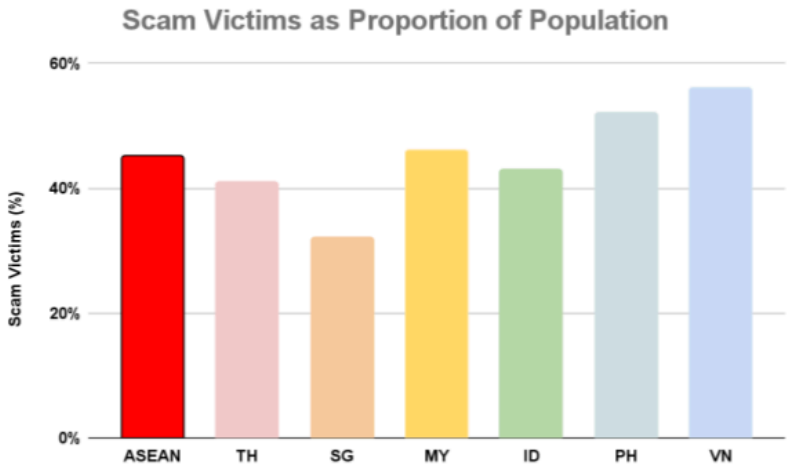
Overview of consumer experiences

Across ASEAN, 45% of people reported having been the victim of a scam, compared to 31% last year. The number of people reporting being a victim of a scam within the last year increased from 6% in 2024 to 8% in 2025, indicating accelerating growth. Significant increases in scams were observed this year, particularly in the Philippines and Thailand, with more moderate increases in Indonesia and Malaysia.

The implication is straightforward: risk factors are rising rapidly, whereas enforcement and controls are patchy and falling. For organisations holding customer data or money, this justifies continued investment in threat intelligence, call-back hygiene, and consumer nudges that blunt social engineering attacks before identity theft or data exfiltration occurs.

Exhibit 1: Lifetime scam victimisation - The size of the impact

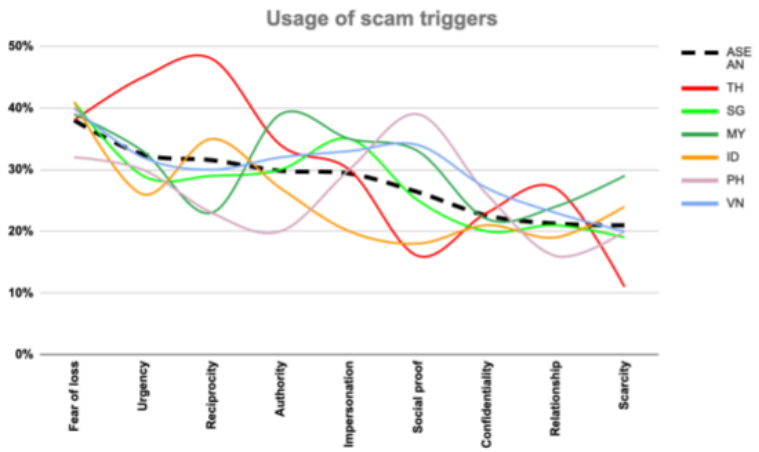
The problem is accelerating with 45% of people reporting being scammed - 8% within the last year



Across ASEAN, scammers use a broad mix of psychological triggers rather than a single script. Fear of loss and urgency tend to appear most often, with authority/impersonation close behind, while reciprocity, social proof, relationship, confidentiality, and scarcity are all present at meaningful but lower levels. Country patterns are relatively consistent, with the exception of Thailand, which shows a more pronounced tilt toward urgency and authority than most markets.

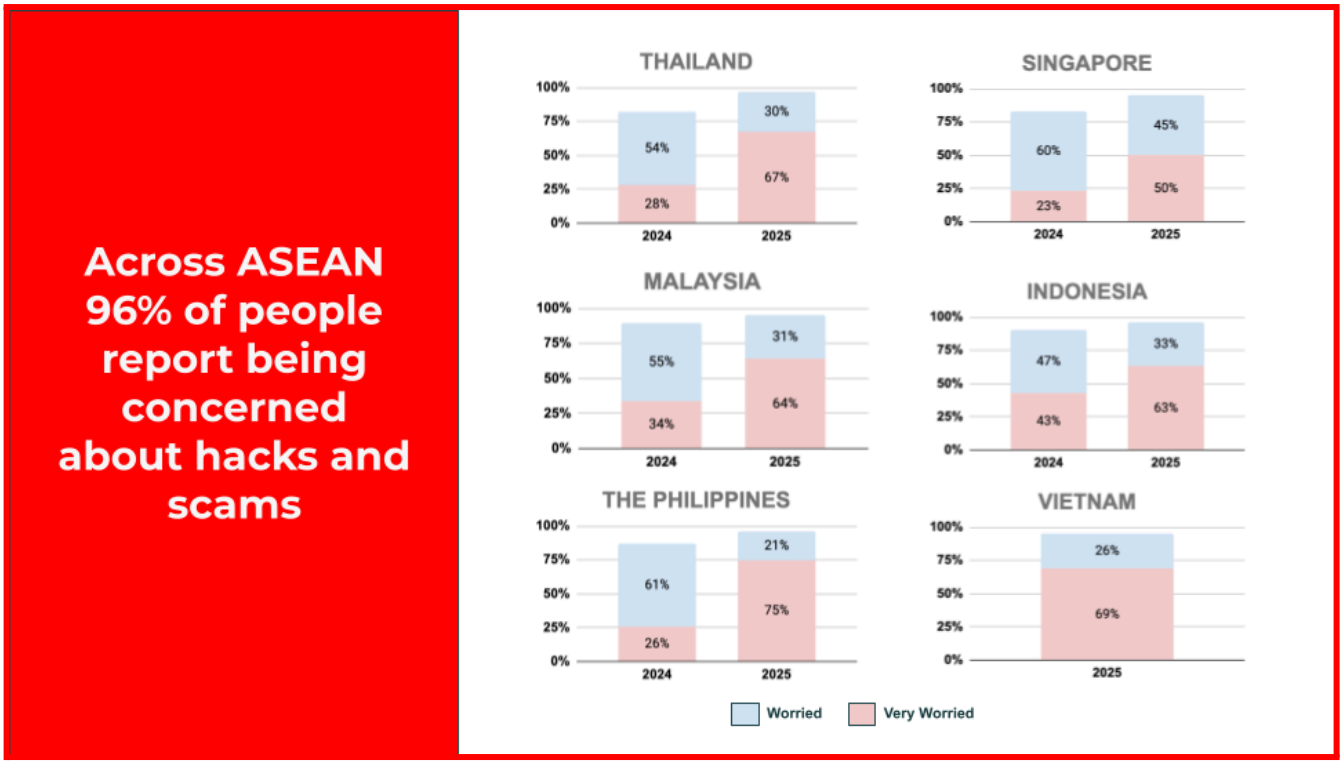
Exhibit 2: Scam Triggers - How scammers are influencing their victims

Fear-of-loss and urgency are the most-used scam triggers, but all triggers are broadly used



This sharp increase in scam activity is also increasing anxiety across the population, and those reporting being worried are now nearly universal across ASEAN: 96% say they are concerned (Top 2), up roughly 10 percentage points from 2024. The shift is not just more people worried; the share saying they are very worried jumped sharply in every market (i.e., TH 28%-67%, SG 23%-50%, MY 34%-64%, ID 43%-63%, PH 26%-75%; VN, measured for the first time, also has a similar result at 69%). This step-up from worried to very worried signals that scams and account takeovers have moved from background concern to a top-of-mind consumer protection issue, reinforcing the need for quick and decisive action to be taken.

