GASA | Gogolook |

STATE OF SCAMS REPORT 2026

PHILIPPINES



Nearly half of Filipino/a adults that interacted with scams lost money



Jorij Abraham
MANAGING DIRECTOR



Brian D. Hanley
CHAPTER DIRECTOR ASIA-PACIFIC

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.

GASA | Gogolook | Global Anti-Scam Alliance

Summary

Scam exposure keeps climbing

Scam exposure continues to rise in the Philippines, with 84% of adults encountering a scam in the past year, up from 77% in 2025. Despite 58% saying they are confident they can recognize scams, 60% of those exposed went on to interact with a scam, suggesting confidence alone is not preventing engagement.

Scam interactions remain a major vulnerability

Exposure frequently translates into engagement. Nearly half of adults (44%) interacted with a scammer, and one in three of those interactions ultimately resulted in financial loss. Shopping, investment, and employment scams were the most commonly interacted-with scam types, indicating continued success for scams focused on money-making opportunities.

Financial losses are significant — and repeat victimization remains common

Scams are estimated to have cost Filipino consumers ₱121.8 billion in the past year, with average losses of ₱10,427 per victim. Losses are often not one-off events: 38% of victims report being scammed more than once, highlighting the ongoing risk of repeat targeting.

The emotional impact is intensifying

The consequences extend well beyond the money lost. More than four in five victims (82%) say being scammed affected their wellbeing, while 22% report being unable to pay for basic essentials as a result.

Victims are often left to discover scams themselves

Formal warnings appear to play a limited role in identifying scams. Seven in ten victims say they realized they had been scammed on their own, while relatively few were alerted by banks, telecom providers, anti-scam services, or public authorities. This suggests many scams are only identified after harm has already occurred.

Reporting is common — recovery is rare

Victims are more likely to report scams to platforms, organizations, and social channels than to authorities. Yet outcomes remain limited: around a quarter say their report was acknowledged but no further action was taken, while only 12% recovered or were reimbursed for any of their lost money.

Platforms face an expectation gap

Filipinos place substantial responsibility for scam prevention on online platforms and website providers, yet these organizations are perceived as underperforming relative to the responsibility assigned to them. By contrast, the police are viewed as delivering the strongest performance in preventing and resolving scams.

Building trust in the digital economy: a shared fight against scams



Helena Forest
EXECUTIVE VICE PRESIDENT, GLOBAL PRODUCT & COMMERCIAL, REAL-TIME PAYMENTS

Mastercard

About Mastercard

Mastercard powers economies and empowers people in 200+ countries and territories worldwide. Together with our customers, we're building a resilient economy where everyone can prosper. We support a wide range of digital payments choices, making transactions secure, simple, smart and accessible. Our technology and innovation, partnerships and networks combine to deliver a unique set of products and services that help people, businesses and governments realize their greatest potential.

Across the Philippines, digital payments have become part of daily life. Real-time transfers through InstaPay and QR codes are now a routine way to pay in city centers, public markets, and neighborhood stores. That transformation is a real achievement, built by Philippine regulators, financial institutions, and innovators who together have created one of the region's most dynamic payment ecosystems.

The rails that let people pay a merchant or send money home can also expose them to risk. Scams are growing in scale and sophistication, exploiting the very qualities of speed, convenience, and accessibility that made real-time payments succeed. It is a tension that every fast-growing market now faces: how to raise protection without weakening the experience people value and hold their trust as volumes grow.

No single measure answers it. What works is a layered defense — reducing risk before a payment is made, using a common language to help spot suspicious activity in real time, acting quickly when harm is suspected, and improving recovery when money is lost.

The Anti-Financial Account Scamming Act sets the framework and the urgency for action, creating the conditions for institutions to detect, delay, and investigate fraudulent activity. As the GASA report shows, the protections themselves have to be built across the ecosystem. Plans for a National Anti-Scam Hub reflect that reality. Prevention and recovery depend on intelligence moving quickly between banks, telecommunications providers, digital platforms, and law enforcement, with each of them acting on it together.

The task now is to put these commitments into practice, strengthen coordinated national defenses, and keep Filipino consumers at the center of the response. Mastercard's work follows the same layered logic, and we are glad to support that effort.

