GASA
Global Anti-Scam Alliance

BioCatch

SCAMADVISER

State of Scams in Southeast Asia

2025 REPORT

INSIGHTS

LEARN MORE

63% of Southeast Asian adults experience a scam, 1 in 5 lost money

Jorij Abraham
MANAGING
DIRECTOR
GASA
Global Anti-Scam Alliance

About GASA

The Global Anti-Scam Alliance (GASA) is a non-profit organization whose mission it is to protect consumers worldwide from scams. We realize our mission by bringing together policy makers, law enforcement, consumer authorities, NGOs, the financial sector, telecom operators, internet platforms and service providers, cybersecurity and commercial organizations to share insights and knowledge surrounding scams. We build networks in order to find and implement meaningful solutions.

This study of 6,000 Southeast Asian adults reveals that 63% of them claim to have had a scam experience in the last 12 months, with scams more prevalent in Vietnam and Malaysia. Two thirds of scams happen within a day of first being contacted by the scammer, highlighting the speed with which scams are carried out.

Many Losses Go Unreported

Just over one fifth of Southeast Asian adults have had money stolen by scammers in the last 12 months. These scam payments are commonly made via wire transfer (48%) and digital / e-wallet (36%) .However, just under three quarters of those who have lost money to scams, have reported the loss to the payment service used and only 22% were able to at least partially recover their money. 18% of those who have experienced a scam did not report it to anyone, mainly in Thailand (25%) and Malaysia (23%), with the main barriers driven by a perceived lack of importance or responsibility (47%) and practical barrier from reporting (46%).

With Scams Affecting More Than Finances

In Southeast Asia, the effects of scams goes beyond financial impact. Just under two thirds found the scam experience very or somewhat stressful, with 44% saying the scam experience had a significant / moderate impact on their mental wellbeing. However, over half say they are now more vigilant of scams as a result of their experience.

By Reaching Scam Victims Through Multiple Channels

Almost four fifths of Southeast Asian adults have been exposed to a scam in the last 12 months, with the most common scam encounters occurring in Vietnam and Malaysia. 11% encounter a scam at least once a day, rising to nearly a fifth in the Philippines. The most common communication channels used by scammers in Southeast Asia are phone calls (62%), text /SMS messages (56%) and instant messaging apps (49%). Seven in ten of those encountering scams have reported it at least once, however, only half recall action being taken by the platform.

Due To Ineffective Vigilance Methods

94% of Southeast Asian adults take at least one step to verify if an offer is legitimate. However, many rely on methods that have lower effectiveness such as following the rule “if it seems too good to be true, it probably is” (32%) and checking for the presence of a phone number (30%). Over a third of Southeast Asian adults look to public service organizations to keep them safe from scammers, particularly, the government (16%).

Highlighting That Confidence Does Not Prevent Scam Victimization

Although majority of Southeast Asian adults (78%) feel confident in their ability to recognise scams, just under two thirds have still experienced a scam. This highlights the persistent prevalence of scams in Southeast Asia and the importance of using more effective methods of vigilance in the future.

GASA Global Anti-Scam Alliance · BioCatch · SCAMADVISER

From Crisis to Coordination: Let's Stop Southeast Asia's Scam Surge Together

Boice Lin
CHIEF BUSINESS OFFICER
SCAMADVISER

About ScamAdviser

ScamAdviser is a global leader in AI-powered scam prevention, protecting businesses and individuals in real time. Our Anti-Scam Intelligence platform can protect users from untrustful websites, messages, and calls. Stopping scammers before they strike. Trusted by 400+ partners and used by over 1 billion people worldwide, ScamAdviser turns data into decisive action—so you can stay safe, stay ahead, and stay in control.

Across Southeast Asia, scams have grown into a multi-billion-dollar crisis, now accelerating at a pace we've never seen before, driven in large part by the rise of generative AI. Scammers are using AI to craft highly convincing messages, impersonate trusted sources, and launch attacks with unprecedented speed and scale.

Scams Are Faster and Smarter, Attacking Through Trusted Channels

Scams feel more real, move faster, and are harder to detect. In the past 12 months alone, Southeast Asians lost an estimated US$23.6 billion to scams. Nearly 1 in 4 adults (22%) report losing money to scammers last year.

These threats arrive through the very channels meant to connect us: phone calls, SMS, WhatsApp, and other messaging apps. A message might appear to come from your bank, a telecom carrier, or even a loved one. But behind it may be an impersonator, or a fraudster with a cloned identity and a well-practiced script.

From Awareness to Action: The Responsibility of Anti-Scam Ecosystems

The good news is that people are paying attention, 94% of Southeast Asians report taking at least one step to verify the legitimacy of suspicious contacts. But despite their efforts, many still fall victim. The reason is simple: scams today are sophisticated, realistic, and often too attractive to resist. Instinct and experience are no longer enough to stay safe.

This is where real-time, data-driven identification becomes essential, recognizing scam threats the moment they appear, whether through a phone call, a message on a platform, or during a financial transaction. Those at the front lines are telecom operators, platform providers, and banks, those with both the greatest responsibility and the clearest opportunity to take action and protect users.
But this responsibility must be shared. According to the report, over one in three people expect governments to take the lead, while another third place the responsibility on businesses or themselves. Scams are no longer isolated incidents, they are part of a sophisticated crime ecosystem. Stopping them requires the same level of coordination and scale: governments, banks, telecom providers, digital platforms, and solution providers all have a role to play.

Our Approach: Data, Technology, and Partnerships in Sync

Our mission is simple: collaborate to fight scams. Powered by the world's largest scam database and advanced AI, our solutions like Anti-Scam Intelligence (ASI) and the Impersonation Solution are already protecting over 1 billion users. We work with governments to monitor impersonation and remove scam ads. We help banks spot abnormal accounts in real time. We enable telecoms and tech platforms to detect suspicious numbers and links before harm occurs. No single entity can solve this alone, but together, we can. By aligning incentives, sharing intelligence, and acting collectively, we can build a safer digital future, one where trust isn't the price of progress.

GASA Global Anti-Scam Alliance · BioCatch · SCAMADVISER

Scam crisis: Cases have surged, and banks must take notice

Subhashish Bose
DIRECTOR GLOBAL ADVISORY
BioCatch

About Biocatch

BioCatch prevents financial crime by recognizing patterns in human behavior. Today, more than 30 of the world's largest 100 banks and 287 total financial institutions deploy our solutions, analyzing 16 billion user sessions per month and protecting 532 million people around the world from fraud and financial crime. Fraud is incessant, pervasive, and ever-evolving. It's relentless. And that's why, at BioCatch, we fight to make banking safer every day.

Over the past decade, Southeast Asia has experienced remarkable economic growth, with a rising middle class and rapid urbanization fueling consumer affluence. By 2030, the region is projected to add more than 100 million new middle-income consumers, many of them young and digital-first.

This consumer shift has triggered an aggressive expansion in digital banking and payments. Mobile banking penetration in Thailand is at 74% of internet users, while Singapore's digital payment adoption is near-universal. The Philippines' digital payments volume leads with 59% market share by value, and Indonesia has been ranked No. 8 in the world's top 10 fastest-growing payments markets.

While digital banking and real-time payments offers consumers much-wanted accessibility, speed, and convenience, it also increases their risk. Cybercriminals exploit the same connectivity and convenience that empowers retail customers.

Regulators and law enforcement agencies have intensified their response to this surge by introducing measures like mandating security checks, device binding, and other bank-side impediments. However, fraudsters have been quick to adapt, evolving their strategies to psychologically manipulate consumers by using emotions like fear, trust and greed.

Almost half the people surveyed in this report believe banks should always be responsible for reimbursing those who fall victim to a scam. Echoing with this sentiment, regulations like the Shared Responsibility Framework in Singapore and Thailand and AFASA guidelines in Philippines have recommended mandatory deployment of real-time scam surveillance systems by banks, failing which they may be liable to reimburse the customer.

AI- and machine-learning-driven behavioral intelligence offers a powerful tool to banks to detect and stop scams before any money leaves the would-be-victim's account. By continuously learning each consumer's behavior patterns, these models can detect if a person is under stress, distracted, or being actively coached, by spotting subtle variations in things like typing cadence, navigation patterns, and other session activity.

For many financial institutions, scam-related losses can balloon into millions of dollars, with some banks already compensating victims under regulatory mandates. Operational costs also rise sharply from increased investigations, dispute handling, and customer support workloads.

Indirectly, damage to brand and customer confidence can be even more costly. Once a bank is perceived as unsafe, customers migrate to competitors with stronger security reputations. There's also the risk of heightened regulatory scrutiny, penalties, and more restrictive compliance obligations if incidents persist.

As such, banks in Southeast Asia should take note of the findings and understand that proactive fraud and scam-detection is no longer just about reducing losses but, rather, is an essential driver of their business.

GASA Global Anti-Scam Alliance · BioCatch · SCAMADVISER

The Global research surveyed 46,000 respondents across 42 markets Globally – this report focuses on the findings from 6 Southeast Asian markets

Southeast Asian markets surveyed | Sample size

Thailand | **1000**

Indonesia | **1000**

Malaysia | **1000**

Singapore | **1000**

Vietnam | **1000**

Philippines | **1000**

GASA Global Anti-Scam Alliance BioCatch SCAMADVISER

Who we spoke to in Southeast Asia

Sample size | 6000 people

Audience | Adults aged 18+ living in each market

Quotas | Quotas were used throughout fieldwork to ensure the sample was nationally representative of the adult population in each market on age, gender and region

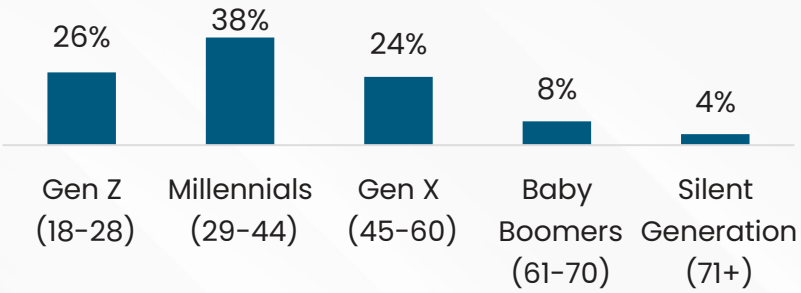
Weighting | Nationally representative of adult population in each market

Methodology | 15-minute online survey

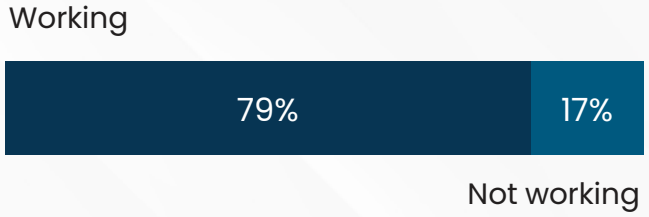
Sample source | Online research panel

GENDER

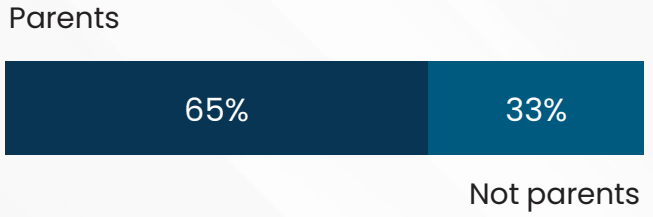
GENERATION / AGE



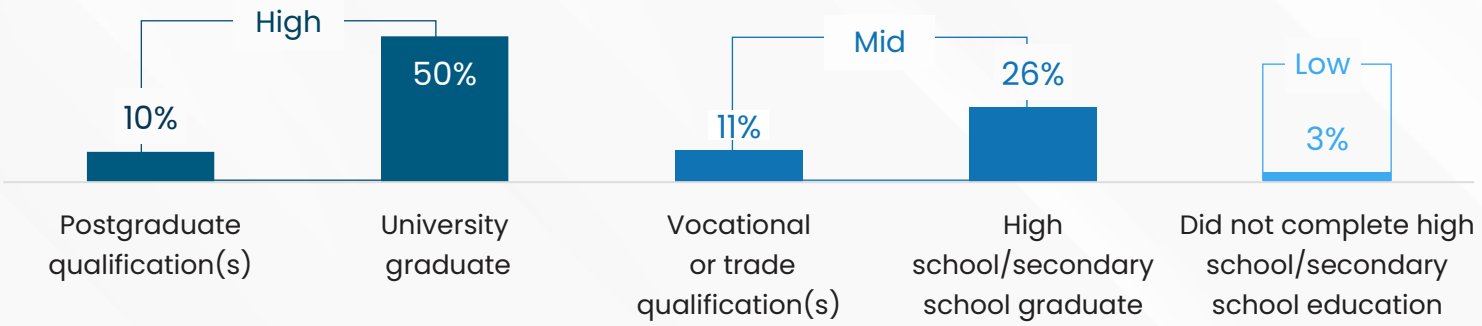
WORKING STATUS



PARENTAL STATUS



EDUCATIONAL STATUS



Base: All respondents Southeast Asia (6,000)

GASA Global Anti-Scam Alliance | BioCatch | SCAMADVISER

Key Southeast Asia findings

PREVALENCE OF EXPERIENCING A SCAM IN LAST 12 MONTHS*

63%

Of **Southeast Asian** adults claim to have had a scam experience in the last 12 months*

Amongst this group, **Investment scam** (63%) is the most common type of scam experienced

*An experience, whether successful or not for the scammer

PREVALENCE OF LOSING MONEY TO SCAMS IN LAST 12 MONTHS

22%

Of **Southeast Asian** adults went on to have money stolen by scammers in the last 12 months

This rises to 32% and 31% in Malaysia and the Philippines respectively

VALUE LOST TO SCAMS

$660

Has been lost to scams, per person, on average in **Southeast Asia** in the last 12 months

Funds are most commonly sent via Wire or bank transfer (**48%**) and digital / e-wallet (**36%**)

PREVALENCE AND OUTCOME OF REPORTING TO PAYMENT PROVIDER

73%

Of **Southeast Asian** adults who were scammed did report the scam to the payment service

However, only **22%** were able to at least partly recover the money

IMPACT OF SCAMS ON VICITM

62%

Of **Southeast Asian** adults who were scammed felt very or somewhat stressed by the experience

52% say they will be more vigilant of scams as a result

PERCEIVED RESPONSIBILITY TO PROTECT PEOPLE FROM SCAMS

37%

Of **Southeast Asian** adults feel it is the responsibility of **Public service organisations** to keep people safe from scammers, primarily the government (**16%**)

The research covered the following key topics

Throughout the report, you can click the 'Home' icon to return to this page

SCAM PREVALENCE

How many people experience scams? What are the most common scam types experienced? And what is the value stolen by scammers?