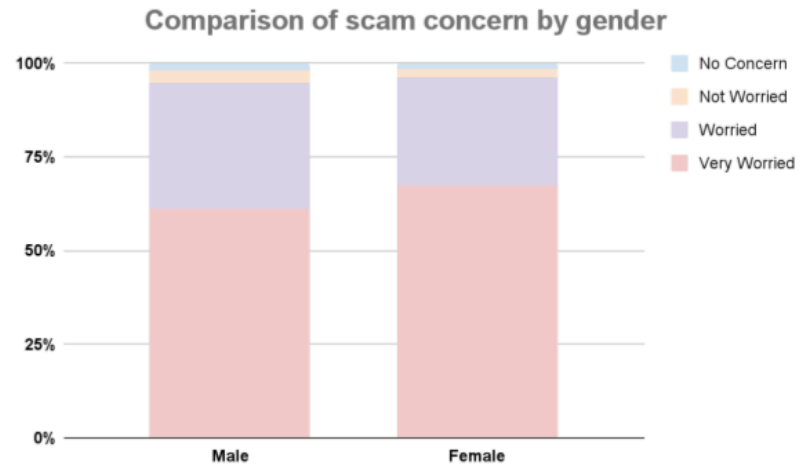
Exhibit 3: Concern about scams & hacks - The ongoing anxiety



When split by gender, the situation becomes even more extreme, with women expressing greater intensity of worry about scams than men. 68% of women say they are “very concerned,” compared with 61% of men. This should leave no doubt about the significance that this topic has taken on within the population and that communication and education should be tailored to the target audience.

Exhibit 4: Gender comparison - Worry is intense for all, and higher among women

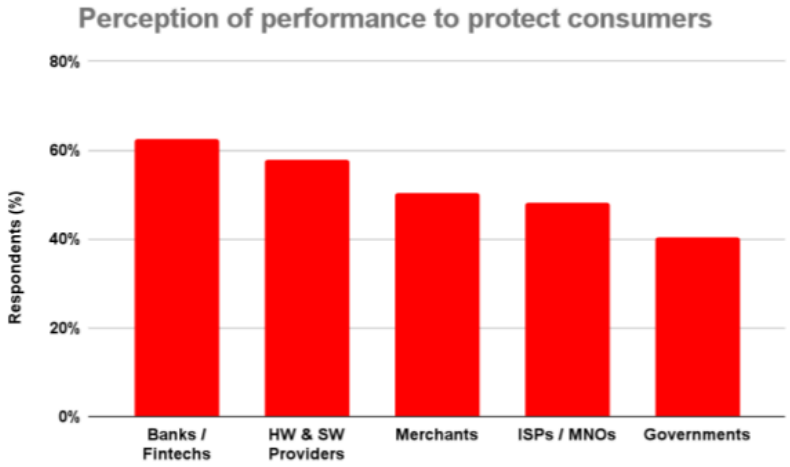
Concern is equal between genders, however, 68% of women are "Very concerned" vs 61% of men



Consumers see everyone playing a role, but some are judged more effective than others. Banks/fintechs lead (~62%), followed by hardware/software providers (~57%), and merchants (~50%); ISPs/MNOs trail slightly (~48%), and governments sit at the lowest level (~40%). This suggests a need to raise visibility of protections and speed of enforcement.

Exhibit 5: Perceptions of performance - Who is demonstrating their success?

All participants are seen as working for the consumer, although Governments likely need to step up quickly



Key fraud concerns and channels

Victims most often describe voice calls and OTT Messaging Apps as contact points, with social platforms also material, particularly where marketplace scams and impersonation occur. SMS remains a meaningful trigger in some markets, and email is the least common route. This multi-channel attack surface reflects the blending of phishing attacks, fake “support” calls, and targeted social engineering.

Defences must be channel-specific, caller display and screening for voice, sender-ID and content controls for SMS, rapid platform escalation for suspicious behaviour on social media, and tighter app-to-person guardrails in OTT.

An emerging vector is fake QR codes, often referred to as “quishing” (QR-code phishing). In our 2025 data, QR routes appear in ~10% of scam contacts across ASEAN (higher in Vietnam at 13% and Malaysia at 11%).

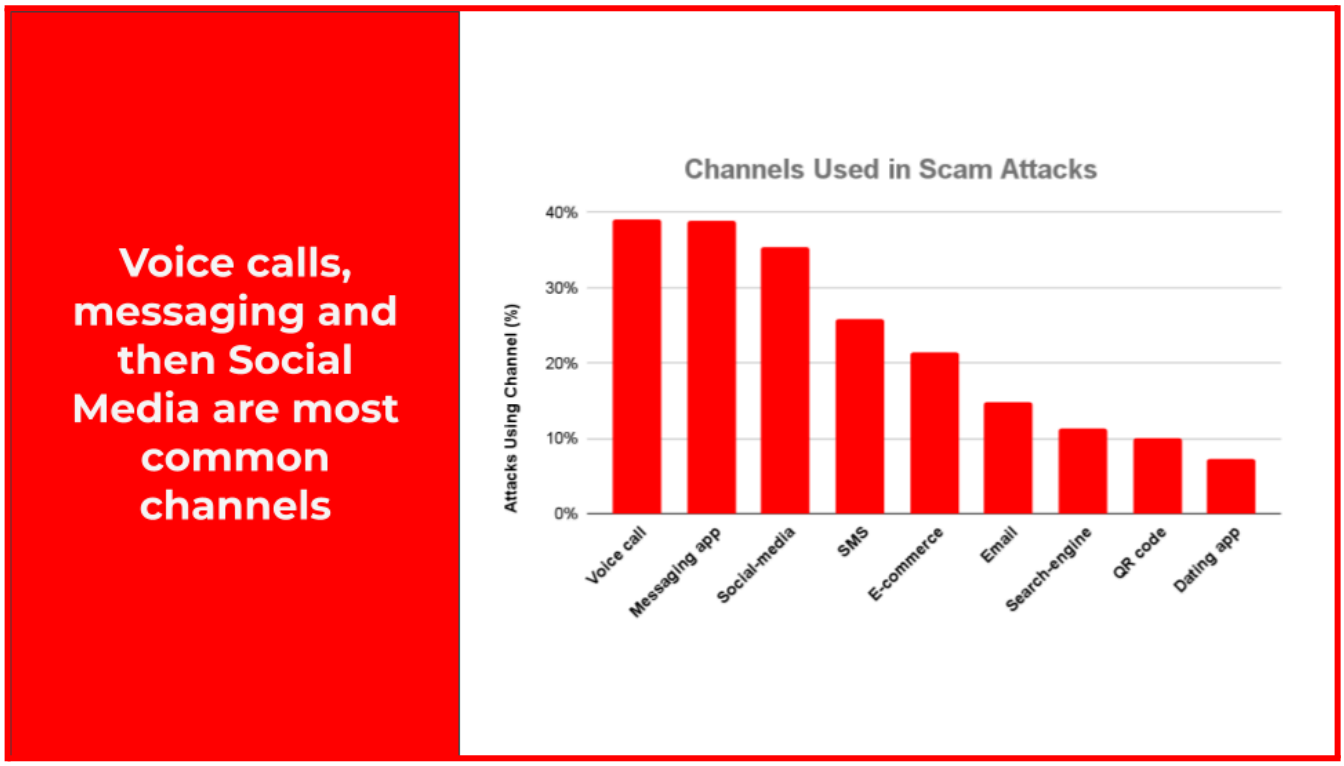
Dating/romance sites and apps account for ~7% (notably SG 12%, TH 10%) but arguably