Collaboration Is Our Strongest Defence Against Scams



Rajat Maheshwari
GASA INAUGURAL CHAPTER CHAIR

Mastercard

About Mastercard

Mastercard powers economies and empowers people in 200+ countries and territories worldwide. Together with our customers, we're building a resilient economy where everyone can prosper. We support a wide range of digital payments choices, making transactions secure, simple, smart and accessible. Our technology and innovation, partnerships and networks combine to deliver a unique set of products and services that help people, businesses and governments realize their greatest potential.

Scams have become one of the defining challenges of the digital age. They undermine trust, inflict significant financial and emotional harm on citizens, and threaten confidence in the digital economy. The findings in this report are a timely reminder of the scale of the challenge facing us today: 84% of people in this Philippines report encountered scams, while 15% have suffered financial losses as a result.

Our journey in Southeast Asia began in 2023, when we invited the Global Anti-Scam Alliance (GASA) to establish its first overseas chapter in Singapore. Since then, it has been our privilege to help build and support GASA chapters across the region, bringing together governments, law enforcement agencies, financial institutions, telecommunications providers, technology platforms, consumer groups, and cybersecurity experts under a common purpose. Because while industries and organizations may operate within boundaries, scammers do not. Collaboration is not optional; it is our strongest defence.

The nature of scams continues to evolve rapidly. What was once viewed as an issue for banks, telcos, platforms, or law enforcement alone has become a national challenge affecting every sector of society. This requires us to evolve our response as well. Two important mindset shifts we will need to make to evolve our fight are: Look at the problem of scams as a scam-chain issue and not a problem for a specific industry only; and more from reactive to preventive measures. This involves building and sharing capabilities in predictive intelligence, and work further upstream to disrupt scams before they reach potential victims.

The insights in this report should serve not only as a reflection of today's threat landscape, but as a catalyst for stronger collective action. By working together across sectors and borders, we can turn the tide against scams and build a safer digital future for all.

Strengthening the Philippines' Response to an Evolving Scam Threat



Mel Migrino
PHILIPPINES COUNTRY HEAD AND GENERAL MANAGER, GOGOLOOK

Gogolook

About Gogolook

Gogolook is a leading TrustTech company established in 2012. With "Build for Trust" as its core value, expanding its business from Asia to Europe and America.
A foundation member of the Global Anti-Scam Alliance (GASA), Gogolook has also teamed up with a number of institutes such as the Taiwan National Police Agency, Thai Royal Police, the Philippines Cybercrime Investigation and Coordinating Center, the Fukuoka city and Shibuya city government, and the Royal Malaysia Police to fight scams, dedicated to creating a "scam-free environment."

Scams pose a major threat to the Philippines' economic stability and financial system integrity. As major scam hubs face enforcement crackdowns, syndicates have decentralized into smaller, pervasive operations across rural areas. Over the past year, Investment Scams, Relationship Scams, Task Scams, Third Party Scams and Identity Theft have proliferated massively, taking a heavy toll on personal and business security.

Beyond financial damage, cyber scams inflict a severe psychological toll on Filipino victims, fueling an urgent demand for centralized reporting and unified inter-agency coordination. In a decisive response, the government enacted the landmark Anti-Financial Account Scamming Act (AFASA), or Republic Act No. 12010/ Regulated by the Bangko Sentral ng Pilipinas (BSP), AFASA penalizes money muling, social engineering, and economic sabotage while empowering institutions to deploy real-time fraud monitoring and temporarily hold disputed funds.

This legislative breakthrough marks a pivotal shift, but policy alone is insufficient. Modernizing our technical infrastructure to detect, respond and recover from scams —specifically through the National Anti-Scam Operations. However, our most complex challenge remains human behavior: changing ingrained digital habits that leave citizens vulnerable.

Scams are now formally recognized as sophisticated cybercrimes by the World Economic Forum, meaning this threat has gone out of proportion and working in silos is no longer an option. Protecting our nation requires an uncompromising whole-of-nation approach. Government, private enterprise, and civil society must sustain this momentum together to engineer a safer, more resilient digital future for all Filipinos.