EXPERIENCE OF BEING SCAMMED

How frequently do scams occur? Which payment channels are used to send funds?

SCAM REPORTING

Are scams reported? If so, what are the outcomes of reporting scam encounters? If not, what are the barriers?

SCAM IMPACT

What impact do scams have on victims' lives, stress and wellbeing?

PREVALENCE OF SCAM ENCOUNTERS

How frequently are scams encountered? And on what platforms?

SCAM PREVENTION

What' self-prevention tactics to consumers use to identify scams? How are public and commercial organisations' seen in their responsibility and performance in preventing and resolving scams?

Click to navigate to sections

ABOUT THE REPORT

ABOUT THE AUTHORS

To find out more about the report and its authors

Scam prevalence

How many people experience scams? What are the most common scam types experienced? And what is the value stolen by scammers?

GASA Global Anti-Scam Alliance
BioCatch
SCAMADVISER

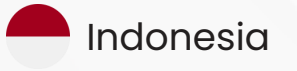
63%

of Southeast Asian adults claim to have had a scam experience in the last 12 months

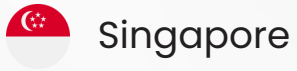
Scam experiences are more prevalent in Vietnam and Malaysia

Prevalence of experiencing a scam in last 12 months


60%
Thailand


35%
Indonesia


73%
Malaysia


66%
Singapore


77%
Vietnam


65%
Philippines

Q8. Have any of the following scams happened to you in the last 12 months? Base: All respondents Southeast Asia (6000), Thailand (1000), Indonesia (1000) Malaysia (1000), Singapore (1000), Vietnam (1000), Philippines (1000)

“Friction for fraud” needs to be the industry norm

Ken Yon Kian Guan
SENIOR DIRECTOR RISK & COMPLIANCE DIVISION

PayNet

About PayNet

Payments Network Malaysia is Malaysia's premier payments network and central infrastructure for financial markets.

We innovate, build and operate world-class payment systems and financial market infrastructures that safely, reliably and efficiently enable the functioning and development of Malaysia's financial system as well as the economy as a whole.

Real-time transfers and payments have made moving money faster than ever, but for scammers, this increasing speed and reach are their greatest allies.

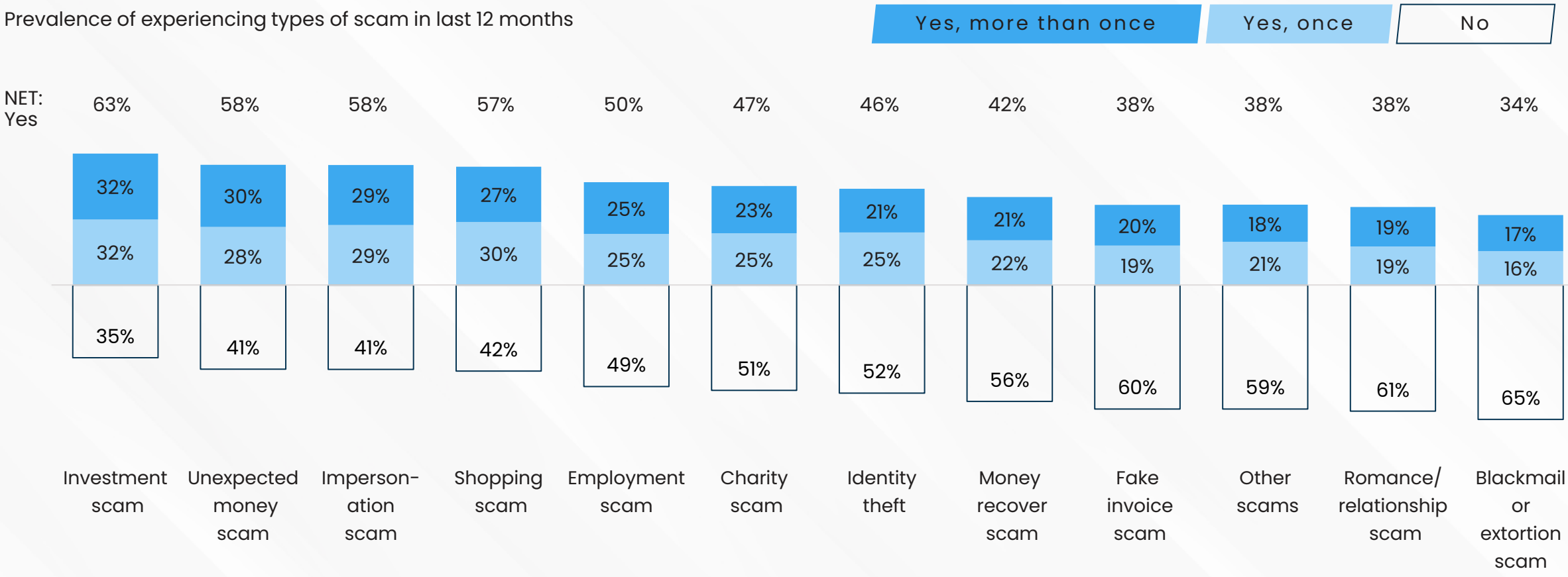
The scam threat has outgrown borders. What begins as a phone call in one country can lead to fraudulent transfers routed through multiple institutions and countries in minutes. In Malaysia, we’ve seen mule accounts span across domestic and overseas institutions and networks, making recovery exponentially harder.

This is no longer just a national challenge, it is a growing regional problem. Prevention and education must adapt to this reality. We must embed real-time risk signals into the payment journey itself, deliver contextual warnings when a transaction looks unusual, and empower frontline systems and responders to act within seconds. And because scams do not respect borders, regulators, payment operators, and financial institutions must be willing to share data, align procedures, and coordinate rapid responses across jurisdictions.

We need to make “friction for fraud” the industry norm. Fast enough for legitimate commerce, but never faster than our collective ability to intercept a scam.

Investment, unexpected money & impersonation scams are the most experienced scam type in Southeast Asia, affecting over half of victims

Prevalence of experiencing types of scam in last 12 months



Q8. Have any of the following scams happened to you in the last 12 months? Base: All Southeast Asian respondents who have been contacted by scammers (3916)

Click here to review full scam descriptions seen by respondents within the survey

Fraudsters employ various methods to deceive Southeast Asian consumers

Scam victim description of experience

"The most recent scam I've encountered is probably one where someone goes to Facebook to ask for work to do at home, but it's a scam to get them to invest through an app by signing up and following up."

Employment scam, Thailand

"Initially they gave me directions to follow several accounts on social media then they paid me, over time they asked me to invest a certain amount to get quite large returns"

Investment scam, Indonesia

"Employment scam where I was offered an attractive position. Once hired was requested to operate a foreign bank account with large initial deposit before I could be paid."

Employment scam, Malaysia

"Pay money to receive a bigger sum, actually received it first few times but had to pay a bigger amount to withdraw my balance"

Unexpected money scam, Singapore

"I was called to pay for a product I didn't buy, the scammer said it was my account and I transferred the money to them"

Shopping scam, Vietnam

"I was scammed in an investment that made me expect to earn a lot but when I made a deposit I was suddenly blocked"

Investment scam, Philippines

Q9. Please describe the scam you experienced in the last twelve months. Base: All Southeast Asian respondents who have been scammed (3896)
NB: The scam type noted is the respondent's understanding of the type of scam they experienced

22%

of Southeast Asian adults went on to have money stolen by scammers in the last 12 months

Funds lost due to scam activity are particularly prevalent in Malaysia and the Philippines

Prevalence of losing money to a scam in last 12 months

14% ↓	14% ↓	32% ↑
Thailand	Indonesia	Malaysia
21%	20%	31% ↑
Singapore	Vietnam	Philippines

Q13. In the last 12 months, in total, how much money did you lose to scams? Please include the total amount of money lost, regardless whether you managed to partially or fully recover it. Base: All respondents Southeast Asia (6000), Thailand (1000), Indonesia (1000) Malaysia (1000), Singapore (1000), Vietnam (1000), Philippines (1000)

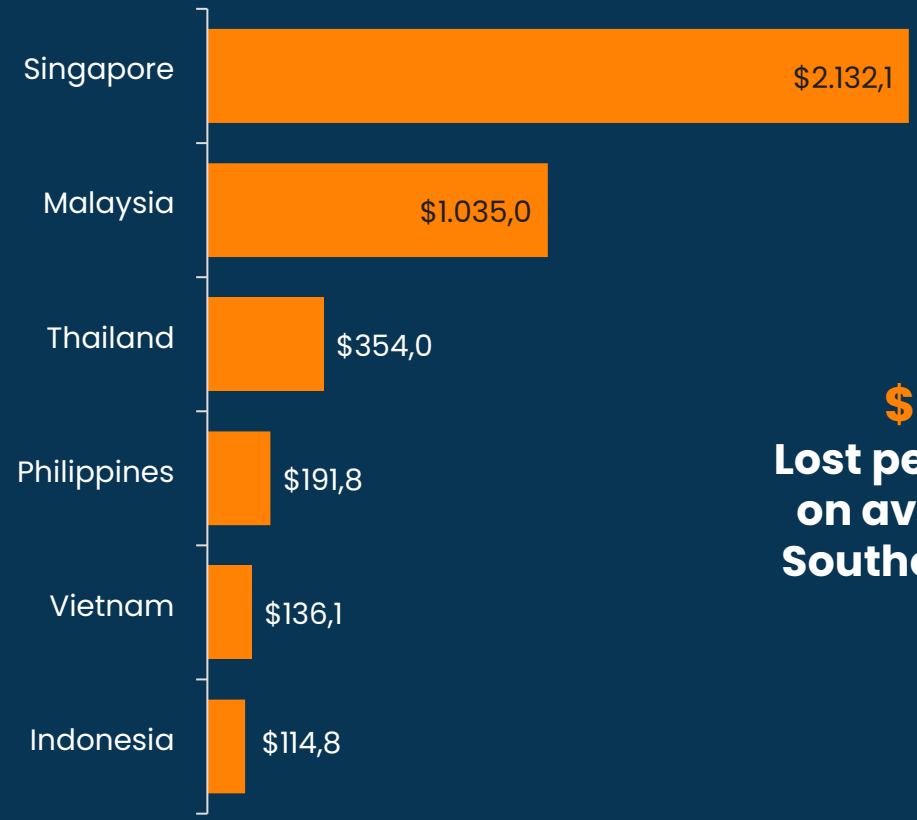
An estimated $23.6 Billion has been lost to scams in Southeast Asia in the last 12 months

Value lost to scams

Q13. In the last 12 months, in total, how much money did you lose to scams? Please include the total amount of money lost, regardless whether you managed to partially or fully recover it.
Base: Southeast Asian adults who lost money (1319)

Those in Singapore lose the most funds per person on average, followed by Malaysia