impact people the most post-scam as they leverage people's emotional connection.

> *"I was scammed into a relationship-app-related investment. Lost a large sum of money through that scam, and I am still paying for loans that I took out."*

These channels represent a small but significant share today and are relatively inexpensive to scale, so they could grow quickly if left unchecked. Safer QR journeys (dynamic codes, trusted-domain previews, post-scan warnings) are effective technology-enabled solutions, and tighter verification and AI-enabled content moderation on dating platforms would blunt romance-style social engineering.

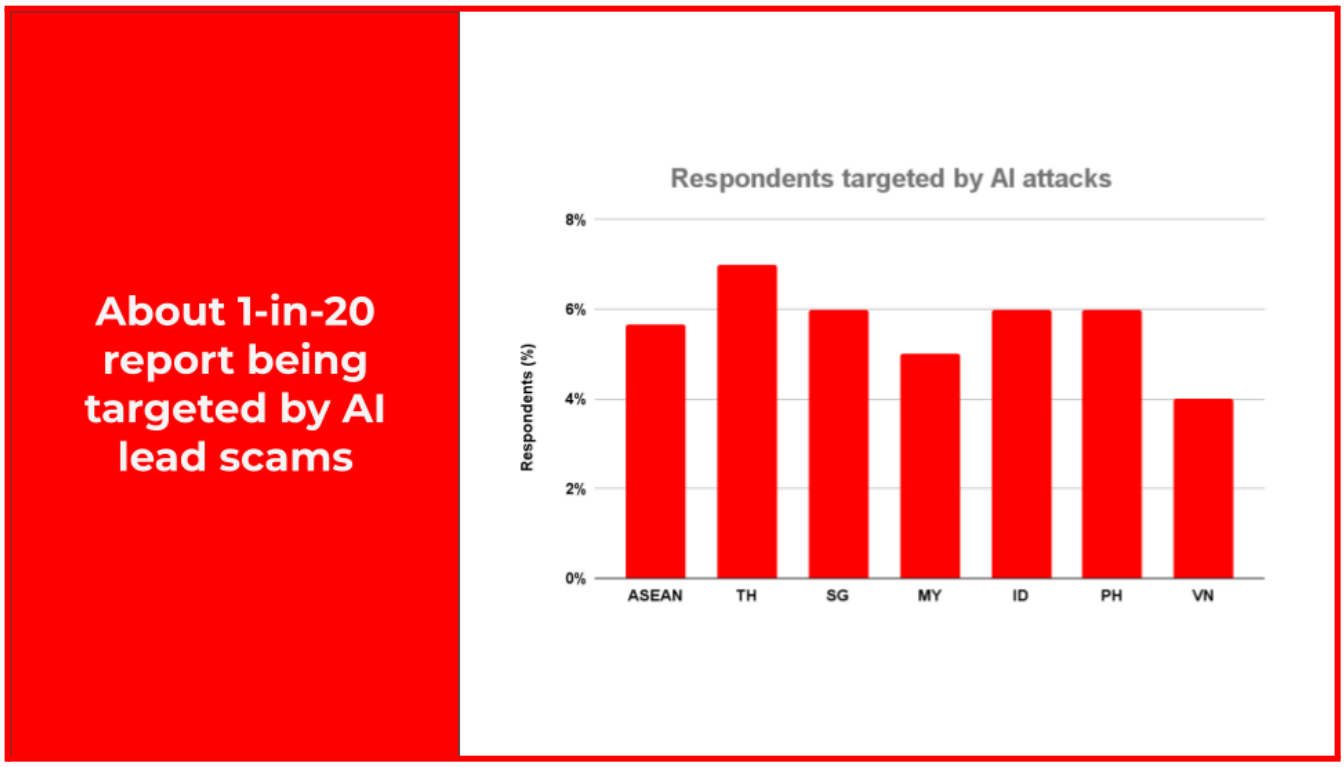
Exhibit 6: Scam channels of attack - How are scammers reaching consumers?



A small but visible share of respondents say they've been personally targeted by AI-enabled scams (around 5–6%) at the ASEAN level. This is self-reported, and attribution is challenging (victims rarely know whether a convincing voice, image, or chat was AI-generated), so results should be interpreted as directional rather than definitive.

Even so, the signal is statistically measurable in our sample sizes and merits ongoing monitoring and further study, especially for voice cloning, deepfake customer-service chats, and real-time OTP relay attacks.

Exhibit 7: AI scams - The start of a new concerning trend

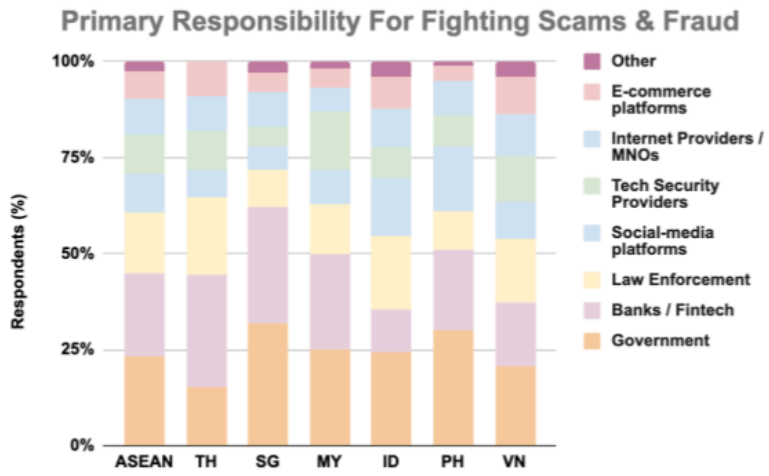


Perceptions of trustworthiness, responsibility, and switching

When asked who should take primary responsibility for protecting people from scams and financial crime, respondents place government/regulators, banks & e-wallets, and police/law enforcement at the top, followed by platforms and telecommunication companies.