How PNPI (formerly BancNet) is coordinating the fight against fraud



Elmarie S. Reyes
CHIEF EXECUTIVE OFFICER

PNPI

About PNPI:

Payment Network of the Philippines Inc (PNPI) formerly BancNet, is the Philippines' national payments network and a key financial market infrastructure provider, operating the country's largest ATM network and managing the country's primary ACHs for both real-time and batch electronic fund transfers.

Instant payments have seen explosive growth in the Philippines in recent years. Elmarie Reyes, CEO of Payments Network of the Philippines, Inc. (PNPI), formerly BancNet, explains: “The growth we’ve seen so far is just the tip of the iceberg - there’s potential to do so much more. But reaching this potential means overcoming the barriers that stand in our way, including financial literacy and internet access, but most urgently, reducing fraud and scams.”

From CEO impersonation and phishing to romance scams and money muling, fraud is a pervasive issue, and the scale of financial losses is undermining confidence in the wider digital payments ecosystem.

Reyes expands, “Scams don’t just impact the victim but the whole financial industry. And as fraud becomes more sophisticated and AI-led it is harder to spot, even for those who are highly financially literate - people in my network often come to me to say they’re worried about falling victim. For many Filipinos, the convenience of digital payments still outweighs the risk, but for others they lack the trust to try. We must fight fire with fire and deploy AI-powered solutions that can detect and prevent fraud.”

Banks and financial institutions are doing what they can to protect customers, but tackling the issue in a meaningful way requires a full and coordinated response from government and industry. This is particularly important with increased use of digital wallets, which are subject to different regulation but must offer the same levels of protection to customers. As Reyes explains, “Banks are trying new tactics – for example, using push notifications to alert customers to potential scams – but many of those using wallets are still falling prey to fraud.”

Continue reading on the next page →

How PNPI is coordinating the fight against fraud



Elmarie S. Reyes
CHIEF EXECUTIVE OFFICER

PNPI

About PNPI:

Payment Network of the Philippines Inc (PNPI) formerly BancNet, is the Philippines' national payments network and a key financial market infrastructure provider, operating the country's largest ATM network and managing the country's primary ACHs for both real-time and batch electronic fund transfers.

PNPI is working to build and mobilize a coordinated approach across all financial institutions in the region through its partnership with Mastercard's TRACE Financial Crime solution, which uses advanced technologies to track the flow of funds across the payments system to help identify suspicious activity and money laundering accounts.

As more organizations join the TRACE network, the data pool grows and insights become smarter and more precise. From January 2025 to June 2026, TRACE successfully identified 3,700 mule accounts, and this number will increase significantly as data volumes grow.

Reyes elaborates, "Collaboration is a powerful force to tackle fraud. We must use our combined resources and energy to get ahead of bad actors and build a system that empowers us to operate proactively rather than reactively. Getting this right is the key to building trust in digital payments for people and businesses across the country. If we don't, we risk the Philippines falling behind other countries in the region and becoming a haven for scammers. At PNPI, we are determined to stop this happening."

PNPI is already working on further opportunities to collaborate with private and public sectors in the future, including supporting the creation of a National Scam Centre, using TRACE insights to create a central mule database, and developing enhanced analytics in partnership with Mastercard to stop fraud before it occurs.