Southeast Asia average lost per person



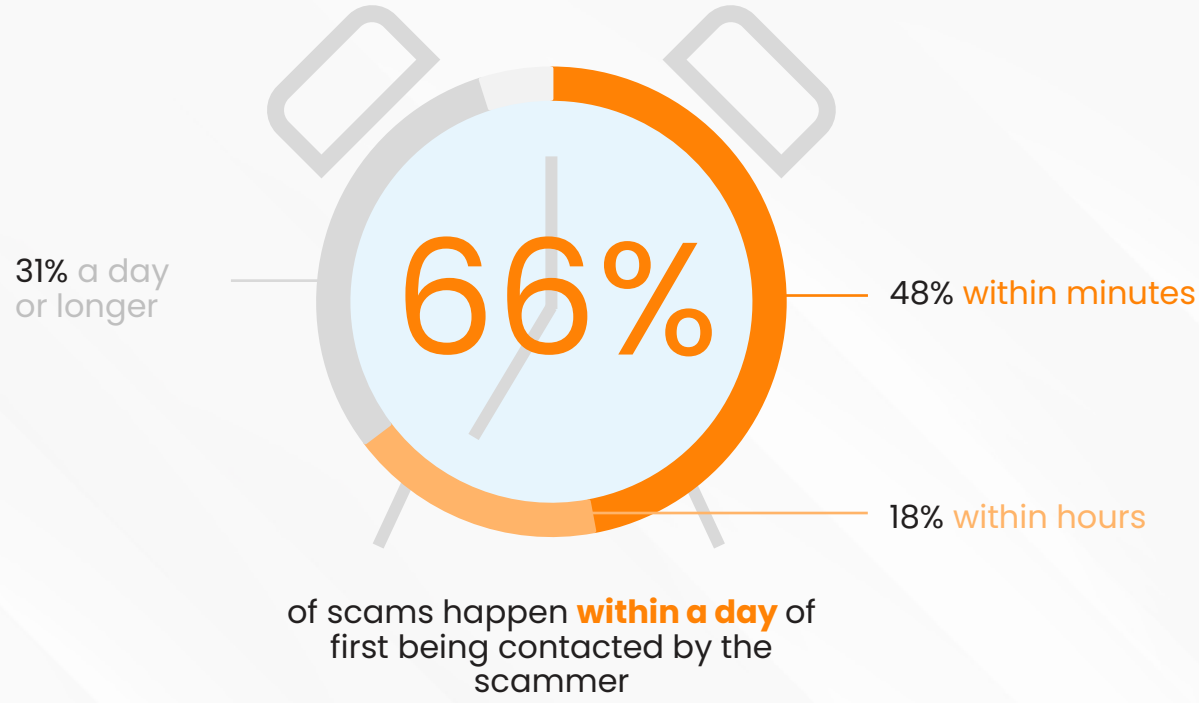
$660
Lost per person, on average in Southeast Asia

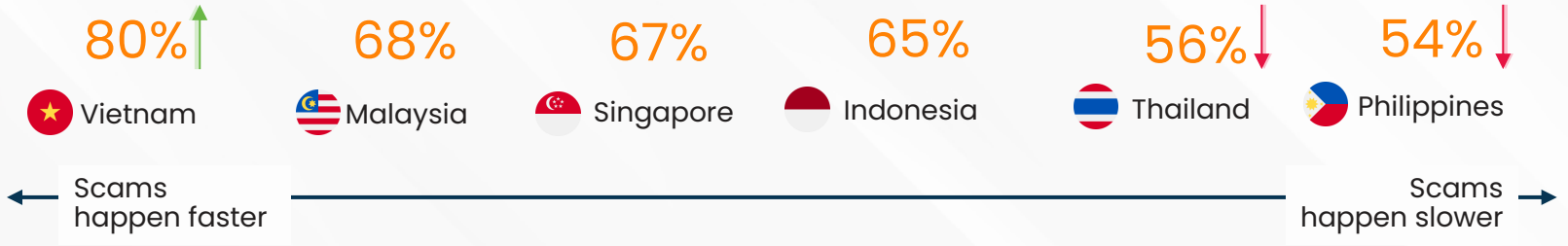
Experience of being scammed

How frequently do scams occur? Which payment channels are used to send funds?

In Southeast Asia, two thirds of scams happen within a day of first being contacted by the scammer

Proportion of scams that happen within a day

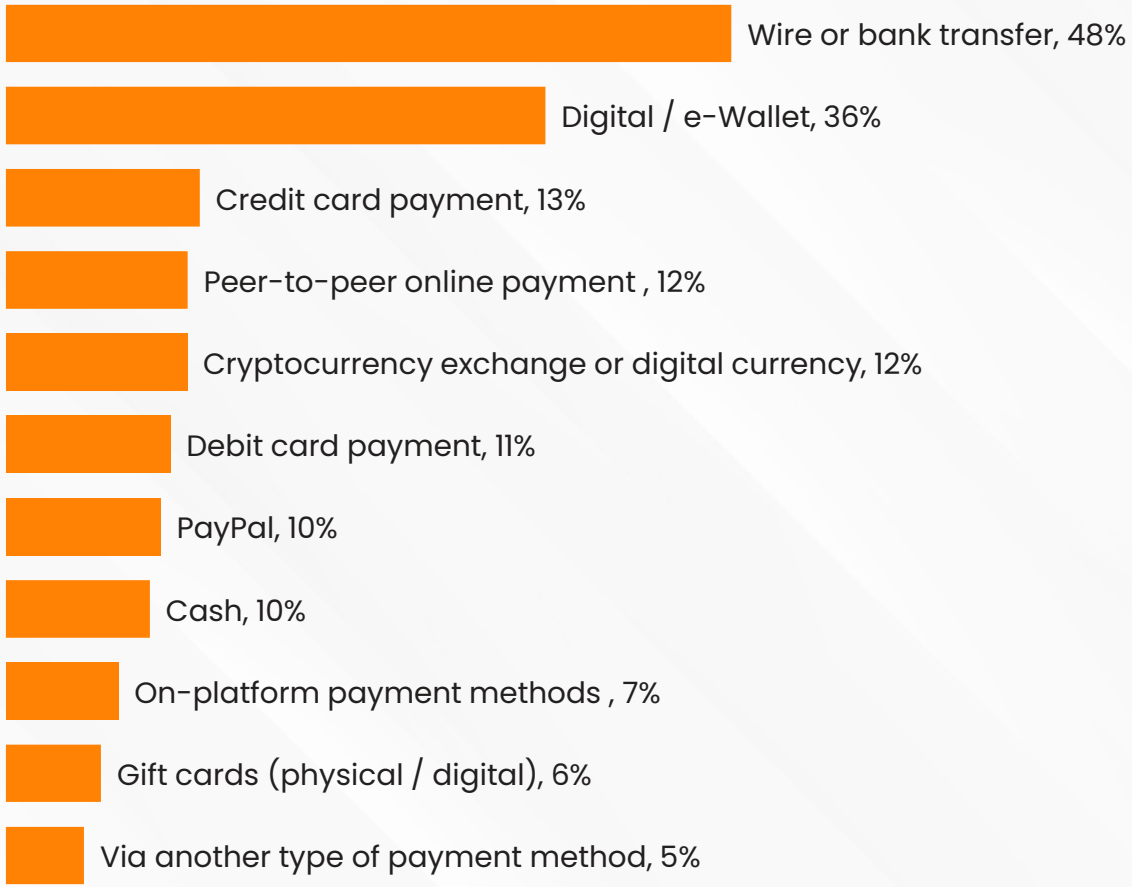




Q10. Thinking about the most recent time you were scammed, how long did it last? Please think about from the first time you heard from the scammer until the last time you were in contact with the scammer. Base: All Southeast Asia respondents who have been scammed (3896), Thailand (621), Indonesia (358) Malaysia (734), Singapore (685), Vietnam (810), Philippines (688)

Scam payments in Southeast Asia are mainly made via wire transfer, except in the Philippines, where digital / e-wallets are more common

Payment channels scammers received the payment



	Thailand	Indonesia	Malaysia	Singapore	Vietnam	Philippines
Wire or bank transfer, 48%	73%	65%	55%	36%	70%	14%
Digital / e-Wallet, 36%	21%	43%	22%	20%	21%	74%
Credit card payment, 13%	10%	5%	20%	26%	9%	4%
Peer-to-peer online payment , 12%	12%	3%	14%	10%	27%	5%
Cryptocurrency exchange or digital currency, 12%	7%	6%	18%	15%	13%	8%
Debit card payment, 11%	7%	9%	17%	19%	4%	6%
PayPal, 10%	5%	5%	12%	15%	9%	10%
Cash, 10%	14%	6%	10%	8%	9%	10%
On-platform payment methods , 7%	7%	3%	11%	6%	9%	6%
Gift cards (physical / digital), 6%	8%	4%	10%	8%	6%	1%
Via another type of payment method, 5%	2%	7%	11%	3%	1%	5%

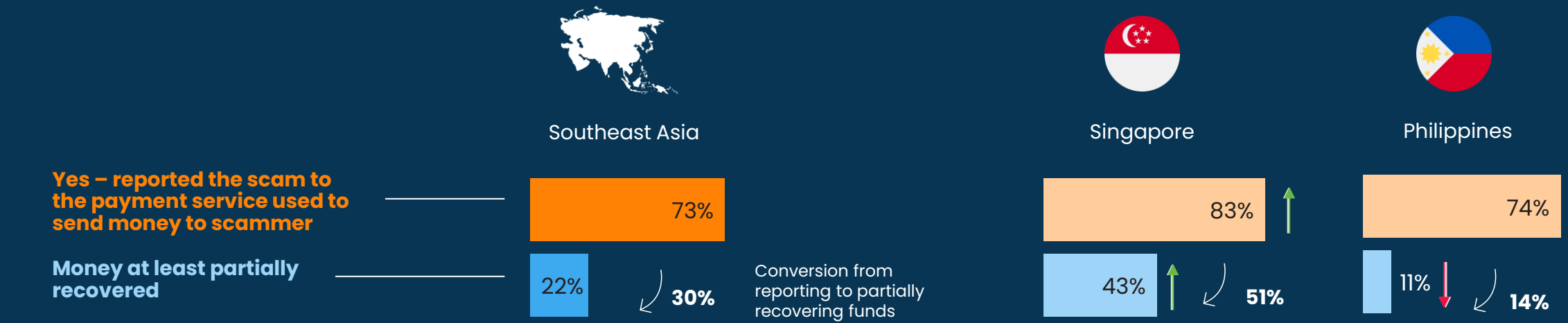
Q14. How did the scammer receive your money? Base: All Southeast Asia respondents who have been scammed and lost money (1340), Thailand (159), Indonesia (144) Malaysia (293), Singapore (206), Vietnam (229), Philippines (309)

Scam Reporting

Are scams reported? If so, what are the outcomes of reporting scam encounters? If not, what are the barriers?

Just under three quarters of those losing money to scams in Southeast Asia reported the loss to the payment serviced used. Only 22% were able to at least partially recover their funds

Prevalence of reporting scams to payment provider & if money was at least partially recovered

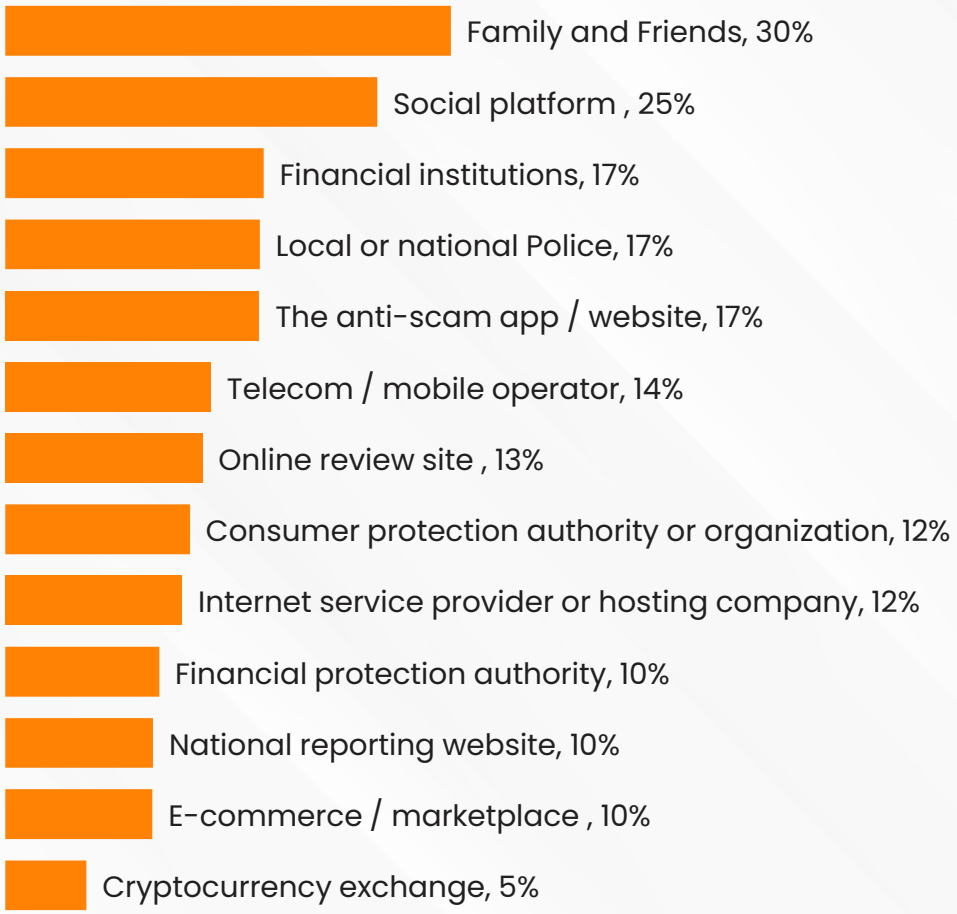


Reporting and financial recovery are more common in Singapore, whereas those in the Philippines are less likely to recover even part of their losses

Q15. Did you report the scam to the payment service that was used to send your money to the scammer? Base: All Southeast Asia respondents who have been scammed and lost money (1340), Singapore (206), Philippines (309)

Overall, scams are reported to the greatest variety of channels in Vietnam and Malaysia