Exhibit 8: Primary responsibility - Who should be accountable?

With national deviations Governments & Banks are seen as responsible for leading anti-fraud measures



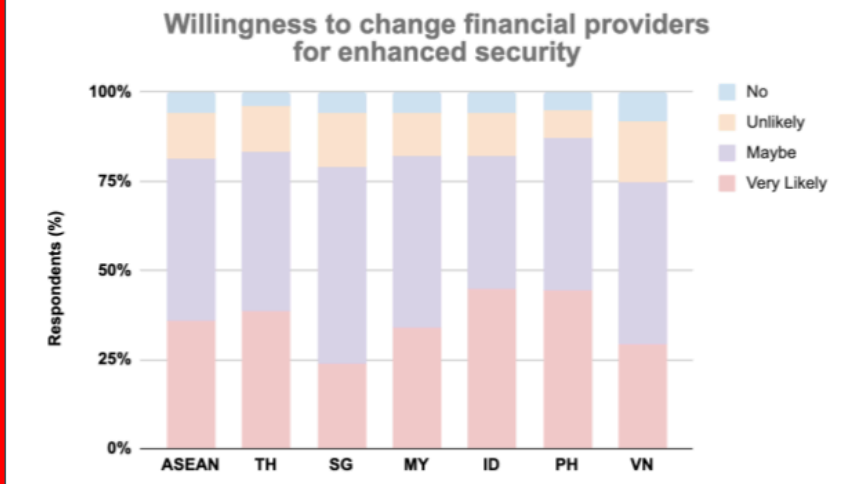
The implication is a strong mandate for multi-stakeholder action: coordinated policy, technical standards, and shared playbooks.

Willingness to switch financial providers for better security increased from 78% (2024) to 81% (2025), a clear growth signal that banks and fintechs can capitalise on by prioritising security in their products. The winning moves are:

- Digital Identity checks at high-risk moments (passkeys, device binding, and authorised, minimal-data signals such as SIM-change/number-verification),
- Transaction verification that shows the payee's name before you send (Confirmation-of-Payee-style checks)
- Safer payment instruments, such as virtual/one-use card numbers for online payments.

Exhibit 9: Switching financial providers for enhanced security

Willingness to switch financial providers for additional security has now grown to 81%

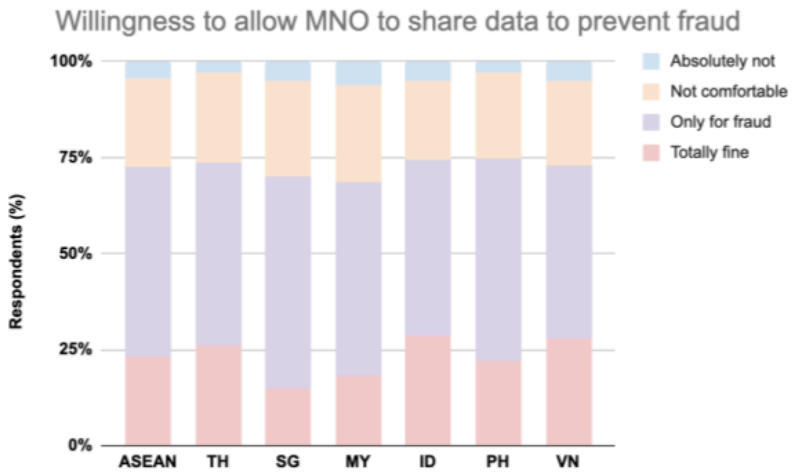


Comfort with MNOs sharing limited, purpose-bound signals for fraud detection stays high, and consumers tell us they support this when it is targeted, transparent, and authorised. The practical role for operators is to expose simple yes/no Digital Identity signals, such as number verification, recent SIM change flags, device status, coarse location confidence, or call-forwarding state, at specific high-risk moments (e.g., new device login, password reset, large transfer, or QR payment).

Used only to verify transactions, these checks help banks and fintechs prevent account takeover routes, such as SIM swap and OTP diversion, while also reducing false positives and unnecessary friction. Critically, the data stays minimal (no message content, no profiling), with clear consent, short retention, and auditability. With plain-language customer messaging, this improves fraud detection and approval rates without compromising privacy.

Exhibit 10: Willingness to allow MNOs to share data

Around 1-in-4 consumers would support targeted data sharing to prevent fraud

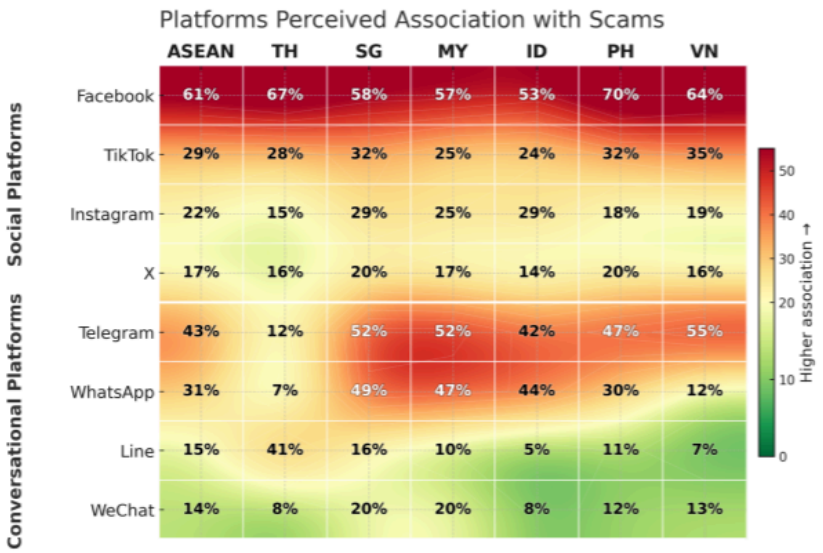


Facebook stands out as the platform most commonly linked to scams in ASEAN, with 61% of overall responses and above 50% in every market (PH 70%, TH 67%, VN 64%, SG 58%, MY 57%, ID 53%), indicating a clear problem, whether perception or lived experience.

Conversational apps carry notable perceived risk, but the app differs by market: Telegram is frequently cited for anonymity-driven scams; Thailand is the exception, where LINE (41%) is most associated; WhatsApp is more prominent in SG (49%), MY (47%) and ID (44%). VN reports only Telegram, likely due to the popularity of Zalo, which, as a platform, was not included in the question.

Exhibit 11: Platform association with scams

The country's major social platform and messaging app are most associated with scams



This illustrates an urgent need for platform-specific mitigation. Tightening of page/account and marketplace verification, ad-buyer KYC, fast takedown and AI monitoring on Social Platforms. Messaging Apps, and in particular anonymous ones like Telegram, have significant issues as they cannot police content but should make efforts to utilise Digital ID (verified accounts / device-binding), add verified-sender labels, require transaction-time verification on risky flows, and apply high-friction link sharing with rapid takedown, partnering with banks and telcos via authorised, minimal-data signals to cut off scam journeys.