Our global research surveyed 58,900 respondents across 42 countries

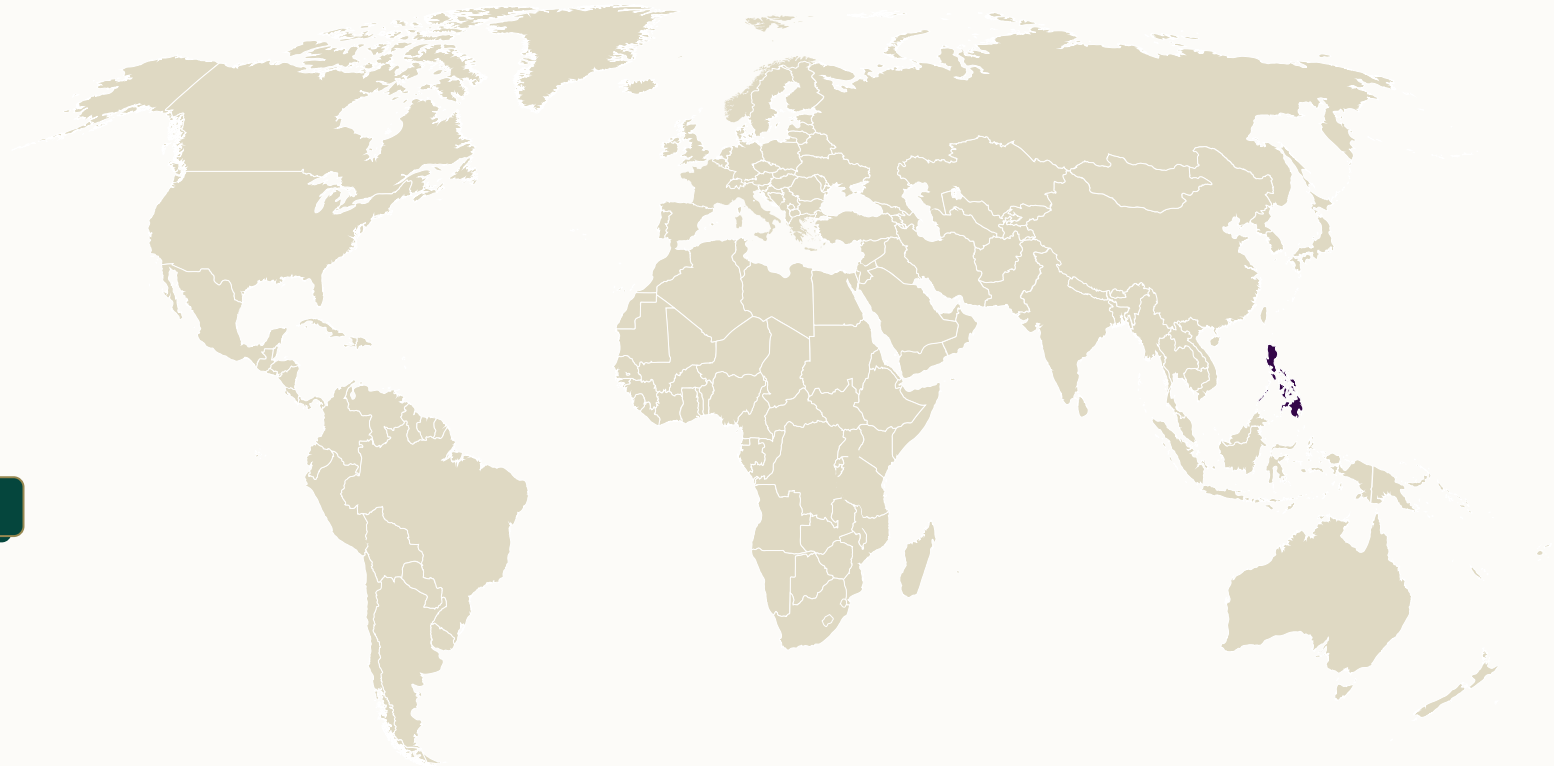
GLOBAL COUNTRIES

Argentina
Australia
Austria
Belgium
Brazil
Canada
China
Denmark
Egypt
France
Germany
Hong Kong
India
Indonesia
Ireland
Italy
Japan
Kenya
Malaysia
Mexico
Netherlands
New Zealand
Nigeria
Pakistan
Philippines
Poland
Portugal
Romania
Saudi Arabia
Singapore
South Africa
South Korea
Philippines
Sweden
Switzerland
Taiwan
Thailand
Türkiye
UAE
UK
United States
Vietnam

ASIAN COUNTRIES

Australia
China
Hong Kong
India
Indonesia
Japan
Malaysia
New Zealand
Pakistan
Philippines
Singapore
South Korea
Taiwan
Thailand
Vietnam

The data in this report will focus on findings within **Philippines**



Who we spoke to in Philippines

Sample size | 1,160 people

Audience | Adults aged 18+ living in Philippines

Weighting | Nationally representative of the Filipino/a adult population on age, gender and region