Channels / organisations scams reported to



	Thailand	Indonesia	Malaysia	Singapore	Vietnam	Philippines
Family and Friends, 30%	23%	32%	24%	18%	43%	36%
Social platform , 25%	23%	22%	25%	19%	28%	30%
Financial institutions, 17%	17%	16%	21%	27%	14%	9%
Local or national Police, 17%	12%	13%	27%	20%	19%	7%
The anti-scam app / website, 17%	16%	18%	14%	22%	17%	14%
Telecom / mobile operator, 14%	16%	13%	11%	8%	17%	16%
Online review site , 13%	10%	15%	14%	9%	12%	19%
Consumer protection authority or organization, 12%	13%	10%	18%	8%	14%	10%
Internet service provider or hosting company, 12%	10%	10%	13%	9%	12%	15%
Financial protection authority, 10%	8%	9%	16%	8%	11%	7%
National reporting website, 10%	7%	12%	11%	12%	9%	10%
E-commerce / marketplace , 10%	10%	2%	12%	9%	15%	6%
Cryptocurrency exchange, 5%	4%	3%	5%	4%	10%	4%

Q21. Who did you report the scam to? Base: All Southeast respondents who have been scammed (3896), Thailand (612), Indonesia (358) Malaysia (734), Singapore (685), Vietnam (810), Philippines (688)

18%

of Southeast Asian adults experiencing a scam in the last 12 months did not report it to anyone

Those in Thailand and Malaysia were more resistant to reporting their scam

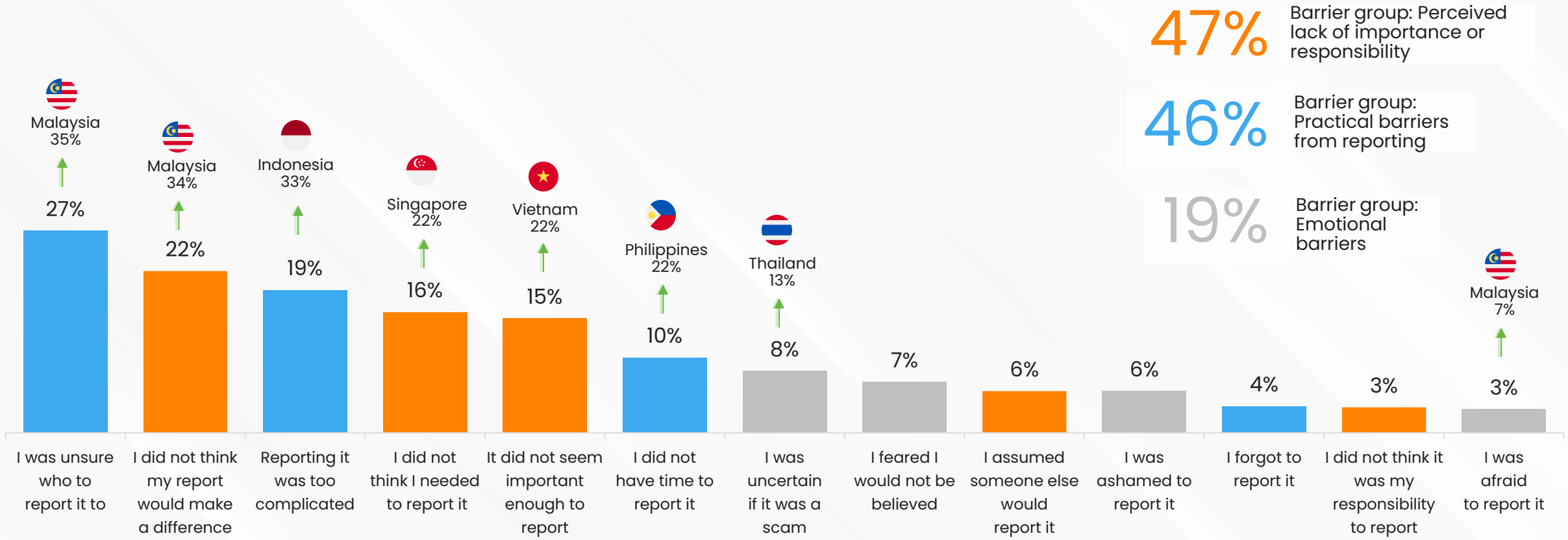
Prevalence of not reporting scams in the last 12 months

25% ↑	20%	23% ↑
Thailand	Indonesia	Malaysia
17%	13% ↓	13% ↓
Singapore	Vietnam	Philippines

Q21. Who did you report the scam to? Base: All Southeast respondents who have been scammed (3896), Thailand (612), Indonesia (358) Malaysia (734), Singapore (685), Vietnam (810), Philippines (688)

Barriers to reporting scams in Southeast Asia are primarily driven by a perceived lack of responsibility or a functional reason

Barriers to reporting scams – top 6



Q22. Why didn't you report the scam? Base: Southeast Asia respondents who did not report the scam (690), Thailand (130), Indonesia (72) Malaysia (164), Singapore (118), Vietnam (102), Philippines (104)

Scam Impact

What impact do scams have on victims' lives, stress and wellbeing?

In Southeast Asia, the impact of scams is both financial and emotional and over half say they are more vigilant of scams as a result of their experience

Impact of scams on victim and family

69% At least one Emotional impact

- 52% More vigilant of scams
- 32% More distrustful of digital tools and platforms
- 19% Drop in confidence and second guessing myself
- 15% Heightened tension and stress in family unit

15% At least one Relationship impact

- 11% Blaming the victim for being careless
- 6% Break down relationships (divorce, fewer friends, etc.)

40% At least one Financial impact

- 18% Reduce normal spending behaviour
- 11% Reduced access to credit
- 11% Take on additional debt or loans
- 10% Unable to pay for basic essentials (rent, utilities, groceries, etc.)
- 8% Relatives and friends required to step in financially to support
- 8% Making additional costs (e.g., legal support, counselling)
- 7% Affect impact life milestones (buy a home, education, etc.)
- 5% Having to sell assets (car, house, etc.)

18% N/A: The scam(s) had no impact on me or my family

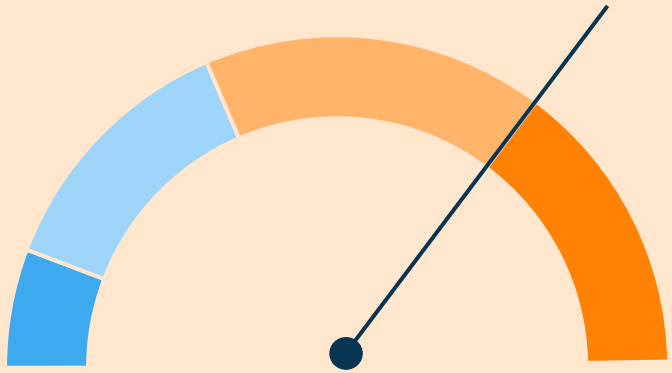
Q18. How has the scam(s) impacted you and your family? Base: All Southeast Asia respondents who have been scammed (3896), Thailand (612), Indonesia (358) Malaysia (734), Singapore (685), Vietnam (810), Philippines (688)

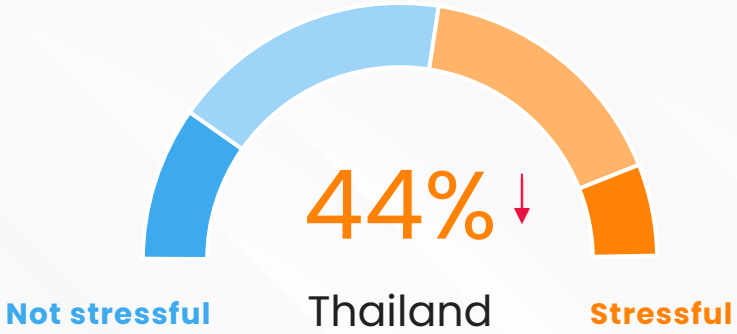
The majority of Southeast Asian adults affected by scams found the experience to be stressful

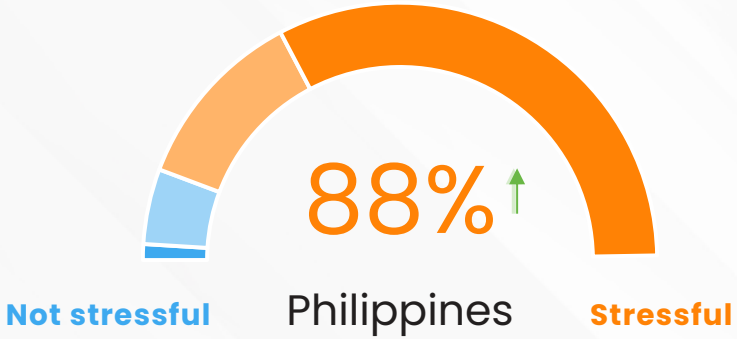
Impact of being scammed on stress

62%

Found the scam experience very (29%) or somewhat (33%) stressful





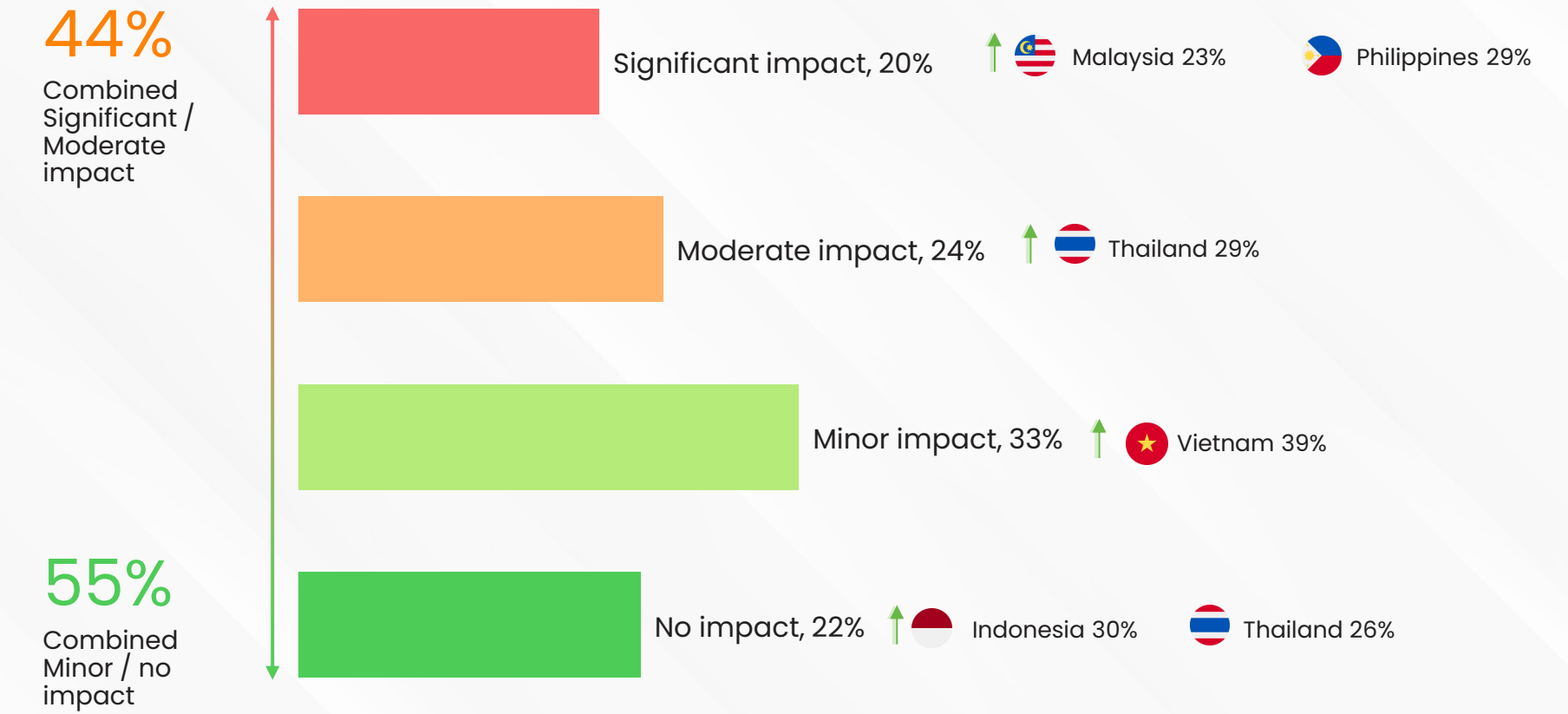


Stress is significantly higher among scam victims in the Philippines, compared to lower levels in Thailand

Q16. To what extent was experiencing the scam stressful? Base: All Southeast Asia respondents who have been scammed (3896), Thailand (612), Philippines (688)

Regions experiencing higher levels of stress were also more likely to report that scams had a significant impact on their mental wellbeing

Impact of being scammed on wellbeing



Q17. To what extent did the scam impact your mental wellbeing? Base: All Southeast Asia respondents who have been scammed (3896), Thailand (612), Indonesia (358) Malaysia (734), Singapore (685), Vietnam (810), Philippines (688)

Prevalence of scam encounters

How frequently are scams encountered? And on what platforms?