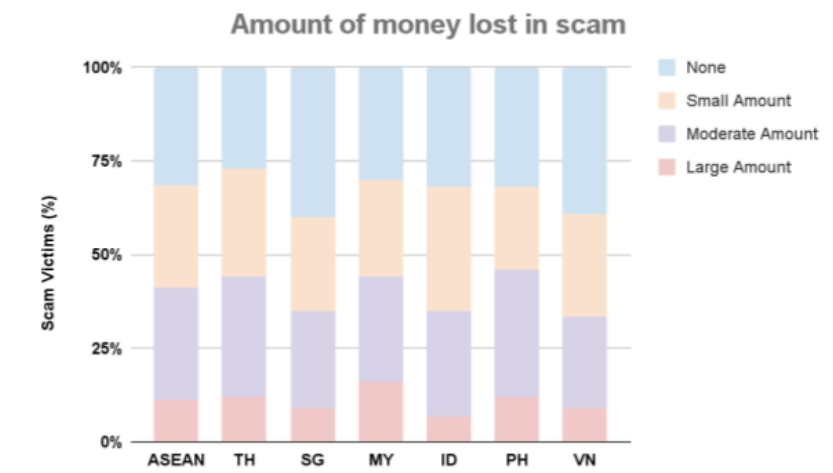
Regular buying on Social Platforms is now routine for a sizeable share of consumers, roughly 1 in 5 across ASEAN, with Vietnam and Thailand the stand-outs for weekly/monthly purchase frequency, yet they are also the least-trusted platform in our study, with the highest perceived association with scams. This trust–use gap matters as people continue to shop where they feel most at risk, increasing exposure to impersonation, counterfeit goods, and payment fraud. The trust–use gap is widening, increasing exposure unless seller verification and takedown speed improve.

Victim impact, reporting and recovery

Harm is material: among victims in 2025, 68% reported losing money, with 30% describing the amount as “moderate” and 11% reporting a “large amount” loss. Combined with the previously mentioned 8% experiencing the scam within the last year, this is a meaningful impact on household finances across the region.

Exhibit 12: Financial impact of scams

11% of consumers report losing a “large amount” of money to a scam



Apart from the monetary loss, many also report second-order harms, time/effort to resolve (~45%), emotional distress (~45%), and ongoing anxiety (~45%). This is no longer a nuisance problem; it is a consumer-protection and liability issue that erodes trust if reporting and/or recovery feels opaque and slow.

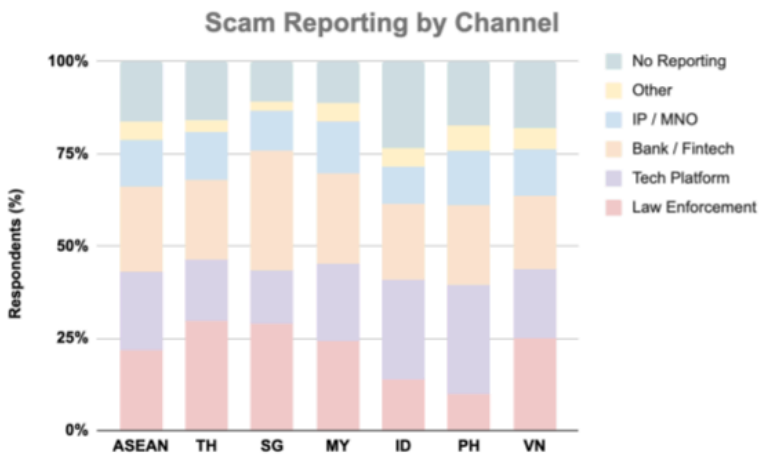
Exhibit 13: Other impacts of scams - Beyond just the financial

Emotional distress, Lost Time & Effort, and Ongoing Anxiety also rank highly with Financial Loss

In 2025 reporting is common but fragmented. About three in four victims (76%) report somewhere, but routes split across banks/e-wallets (~36%), police (~34%), and the platform where the scam occurred (~33%).

Exhibit 14: Scam reporting - Where do people go when they are scammed?

Reporting is common but fragmented and differs by market - no single organisation has the full picture



No single institution sees the whole picture, so cases fall through the cracks without coordinated handoffs; however, this creates clear opportunities for improvement.

- Make reporting “no wrong door.” Any entry point (bank, platform, police, telco) should capture a minimal, standard case record, generate a single case ID, and route ownership to the right lead.

- Define and publish recovery SLAs. Commit to time-to-first-response, time-to-update, and time-to-closure targets. Freeze/recall funds when possible, file SAR/AML reports as required, and keep victims informed throughout the remediation process.

- Reduce stress and time costs. Provide a status tracker, secure document upload, clear “what happens next” guidance, and named contacts. These directly address the ~45% who cite process pain.

- Share authorised signals to speed triage. Use Digital Identity checks and minimal,

purpose-bound signals (e.g., number verification, recent SIM change) at payment time to confirm attribution and prioritise recovery (without broad data sharing).

- Measure outcomes, not activity. Track and report: % victims reimbursed / funds recovered, time-to-first-response, time-to-customer-update, time-to-closure, and % non-reporting; set targets to cut that non-reporting gap further.

The bottom line is that high financial loss prevalence, combined with widespread reporting, creates a real opportunity to reduce harm now, if institutions coordinate handoffs, make recovery timelines transparent, and turn every report into a swift, auditable incident response.

Privacy, transparency and trust

Alongside concerns about scams and anxiety, concern about privacy remains near-universal (96% in 2024 to 97% in 2025), while the share stating that companies disclose what data they share with others has also remained at extremely high levels (95% in 2024 to 98% in 2025).

This reinforces that although consumers are highly concerned about scams, they also recognise that the private information that companies have can be leaked and used against them. This means that data sharing must be done very cautiously with clear, purpose-limited disclosure, short retention, and easy opt-out, without these companies inviting regulatory scrutiny and reputational damage.