Scam exposure is most common in Vietnam and Malaysia

Prevalence encountering a scam in the last 12 months

77%

of Southeast Asian adults have been exposed to a scam in the last 12 months

72% ↓	66% ↓	85% ↑
 Thailand	 Indonesia	 Malaysia
75%	86% ↑	77%
 Singapore	 Vietnam	 Philippines

Q2. How often, if ever, are you exposed to attempts to scam you? Base: All respondents Southeast Asia (6000), Thailand (1000), Indonesia (1000) Malaysia (1000), Singapore (1000), Vietnam (1000), Philippines (1000)

11% of Southeast Asian adults encounter a scam at least once a day

Prevalence of daily scam encounters

13% Thailand

4% Indonesia

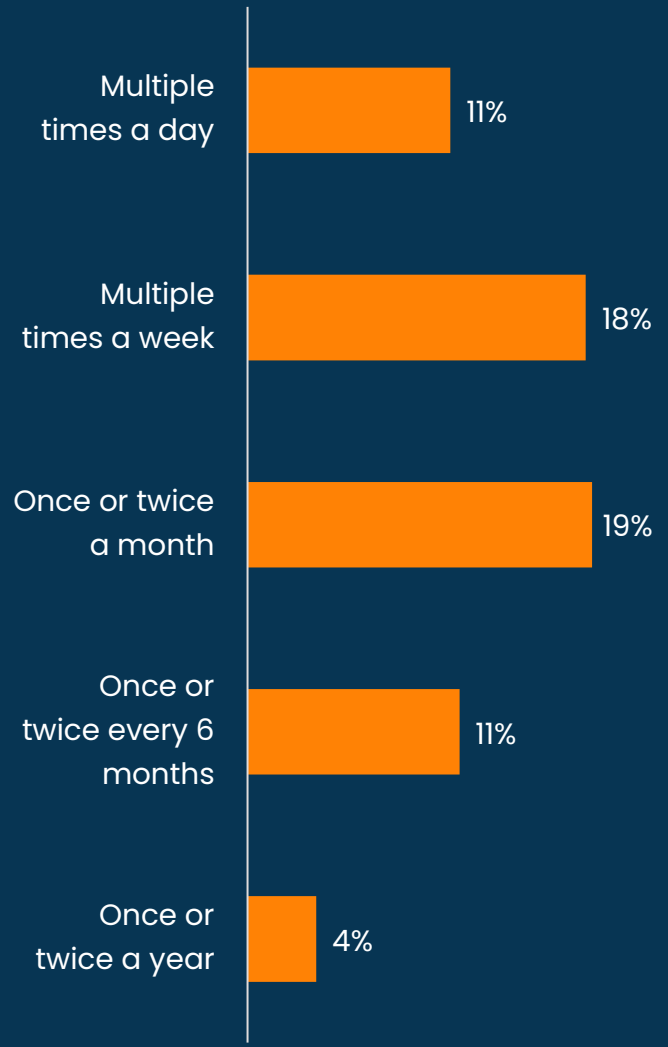
11% Malaysia

9% Singapore

11% Vietnam

18% Philippines

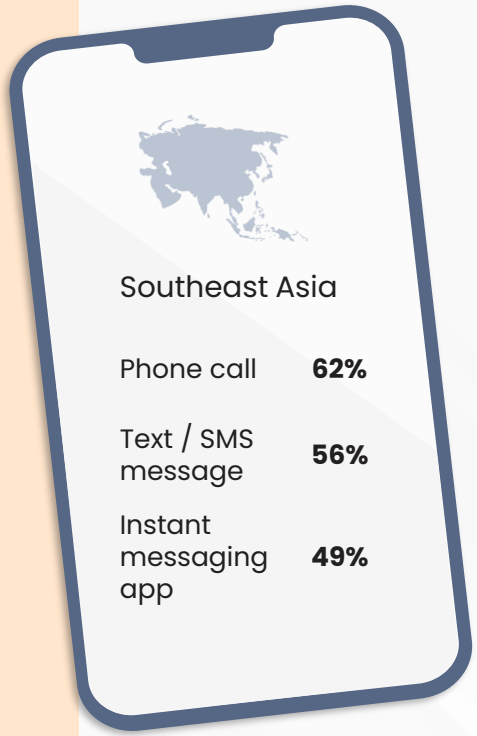
This rises to nearly a fifth in the Philippines. Meanwhile daily exposure to scams is less common in Indonesia



Q2. How often, if ever, are you exposed to attempts to scam you? Base: All respondents Southeast Asia (6000), Thailand (1000), Indonesia (1000) Malaysia (1000), Singapore (1000), Vietnam (1000), Philippines (1000)

The most common communication channels used by scammers in Southeast Asia are phone calls, text messages and instant messaging apps

Top three most common scammer communication channels in Southeast Asia and by market



Southeast Asia

Phone call	62%
Text / SMS message	56%
Instant messaging app	49%

Thailand

Phone call	68%
Text / SMS message	56%
Social media	40%

Indonesia

Phone call	64%
Instant messaging app	67%
Text / SMS message	59%

Malaysia

Email	73%
Instant messaging app	56%
Text / SMS message	51%

Singapore

Text / SMS message	61%
Phone call	59%
Instant messaging app	51%

Vietnam

Phone call	77%
Social media	48%
Instant messaging app	44%

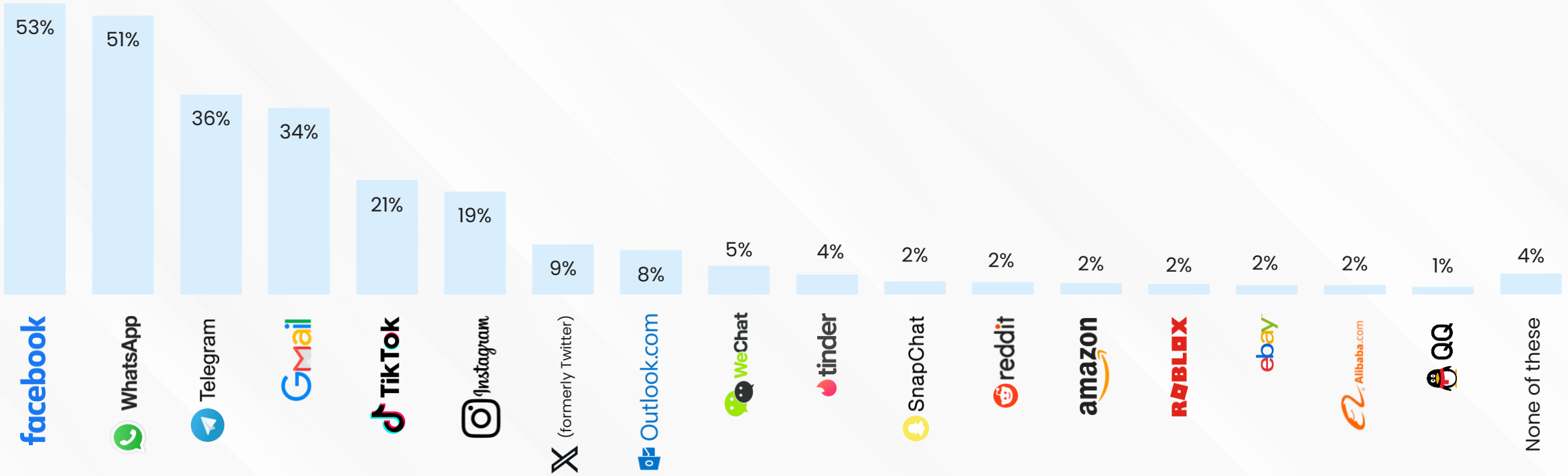
Philippines

Text / SMS message	75%
Instant messaging app	50%
Social media	50%

Q3. Through which communication channel(s) did scammers approach you in the last 12 months? Base: All Southeast Asian respondents who have been exposed to a scam attempt (3916), Thailand (623), Indonesia (360), Malaysia (736), Singapore (694), Vietnam (812), Philippines (691)

Scam encounters in Southeast Asia most frequently take place on Facebook, WhatsApp and Telegram

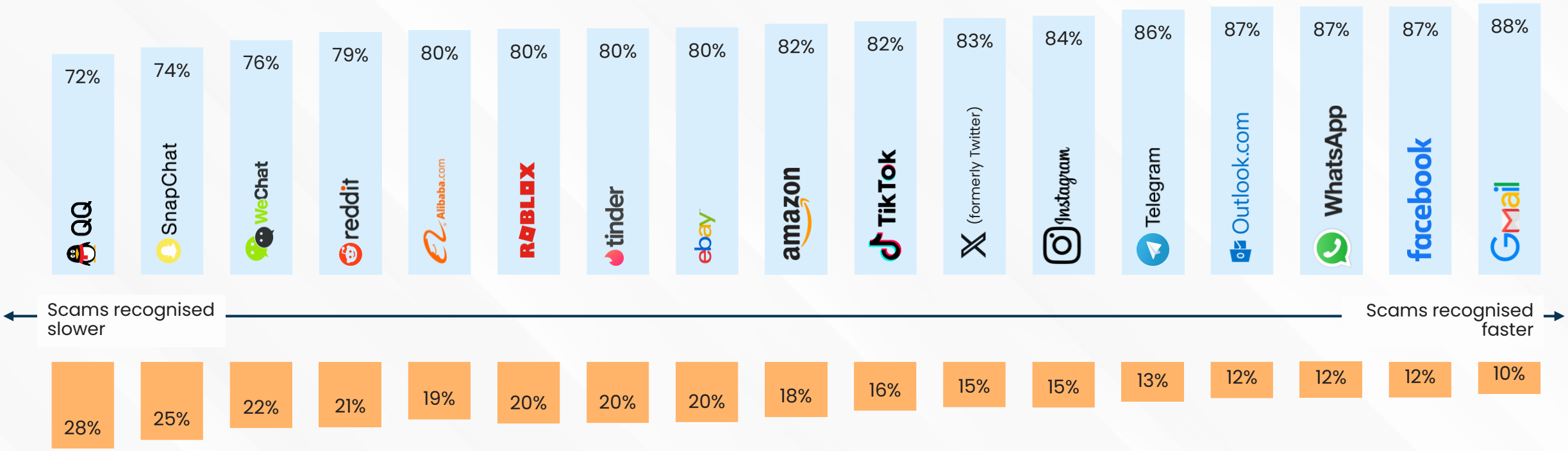
Online platforms used by scammers in last 12 months



Q4A. Through which, if any, of the following global service or platform(s) did scammers contact you in the last 12 months? Base: All Southeast Asian respondents who have been exposed to a scam attempt (3916), Thailand (623), Indonesia (360), Malaysia (736), Singapore (694), Vietnam (812), Philippines (691)

Scams tend to be recognised more slowly on platforms such as QQ, Snapchat, WeChat, and Reddit

Time taken to realise scam encounter, per platform

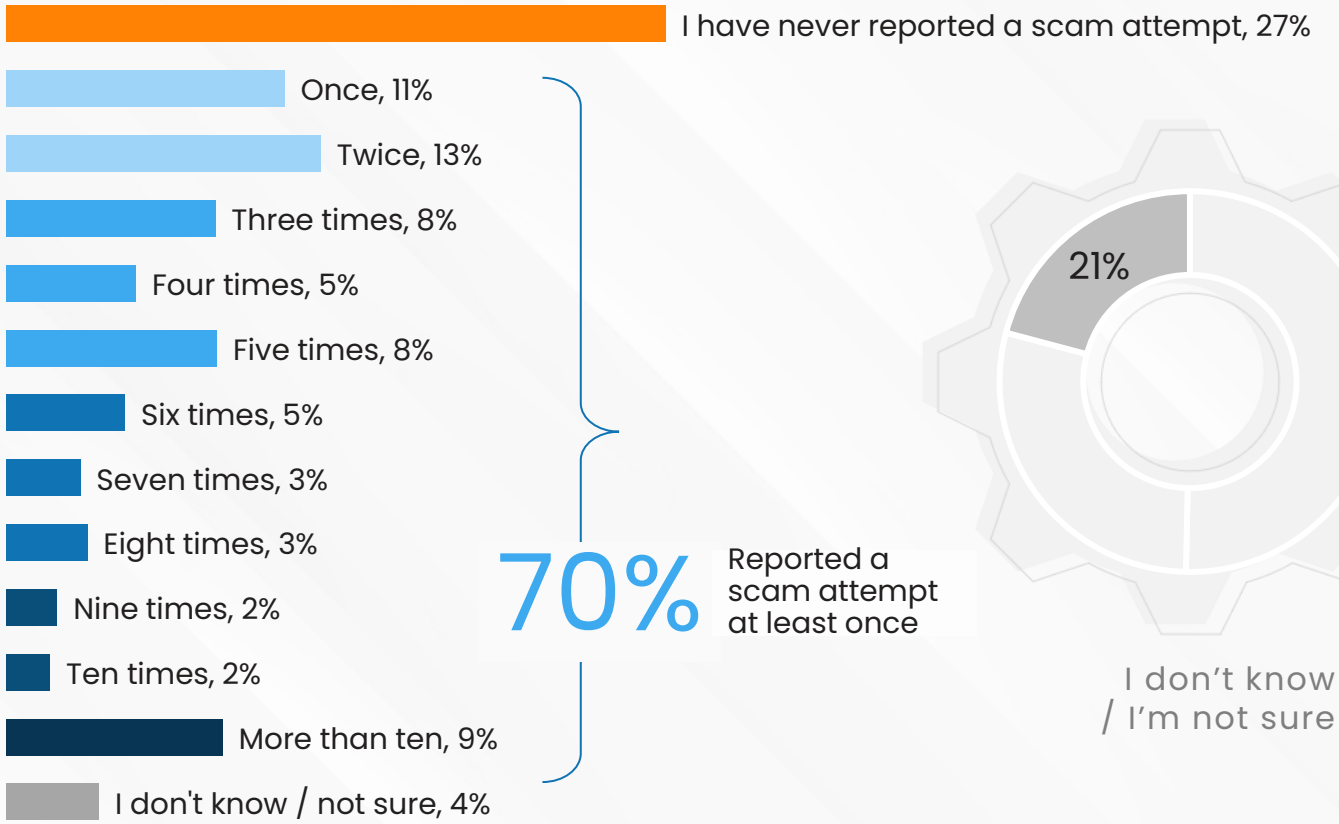


Q10. Through which, if any, of the following social service or platform(s) did scammers contact you in the last 12 months? Base: All respondents how have been exposed to a scam (2798)