Exhibit 15: Concern for privacy - Data sharing is a double-edged sword

Privacy concern is near universal

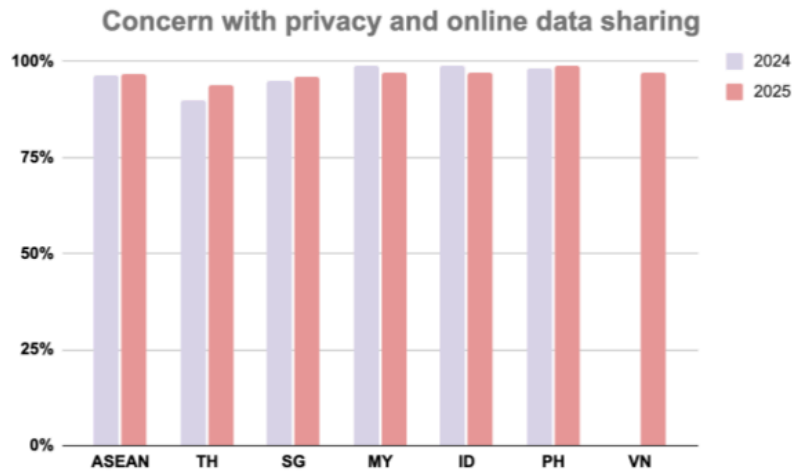
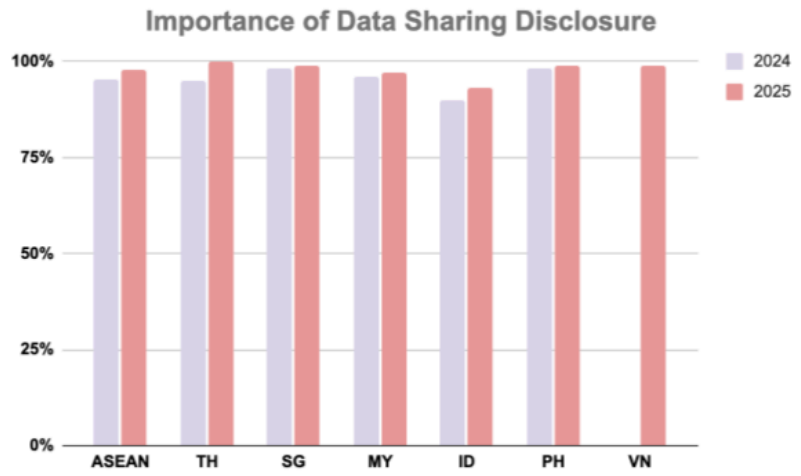


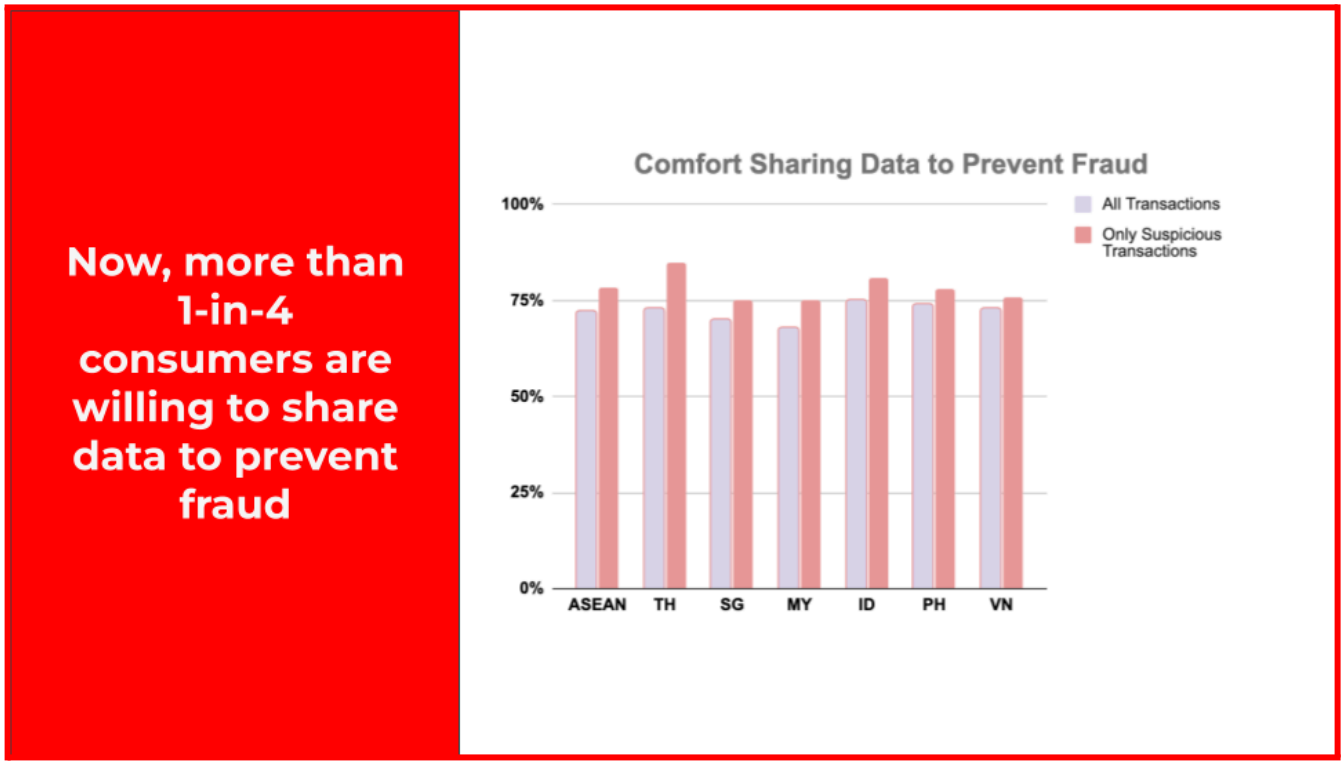
Exhibit 16: Data disclosure - When you do share data

Data Sharing disclosure importance continues to rise



Comfort with protective signal-sharing remains strong, and it gets stronger when it's purpose-limited. Across ASEAN, about seven in ten (72%) are comfortable with providers using minimal signals at transaction time to stop fraud; that climbs to 78% when sharing is done only on suspicious transactions (+6pp). The pattern is broad-based across all countries, providing a significant and largely untapped opportunity for companies to utilise external industry data signals in reducing fraud while being mindful of privacy, data sharing, and disclosure.

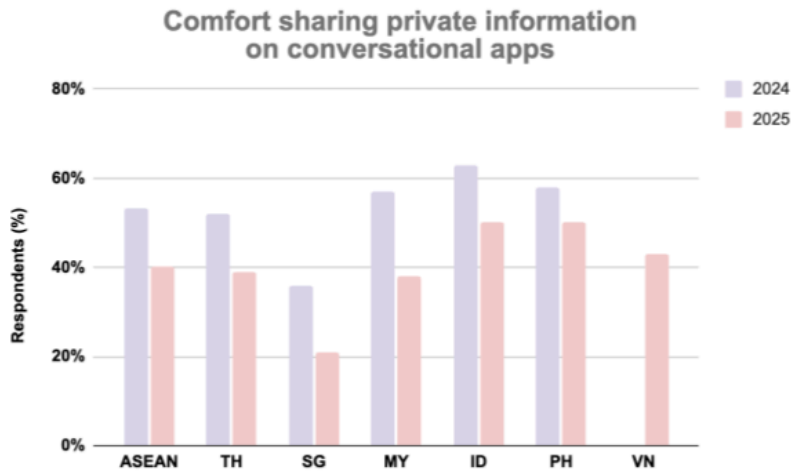
Exhibit 17: Data sharing - Sharing with a purpose



Given that many scams are occurring across messaging apps, we are seeing consumers decline in comfort with sharing personal data on these platforms. Despite the decline, still 40% of people feel moderately to very comfortable sharing personal data across these platforms. This creates a unique issue for conversational apps, most of which encrypt conversations and cannot therefore identify fraud attempts. For this reason, it is important to work on digital-ID verification that will enable people to verify they are dealing with a trusted entity and create low-friction paths to transactions that occur outside of the encrypted environment.

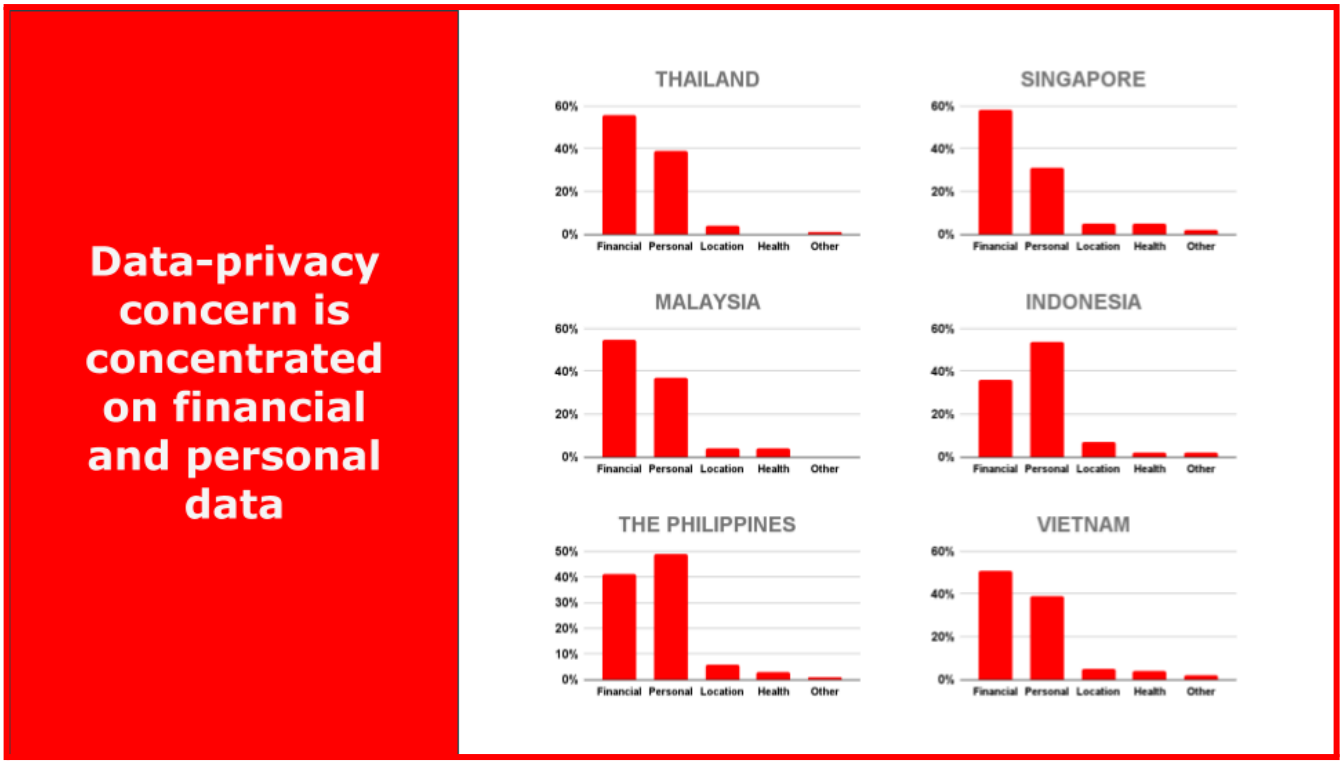
Exhibit 18: Personal data on conversational apps - Are people engaging in risky behaviour?

Comfort with sharing private details on conversational platforms has fallen sharply



When asked to choose which data they were most concerned about protecting, consumers overwhelmingly indicated that financial data was their top concern (49%) and personal identity and contact data was their second concern (42%); other categories were distant concerns, including location (5%) and health (3%). The pattern is broad and uniform, although it is unclear which of the financial vs. PII flips between markets. This suggests that consumers differentiate significantly between the types of data they would share, and this should be taken into account when designing systems. There is an opportunity for greater inclusion of data consumers are more willing to share, and strict controls and communication on those to which they are sensitive are aimed at keeping all of their data safe.

Exhibit 19: Concern over data types - What are people afraid of sharing



Opportunities for mobile network operators

MNOs are uniquely positioned to reduce deceptive practices without exposing broad data. The priority is outcome-based signals that strengthen authentication, deter takeover and guide safe behaviour, implemented with due diligence, audited internal controls, and clear guardrails.

Harden the hot routes

Focus on the channels that matter most: voice and OTT voice/messaging. Expand verified caller display and screening on risky calls; tighten SMS sender-ID regimes to counter impersonation; scale takedown and escalation pathways with social platforms for pattern recognition of suspicious activity. The goal is to reduce the chances for social engineering to succeed.

Focus and gain ground on easy wins

Default prompts for 2FA/authenticator and “official call-back only” behaviours reduce identity theft and account takeover. A near-term opportunity is SIM-swap / number-binding checks at high-risk moments to reduce false positives for banks and wallets at moments of high risk but significant opportunities to scale beyond.

Share signals with guardrails

Keep data purpose-limited and transparent, for example, device/SIM change status at the time of a risky transaction, or coarse location confidence for anomaly detection. Publish a short data use and retention note so customers and journalists can see the attribution, chain of custody, and remediation steps.

Turn reporting into resolution

With most victims already reporting, integrate bank, telco, platform and police workflows so customers see visible progress. Shorten the loop from report to forensic analysis to incident response. Share de-identified threat intelligence to improve fraud detection across the ecosystem.

Scaling detection with AI at the network edge

Mobile networks are starting to use AI-driven pattern recognition to spot emerging scam tactics in real time, at a scale that manual rules can’t match. Several operators in the region already run near-real-time anomaly detection with human-in-the-loop review, enabling rapid blocks and takedowns without inspecting message content. Early results include faster identification of impersonation bursts, detection of brand-new sender names before they’re widely abused, and cross-channel correlation that reveals coordinated campaigns. This will become increasingly critical as a means to scale and coordinate responses with the shifting tactics of scammers.

Country snapshots

Thailand (TH)

Thailand aligns with ASEAN on concern levels but stands out in terms of scale and where people turn. Victimisation is materially higher (+21pp YoY), with Voice (48%) and OTT (38%) being the primary routes, and LINE uniquely prominent (41%) among conversational apps, due to its high usage in the country. Police reporting is notably high, so case flow often starts in law enforcement rather than banks or platforms.

Acceptance of protective signals shows the biggest jump region-wide (73% to 85%), indicating strong public backing for sharing data to minimise and prevent growing fraud patterns.

Singapore (SG)

Singapore mirrors ASEAN in its support for minimal, purpose-bound checks and reporting, which is the region's strongest, typically bank-first approach, thereby tightening the handoff to recovery.