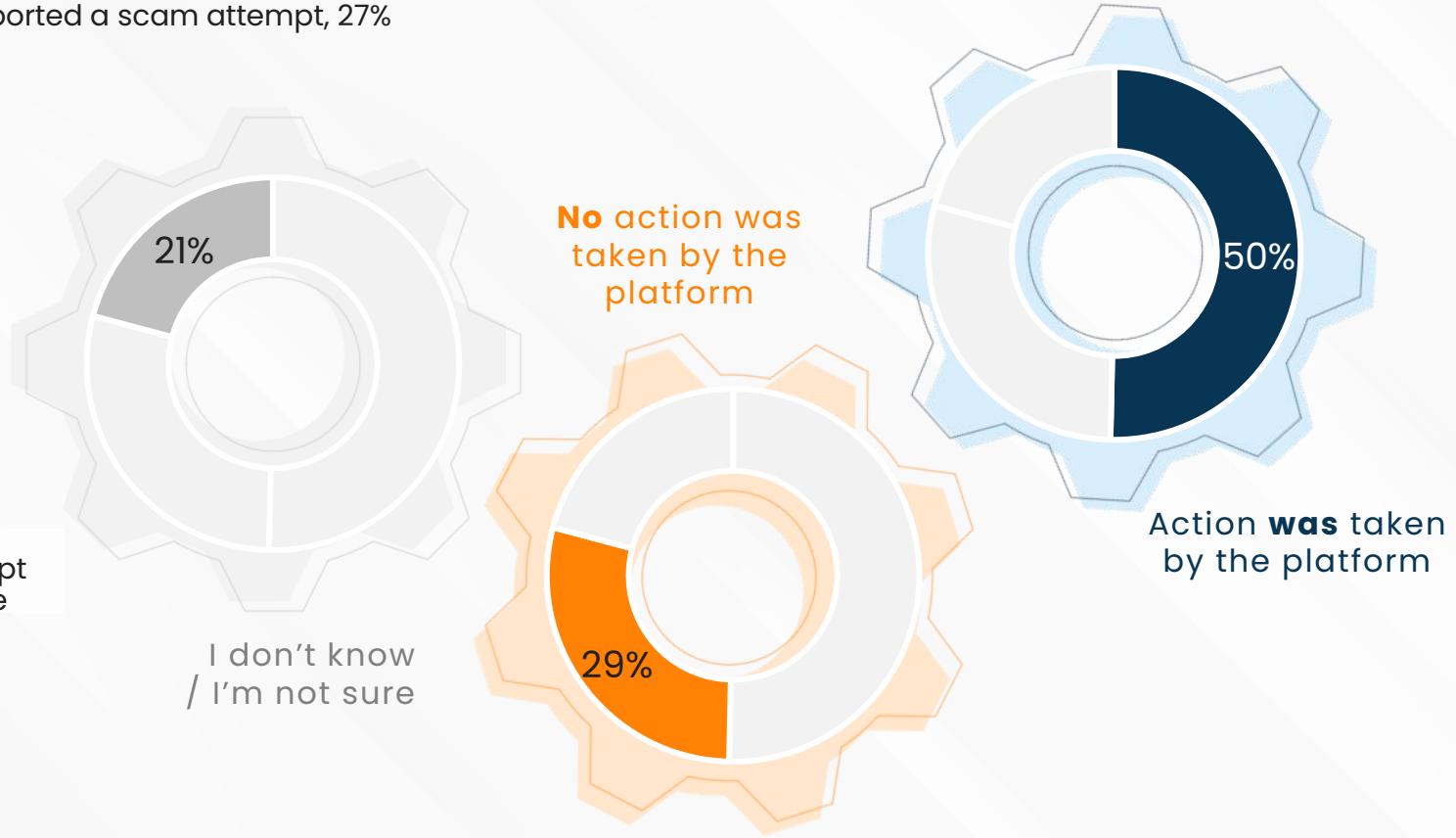
Q11. When a scammer approached you on , how long did it take you to realise they were trying to scam you? Base: All those in Southeast Asia who have been contacted by a scammer on an online platform (3754)

7 in 10 of those encountering a scam in Southeast Asia have reported it at least once. However, only half recall action being taken by the platform

Frequency of reporting a scam encounter in the last 12 months



Outcome of reporting scam encounter to platform / service provider



Q5. How many times, if any, have you reported a scam attempt to the service or platform provider where you experienced the scam attempt in the last 12 months? Q6. What happened when you reported the scam attempt to the platform or service provider? If you've reported more than one scam attempt, think about the most recent time. Base: Southeast Asian respondents contacted by scammers (3876), who reported scam attempts (2778)

Lack of action is one of the main reasons scam encounters go unreported in Southeast Asia, with not losing any money being the main barrier

Frequency of reporting a scam encounter in the last 12 months

Barriers to reporting scam encounters

72% Barrier group: Perceived lack of importance

- 48% I did not lose any money
- 31% I did not think it would make a difference / no action would be taken
- 17% I did not think it was important enough
- 4% It is not my responsibility

47% Barrier group: Uncertainty

- 38% I was not sure who to report the scam to
- 17% I was not certain that it was a scam

33% Barrier group: Practical barriers

- 23% The platform's reporting process was too complex
- 12% I did not have time
- 3% I forgot

8% Barrier group: Emotional barriers

- 5% I was too embarrassed
- 5% I was afraid

Q7. Why haven't you reported any scam attempts to service or platform providers in the last 12 months? Base: Southeast Asian respondents who have not reported scam attempts (978)

Scam Prevention

What self-prevention tactics to consumers use to identify scams? How are public and commercial organisations' seen in their responsibility and performance in preventing and resolving scams?

The believability of the scam is the main reason why victims in Southeast Asia think they were scammed, particularly for those in Thailand and Vietnam

Reasons why scams experienced

22% The scam was very realistic / believable
Thailand, Vietnam

18% I was attracted to the offer that was made
Malaysia, Philippines

13% I acted too fast to recognise the deceit

9% It was the first time using the platform or service and so I was not experienced enough to identify the warning signs
Malaysia

8% I was not certain it was legitimate, but I chose to risk it
Philippines

7% I wasn't familiar enough with the brand the scammer was impersonating, so I couldn't tell if it was fake
Indonesia, Thailand

5% I trusted a friend/family member
Vietnam

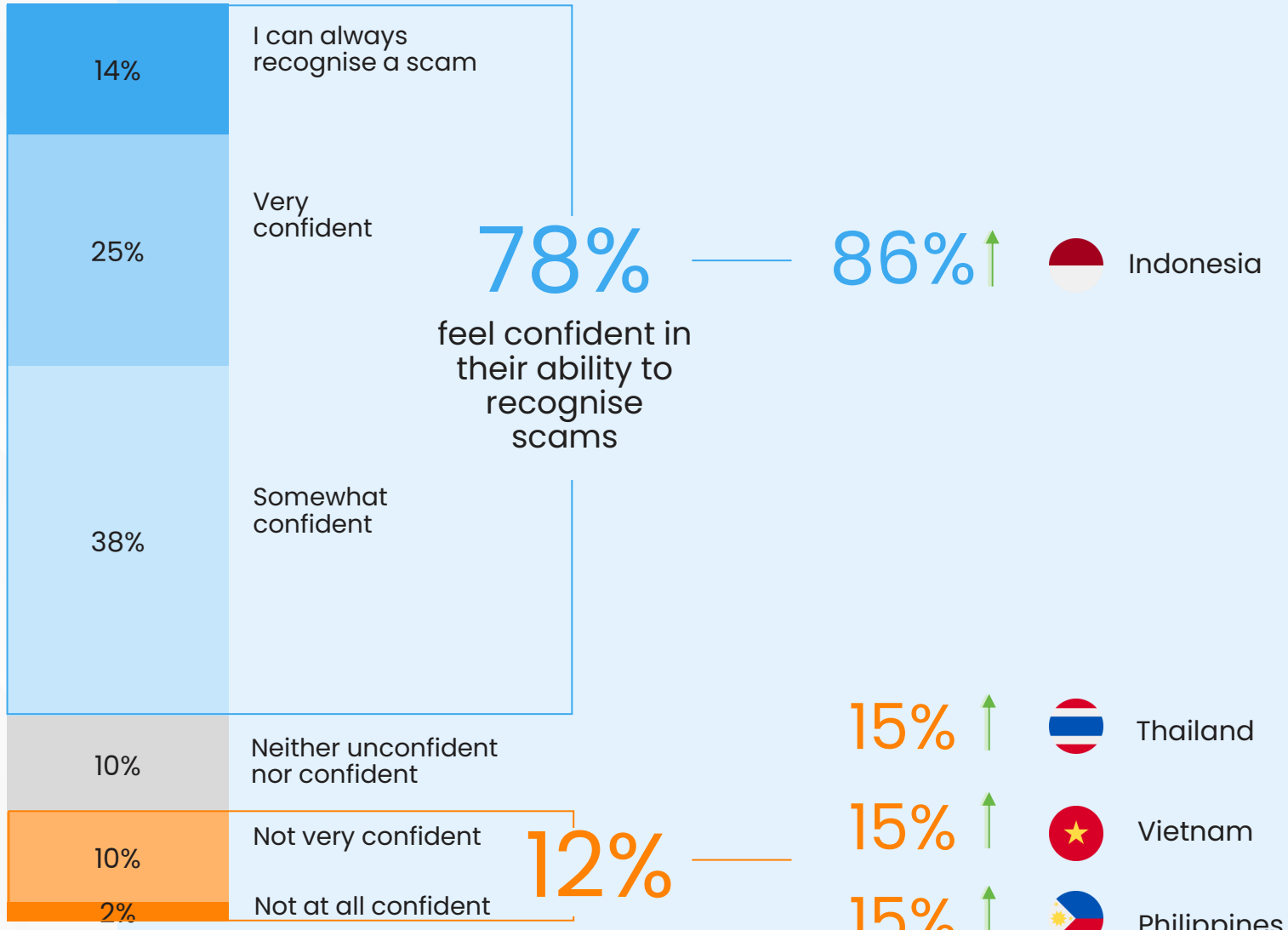
3% I was coerced into participating
Philippines

10% I don't know / not sure
Singapore

Q19. Why do you think you were scammed? Select the main reason.
Base: Base: All Southeast Asian respondents who have been scammed (3896), Thailand (621), Indonesia (358) Malaysia (734), Singapore (685), Vietnam (810), Philippines (688)

Whilst the majority feel confident in recognising scams, those in Thailand, the Philippines and Vietnam report having less confidence