The contact mix is Voice (30%) and OTT (30%) with SMS (23%) and Social (21%) showing more broad channels than ASEAN averages. Perceived risk on Telegram (52%) and Facebook (58%) is high and aligned with ASEAN levels, so vigilance on conversational-app commerce is still warranted.

The comfort level of data sharing has increased on an exception basis (from 70% to 75%), reinforcing that the "use the minimum signals, only when needed" approach is comfortable for consumers.

Malaysia (MY)

Malaysia appears to align closely with ASEAN on overall concerns and willingness to share protective signals, but its reporting behaviour is more financial provider- and platform-centric than police-centric. The entry points skew towards OTT (52%) and Voice (40%), with Social

(34%) and SMS (25%) remaining active, implying hybrid playbooks rather than SMS-first approaches.

Malaysians are increasingly comfortable sharing with scope control (comfort increasing 68% to 75% on an exception basis) and show steady reporting, giving MY one of the better bases for measurable time-to-recovery improvements versus peers.

Indonesia (ID)

On most measures, Indonesia tracks the ASEAN picture: victimisation is up and people are broadly supportive of purpose-limited data sharing to stop fraud. The perception of risk is concentrated on Facebook and Telegram, a trend that is also consistent across the region.

Where ID differs is the channel mix and follow-through. Scams are even more mobile-first, with OTT (50%) and Voice (44%) both above the ASEAN average, and Social (36%) still material so multi-channel spillover is common. Reporting lags peers (a higher share of victims don’t report, compared with SG/TH), and victims lean less to banks and more to police/tech platforms.

Comfort in telcos sharing personal data rises from 75% to 81% when limited to suspicious transactions.

Philippines (PH)

The Philippines follows ASEAN on anxiety and support for tight, outcome-based controls, but diverges sharply on exposure and channels. It records the second-highest lifetime victimisation (52% vs ASEAN at 45%), and victims cite Social (48%) and SMS (37%) far more than Voice, an inversion of the regional pattern.

Facebook association is the highest (70%), and Telegram is also elevated (47%), consistent with regional averages; therefore, platform escalation is the critical chokepoint. Comfort with exception-based data sharing has increased (from 74% to 78%), but the shift in the mix means that sender-ID hygiene and social-platform enforcement are more effective than call controls.

Vietnam

This is the first time that Vietnam has been included in the survey.

Vietnam reports the highest level of scams experienced in total (56%) and also within the last 12 months (11% of respondents, compared to the ASEAN average of 8%). This indicates that scams and fraud are hitting this developing market the hardest of all markets measured in the survey.

It matches ASEAN on high concern and broad acceptance of purpose-limited checks, and the contact mix tilts to Voice (52%) with Social (35%) next (closer to ID/TH than to PH/SG).

Police reporting is relatively strong, while bank/platform routes are less consistent, which affects the speed of recovery.

Risk perception clusters around Facebook (64%) and Telegram (55%), as with the rest of the region.

Comfort with exception-basis sharing is positive (76%), suggesting room to introduce a range of transaction risk-based checks.

Conclusion and the path forward

The picture is consistent across the new analysis: scams are rising, they arrive through everyday mobile channels, and people expect visible protection without a privacy trade-off. The opportunity is to meet them where scams actually land (i.e., voice, OTT, social, and SMS) with controls that are targeted, transparent, and fast.

Start with the routes that matter. Make caller screening and verified senders routine, tighten SIM-change/number/device checks at login and payment, and push official call-back as the default habit. Use Digital Identity the way consumers accept it: minimal signals, only when risk is present, and with simple disclosures.

Close the trust–use gap on platforms. People buy on Social Media Platforms every week, despite rating it the least trusted environment; this combination increases exposure to impersonation and counterfeit goods. The fix is practical: better seller verification, faster takedowns, safer payments and clear dispute routes, plus a coordinated hand-off to banks when money moves. As crypto adoption grows to roughly 1 in 4 online adults, exchanges and wallets also need number binding and recent SIM change/device checks to reduce SIM-swap takeovers.

Scale detection to keep pace. Rule-based filters won’t keep up with real-time OTP relays and fast-moving impersonation. MNOs can lead with AI anomaly detection on network signals (call patterns, sender behaviour, device/SIM events), human-in-the-loop review, and privacy-preserving audit trails. That gives operators, banks, and platforms a shared view of emerging campaigns without requiring content inspection.

Finally, turn reporting into outcomes. Victims do report, but to different doors, banks, police, platforms and telcos, so cases stall. A “no-wrong-door” approach, with a single case ID, standard data fields, and agreed-upon time-to-first-response and funds-recovery SLAs, will shorten resolution times and rebuild confidence. Consumers are ready to reward this: a large majority say they will switch to a provider offering better security. The organisations that make protection obvious, accelerate recovery, and explain their data use in plain language will reduce losses, limit liability, and win market share.

Consumer survey methodology

The insights in this report are based on two cross-sectional online surveys of adults (18 years and above) in ASEAN markets. Wave 1 (2024) covered Indonesia, Malaysia, Philippines, Singapore and Thailand (n≈500 per market). Wave 2 (2025) repeated these markets and added Vietnam as a baseline (n≈500–520 per market). Fieldwork was conducted in local languages via self-administered CAWI (computer-assisted web interviewing) using reputable access panels. The research focuses on scams, fraud exposure and consumer protection behaviours (e.g., channels, reporting, recovery, comfort with protective signal-sharing).

To achieve national representativeness in each market, non-interlocking quotas were applied at recruitment:

- Age × gender
- Region/state (and urbanicity where applicable)
- Socio-economic class/household income (market-appropriate measures)

Interviewing adhered to local norms and privacy laws. Respondents gave informed consent; data were anonymised and handled in line with GDPR/PDPA principles.

Sample sizes and reporting. Each market targeted ~500 completes per wave (2025 ranges TH 508, SG 501, MY 506, ID 515, PH 501, VN 517). We report unweighted percentages with base sizes. ASEAN aggregates are equal-weighted across included markets and recomputed per exhibit when a market is excluded for non-comparability (e.g., VN not in 2024 YoY).

Question formats. The instrument combined single-select, multi-select and Likert-type items. Unless noted, Likert results are shown as Top-2 box. Victim impact and recovery metrics are calculated based on the experiences of victims only. Multi-select channel questions reflect all appropriate answers.

Statistical testing and confidence. Year-on-year and cross-market differences were tested at 90% confidence. For quota (non-probability) samples, confidence intervals are indicative; at

n≈500, the worst-case 90% margin is ±3.7pp per country. Equal-weighted ASEAN aggregates have tighter bounds (≈±1.4–1.5pp). Subgroup estimates (e.g., victims) have wider intervals.

Quality controls. The study applied standard panel QA, including device and geo checks, duplicate detection, time-on-task thresholds, attention/consistency checks, and removal of low-quality cases before analysis.

Limitations. As an online survey, coverage of populations with limited internet access may be lower; rare or highly sensitive behaviours may be under-reported. These risks were mitigated through quota controls, local language instruments, and neutral wording. Full technical details (fieldwork windows, incidence, exclusion rates) are available on request.