Confidence in recognising a scam

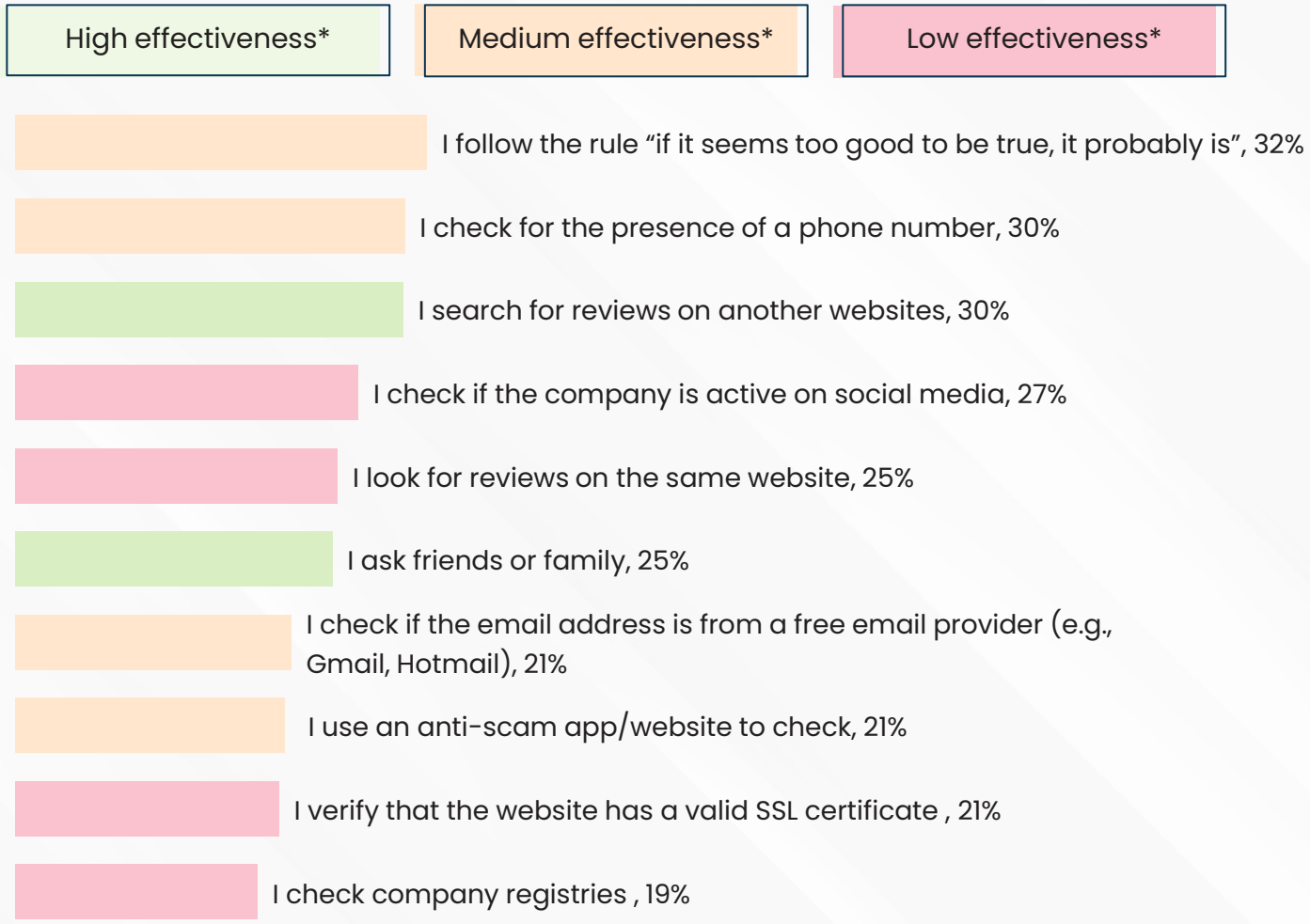


Q1. How confident are you that you can recognise scams? Base: All respondents Southeast Asia (6000), Thailand (1000), Indonesia (1000) Malaysia (1000), Singapore (1000), Vietnam (1000), Philippines (1000)

94%

of adults in Southeast Asia take at least one step to verify whether an offer is legitimate. However, many rely on methods that are have low effectiveness

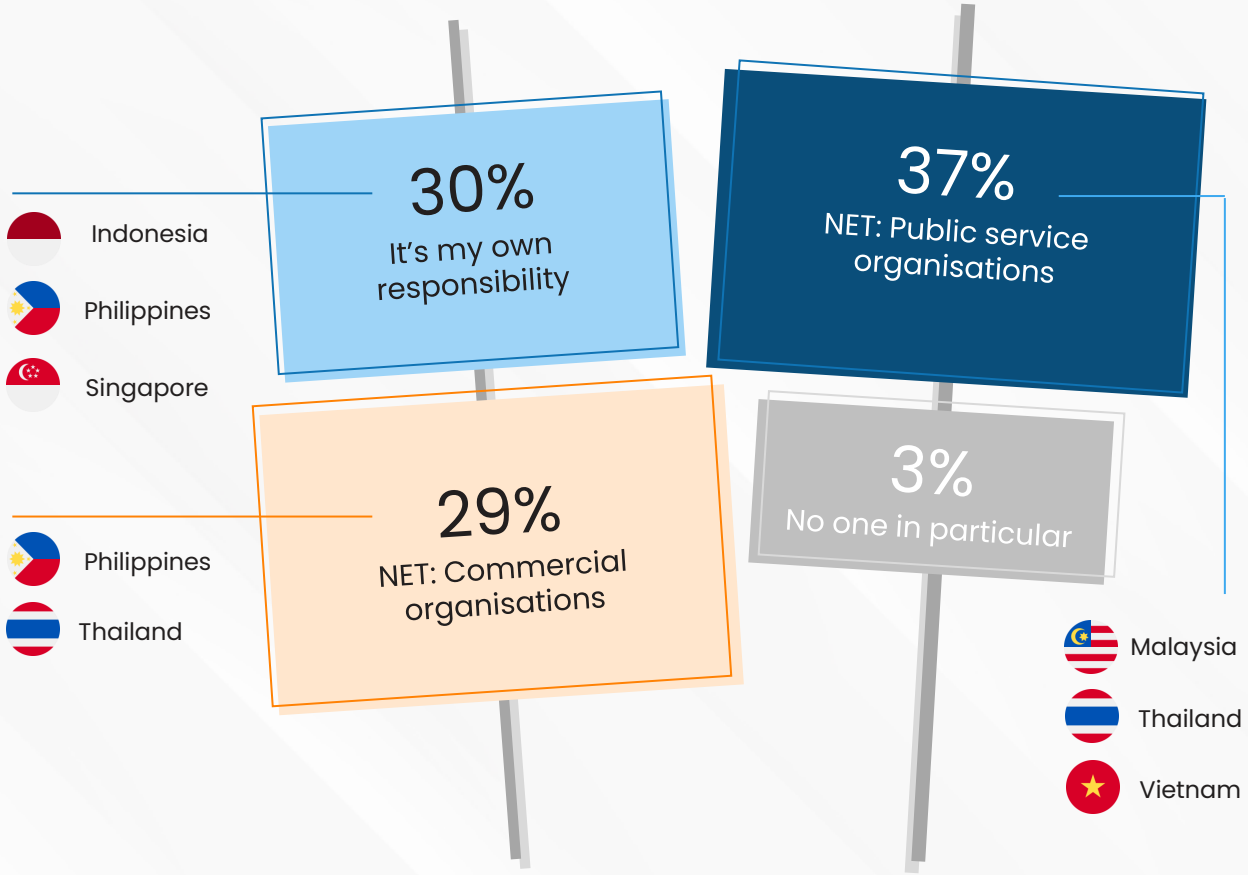
Steps taken to check legitimacy of offer – top 10



Q20. What steps do you take to check if an offer is real or a scam? Base: All respondents Southeast Asia (6000), Thailand (1000), Indonesia (1000) Malaysia (1000), Singapore (1000), Vietnam (1000), Philippines (1000) *Effectiveness groupings provided by GASA

Over a third of Southeast Asian adults point to public bodies to keep people safe from scammers whilst three in ten feel personally responsible

Responsibility for keeping people safe from scammers ranking:



- 16% The government
- 11% The online platform used by the scammer
- 9% The police
- 8% Consumer protection authorities
- 7% The website provider / hosting company used by the scammer
- 5% My telecom or mobile operator
- 5% Financial protection authorities
- 5% My bank, payment method or crypto exchange
- 1% Insurance companies

Most responsible ↑ ↓ Least responsible

GASA Global Anti-Scam Alliance · BioCatch · SCAMADVISER

Q24. Who do you think should be most responsible for keeping people safe from scammers? Base: All respondents Southeast Asia (6000), Thailand (1000), Indonesia (1000) Malaysia (1000), Singapore (1000), Vietnam (1000), Philippines (1000)

Whilst these organisations are generally seen as adequate in scam education & reporting, there is room for improvement across the board

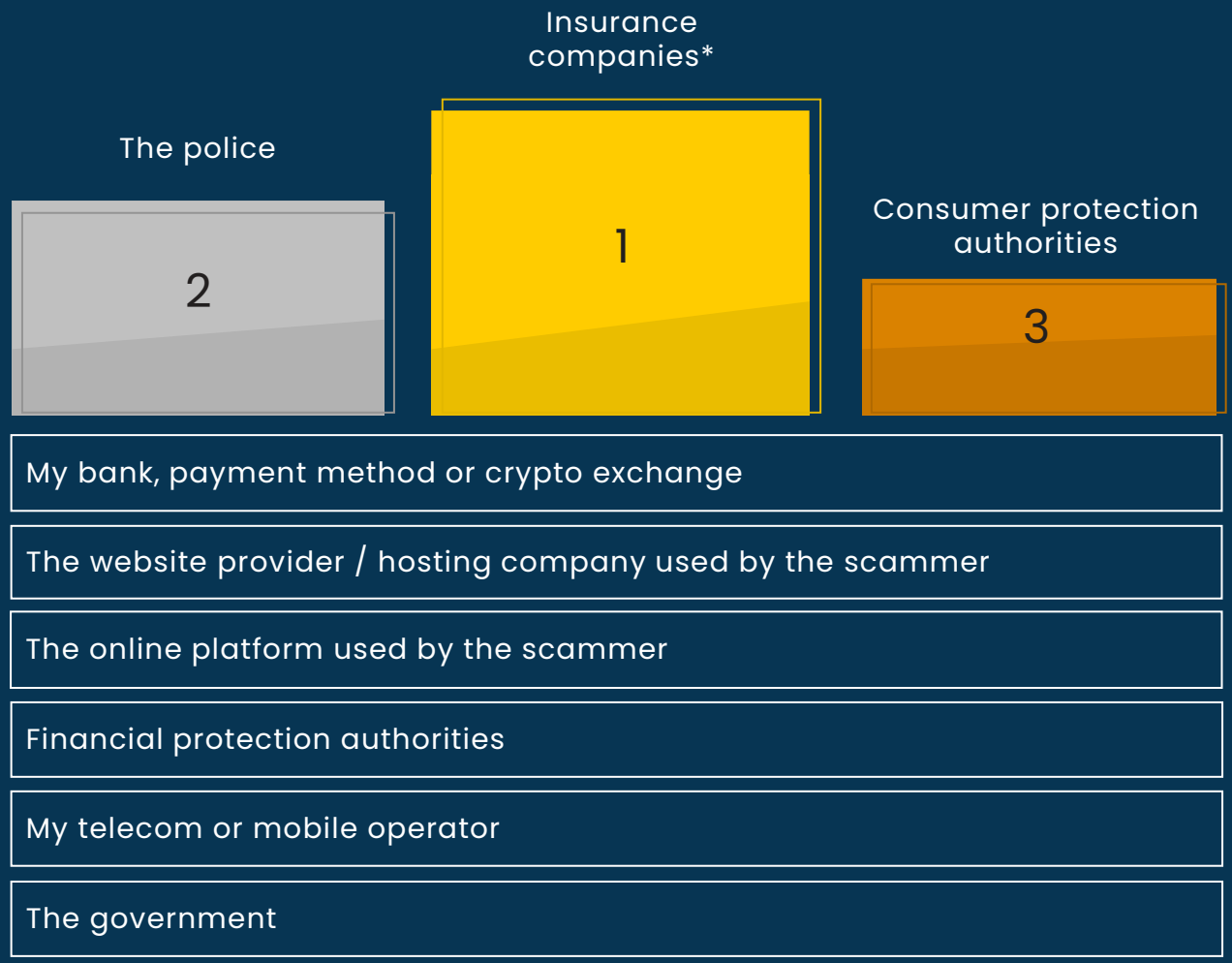
Consumer rating on aspects of pre & post scam support – NET: Good

	The government	The police	Consumer protection authorities	Financial protection authorities	The online platform used by the scammer	The web provider/ hosting company used	My bank, payment method or crypto exchange	My telecom or mobile operator	Insurance companies*
Responsibility ranking	1st	3rd	4th	7th	2nd	5th	8th	6th	9th
Scam education & awareness	39%	57%	53%	44%	42%	44%	51%	37%	63%
Scam blocking / payment prevention	32%	51%	45%	40%	39%	44%	41%	32%	59%
Ease of scam reporting	33%	54%	48%	41%	44%	45%	42%	32%	64%
Victim support / helpdesk	29%	55%	43%	35%	38%	34%	39%	33%	54%
Scammer investigation / arrest	34%	59%	41%	34%	33%	42%	39%	31%	47%
Reimbursement / compensation	24%	39%	31%	26%	29%	32%	38%	28%	57%
Southeast Asia ranking across all aspects	9th	2nd	3rd	7th	6th	5th	4th	8th	1st

Q25. You said [ORGANISATION] should be most responsible for keeping people safe from scammers. How do you rate [ORGANISATION] on the following aspects: Base: All respondents Southeast Asia who think someone else should be responsible for keeping people safe from scammers (3942), those who think The government (982), The police (522), Consumer protection authorities (484), Financial protection authorities (279), The online platform used by the scammer (649), The website / hosting company (388), My bank, payment method or crypto exchange (266), My telecom or mobile operator (329), Insurance companies (43*) should be responsible *Caution: Low base size

Overall, Insurance companies, the police and consumer protection authorities are perceived to perform the strongest across all aspects of pre & post scam support in Southeast Asia

Performance ranking on pre & post scam support – across all aspects



Q25. You said [ORGANISATION] should be most responsible for keeping people safe from scammers. How do you rate [ORGANISATION] on the following aspects: Base: All respondents Southeast Asia who think someone else should be responsible for keeping people safe from scammers (3942), those who think The government (982), The police (522), Consumer protection authorities (484), Financial protection authorities (279), The online platform used by the scammer (649), The website / hosting company (388), My bank, payment method or crypto exchange (266), My telecom or mobile operator (329), Insurance companies (43*) should be responsible
*Caution: Low base size

Whilst the police outperform Southeast Asian consumer expectations, governments fall short

Responsibility for keeping people safe from scammers ranking:

- The government
- The online platform used by the scammer
- The police
- Consumer protection authorities
- The website provider / hosting company used by the scammer
- My telecom or mobile operator
- Financial protection authorities
- My bank, payment method or crypto exchange
- Insurance companies

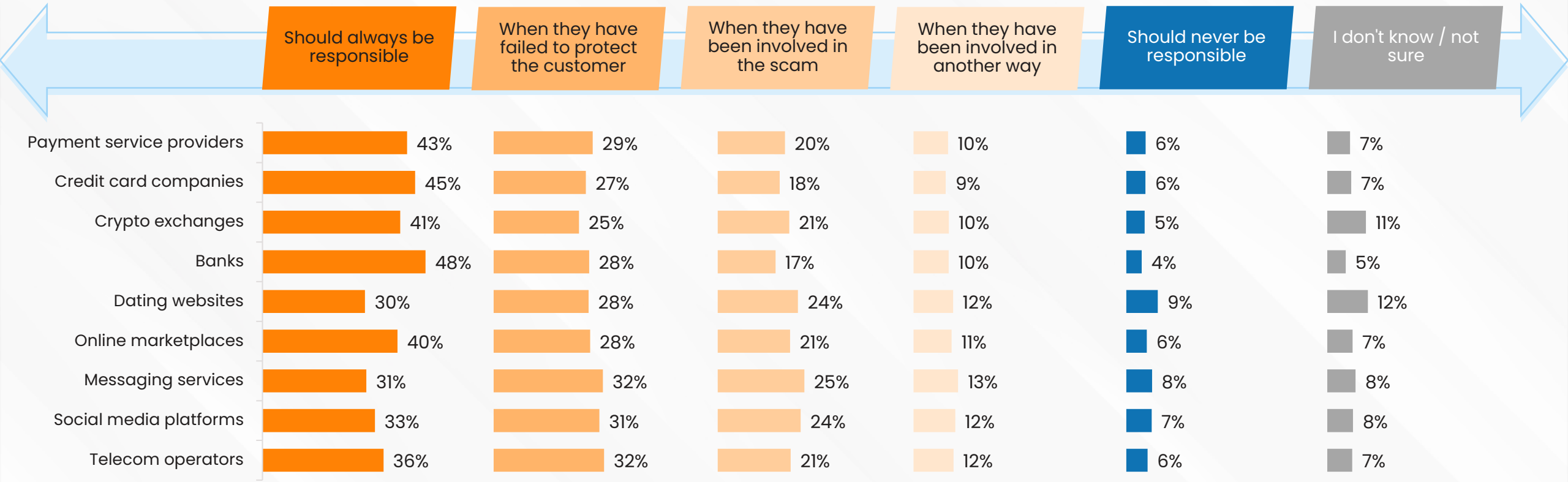
Performance ranking on preventing / resolving scams:

- Insurance companies*
- The police
- Consumer protection authorities
- My bank, payment method or crypto exchange
- The website provider / hosting company used by the scammer
- The online platform used by the scammer
- Financial protection authorities
- My telecom or mobile operator
- The government

Q24. Who do you think should be most responsible for keeping people safe from scammers? Base: All respondents Southeast Asia (6000)
Q25. You said [ORGANISATION] should be most responsible for keeping people safe from scammers. How do you rate [ORGANISATION] on the following aspects: Base: All respondents Southeast Asia who think someone else should be responsible for keeping people safe from scammers (3942), those who think The government (982), The police (522), Consumer protection authorities (484), Financial protection authorities (279), The online platform used by the scammer (649), The website / hosting company (388), My bank, payment method or crypto exchange (266), My telecom or mobile operator (329), Insurance companies (43*) should be responsible
*Caution: Low base size

Almost half of adults in Southeast Asia believe Banks should always be responsible for reimbursing those experiencing a scam

Level of expected responsibility for reimbursing scams



Q26. If someone is scammed on any of the following platforms, in what circumstances do you think the platform provider should be responsible for reimbursing them? Base: All respondents Southeast Asia (6000)

GASA RECOMMENDATIONS

GASA Global Anti-Scam Alliance

SCAMADVISER

whoscall

GASA's ten recommendations to turn the tide on scams

Jorij Abraham
MANAGING DIRECTOR
GASA
Global Anti-Scam Alliance

Online scams are not just a consumer issue — they are now a major threat to digital trust, economic stability, and personal safety. As fraud networks become faster and more sophisticated, Europe needs to act decisively.

Governments often prioritize protecting critical infrastructure from cyberattacks. Yet scams targeting consumers undermine confidence in the digital economy — and criminals are evolving faster than our defences.

Through collaborative work at our global events, experts identified ten key actions to better protect consumers.

Empowering Consumers

1. Launch unified, permanent national campaigns to raise scam awareness.
2. Establish national helplines for scam victims, accessible online and by phone.
3. Create integrated victim support systems offering financial, legal, and psychological help.

Creating a Safer Internet

4. Build infrastructural protections with telecoms and tech providers to block scams before they reach consumers.
5. Improve fraud traceability across borders by requiring transparency from sellers, platforms, and payment providers.

Strengthening Cooperation

6. Set up an international network of national anti-scam centres, combining law enforcement, cybersecurity, and private sector expertise.
7. Develop a global scam data-sharing hub to detect cross-border fraud in real time.
8. Make service providers responsible and liable for fraud committed through their platforms.
9. Allow preventive action: enable providers to warn, block, and take down fraudulent activities without excessive liability risk.
10. Create a global scam investigation and prosecution network to target organized fraud groups across jurisdictions.

Protecting consumers is essential to securing the digital future. The Global Anti-Scam Alliance, its membership, and the international public & private sectors must lead the way.

ABOUT THIS REPORT

Who are we?

The Global Anti-Scam Alliance (GASA) is a non-profit organization whose mission it is to protect consumers worldwide from scams. We realize our mission by bringing together policy makers, law enforcement, consumer authorities, NGOs, the financial sector, telecom operators, internet platforms and service providers, cybersecurity and commercial organizations to share insights and knowledge surrounding scams. We build networks in order to find and implement meaningful solutions.

GASA releases the annual Global State of Scams report, alongside many secondary reports which focus on the state of scams in various countries.

BioCatch helps the world's largest financial institutions protect their customers from fraud and financial crime.

It believes behaviour has become the only element of our digital identities that remains truly, and uniquely, human.

ScamAdviser is a global leader in AI-powered scam prevention, protecting businesses and individuals in real time. Our Anti-Scam Intelligence platform can protect users from untrustful websites, messages, and calls. Stopping scammers before they strike. Trusted by 400+ partners and used by over 1 billion people worldwide, ScamAdviser turns data into decisive action—so you can stay safe, stay ahead, and stay in control.

Opinium is an award-winning strategic insight agency that utilises robust methodologies to deliver insights with impact for organisations across the private, public and third sectors.

GASA have partnered with Opinium to lead the 2025 Global State of Scams research programme.

Contact europe@opinium.com for enquiries.

Methodology notes

SAMPLE AND METHODOLOGY

- Sample size | 6,000 people
- Audience | Adults aged 18+ living in Thailand, Indonesia, Malaysia, Singapore, Vietnam, Philippines
- Quotas | Quotas were used throughout fieldwork to ensure the sample was nationally representative of the adult population of each market on age, gender and region
- Weighting | Weighting was applied on the final dataset to be nationally representative of the adult population of each market on age, gender and region
- Methodology | 15-minute online survey
- Translations | Whilst this report is in English, the survey was translated into the local language for each market prior to completion by respondents
- Sample source | Online research panel
- Fieldwork | 7th – 20th March 2025

FULL Q8 SCAM WORDING USED IN SURVEY

- **Investment scam**: Invested money with a person or company that deceived you about what you would receive, such as promising a guaranteed return on your investment or no risk of financial loss
- **Shopping scam:** Paid for any products or (subscription) services that you never received or that turned out to be a scam
- **Employment scam:** Paid money or given personal/financial information to get a job, employment, work-at-home position or business opportunity but were deceived about how the money would be used or what you would receive in return
- **Unexpected money scam:** Paid money or given personal/financial information to receive a prize, grant, inheritance, lottery winning, or sum of money that you were told was yours, but never received
- **Impersonation scam:** Paid money or given personal/financial information to a person who claimed to be a government official or working for a bank/lender or other company of authority
- **Charity scam:** Donated money to a charity or a charitable cause that later turned out to be fake or that you later suspected was fake
- **Romance/relationship scam:** Given money or personal/financial information to someone who pretended to be or pretended to be calling on behalf of a family member, friend, caregiver, or someone interested in you romantically, but that person was not who they claimed to be
- **Fake invoice scam:** Paid an invoice or a debt, but you found out you were being deceived, and the invoice/debt was not real or not yours
- **Blackmail or extortion scam:** Paid money or given personal/financial information because someone threatened or extorted you
- **Identity theft:** Personal information, e.g. your credit card, used without your consent OR did someone get access to a personal account(s), e.g., your bank, email, social media account, for financial gain, for example, to transfer money, take out a loan, request official documents, or buying products and/or services
- **Money recover scam:** Paid money or given personal/financial information to a company or person who promised to help me recover from a scam, but in the end deceived me.
- **Other scams:** Where you have paid money or given personal/financial information to someone who used deception in another situation not previously listed

ABOUT THE AUTHORS

About the authors

Jorij Abraham

MANAGING DIRECTOR

Jorij Abraham has been active in the Ecommerce Industry since 1997. From 2011 to 2017, he was the Research Director of Thuiswinkel.org, Ecommerce Europe (the Dutch & European Ecommerce Association) and Managing Director of the Ecommerce Foundation.

From 2015 to 2024, Jorij was also a Professor of Ecommerce at TIO University. In 2018, Jorij took over ScamAdviser.com to help consumer due diligence efforts against online scams. He sold ScamAdviser to Gogolook in 2024 to focus on his current role as Managing Director at the Global Anti-Scam Alliance (GASA).

Molly Maclean

ASSOCIATE DIRECTOR

Molly Maclean is an Associate Director specialising in research for Thought Leadership.

Molly works with brands and organisations to help them use insights to raise awareness of key issues, influence decision-makers, and drive positive change.

She has over six years of experience conducting research for technology brands and organisations, particularly in the cybersecurity space.

Metje van der Meer

MARKETING DIRECTOR

Metje van der Meer leads global communications, brand strategy, and stakeholder engagement at the Global Anti-Scam Alliance (GASA). With over a decade of experience in B2B marketing and international outreach, she develops multi-channel campaigns and partnerships that advance GASA's mission to combat online fraud through cross-sector collaboration.

Metje plays a key role in promoting GASA's global and regional initiatives, including the Global Anti-Scam Summit (GASS) and the alliance's work across Southeast Asia. Her efforts focus on aligning public and private sector stakeholders to raise awareness and drive coordinated action against scams worldwide.

Join GASA, the Network to Defeat a Network

Exclusive Intelligence Sharing
Stay ahead of emerging scam trends through members-only webinars, expert-led discussion groups, and our monthly newsletter which is trusted by over 20,000 anti-scam professionals worldwide.

Authoritative Research Access
Get insider access to our Global State of Scam reports, 30+ in-depth regional studies, and best practice database that help shape anti-scam strategies.

High-Impact Networking
Connect with global changemakers at international summits, collaborate through local GASA chapters, and find partners through our members-only directory.

Global Solutions
Co-create or join concrete solutions to fight scams like the Global Signal Exchange where data is shared real-time scam intelligence and Scam.Org, the anti-scam hub being developed for consumers worldwide.

Become part of a global force against scams and help protect consumers everywhere.

See all benefits: **gasa.org/membership**

Our Foundation Members

amazon, Bitdefender, Capital One, Citizens, CSC, F-Secure, feedzai, Gen, Gogolook, Google, GSMA, ibfed International Banking Federation, JPMorganChase, LexisNexis Risk Solutions, Lloyds Banking Group, Mastercard, Match Group, McAfee, Meta, Microsoft, netcraft, Scamadviser, Scotiabank, The Media Trust, Trend Micro, VISA

Our Corporate Members

AnyDesk, البنك العربي Arab Bank, Arkose Labs, Banca Transilvania, cellcard, Chainalysis, Crystal, Cyberdefense, DANA, EBRAND, FICO, Remitly, Santander, sea connecting the dots, TeamViewer, tietoevry, VoiSek, Vonage Part of Ericsson

GASA
Global Anti-Scam Alliance

BioCatch

SCAMADVISER

07 Op Opinium

DISCLAIMER

This report is a publication by the Global Anti-Scam Alliance (GASA) supported by BioCatch and ScamAdviser. GASA owns the copyrights for the report. Although the utmost care has been taken in the construction of this report, there is always the possibility that some information is inaccurate. No liability is accepted by GASA for direct or indirect damage arising from the use of information contained in the report.

COPYRIGHT

Global Anti-Scam Alliance (GASA)

Oder 20 - UNIT A6311
2491 DC The Hague
The Netherlands

General & Press Inquiries: partner@gasa.org

X (Twitter): @ScamAlliance

LinkedIn: linkedin.com/company/global-anti-scam-alliance