Methodology | 15-minute online survey

Sample source | Online research panel

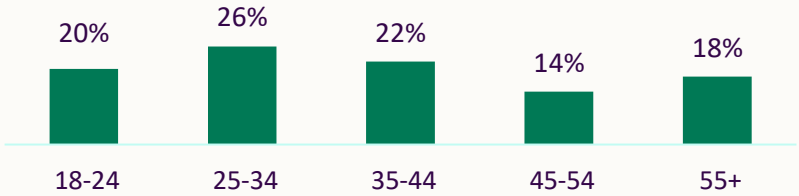
Fieldwork | 16th March – 13th April 2026

Base: All respondents (Base = 1,160)

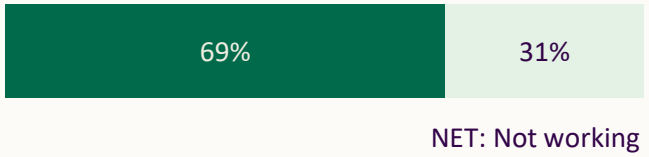
GENDER



GENERATION / AGE



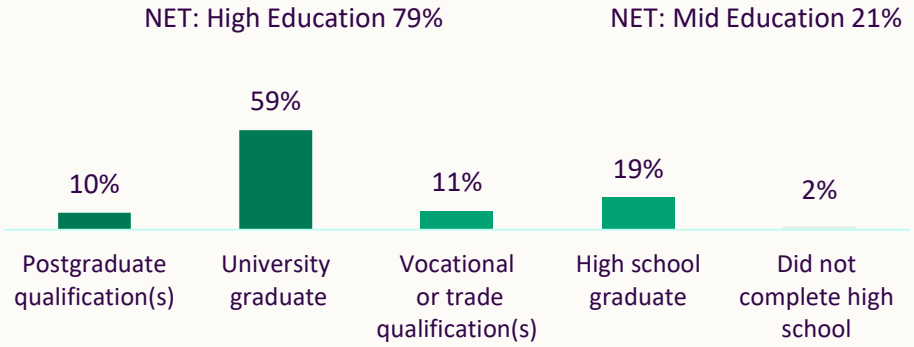
WORKING STATUS



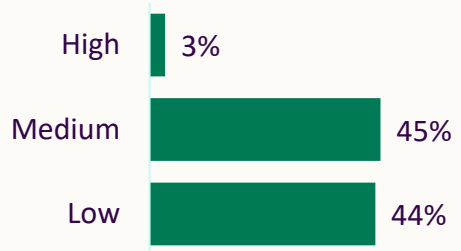
PARENTAL STATUS



EDUCATIONAL STATUS



HOUSEHOLD INCOME



GASA | Gogolook | Global Anti-Scam Alliance

Methodology

VALUE LOST TO SCAMS METHODOLOGY

Identifying scam victims

Respondents are first asked whether they have encountered a scam in the past 12 months (Q2). Those who have, are shown a list of common scam types, with the option to select other scams not listed (Q6). Respondents who reported interacting with at least one scam are then asked whether they have either given money to a scammer or shared personal information that resulted in money being stolen (Q7A).

Verifying reported financial losses

Respondents who reported a financial loss are asked a series of validation questions to establish the total amount lost (Q12A to Q12D). First, they select a loss band from a predefined ranges, with upper and lower limits informed by the 2025 distribution of losses. Respondents reporting higher value losses (top 50% of reported losses in 2025) are asked to confirm or amend the loss range they initially selected. All respondents indicating to have suffered a loss, are then asked to provide the exact amount lost. Subsequently, again if the entered value (open numeric) fell into top 50% of highest reported losses of 2025 are again given the opportunity to reconfirm or revise their answer.

Data cleaning and quality checks

During cleaning, responses are removed if they contained unresolved contradictions for value lost, if respondents changed their answers multiple times or if open numeric values do not align with selected bands. Respondents are also removed if their losses are higher than their annual household income unless substantiated by reports of incurred debt or a qualitative description consistent with the scale of the financial loss.

Calculating total value lost

The final value lost to scams was calculated using the mean loss per victim and extrapolated to the national adult population using official population statistics.

In Philippines, 165 of 1,160 respondents reported losing money to scams, equating to an estimated 11,683,393.45 affected adults nationally.

Multiplying this by the average loss (₱10426.9) produces an estimated total loss of ₱121,821,575,145.83

Population statistics sourced from: US Census

To view the questions and definitions provided for scam encounters, interactions, and money lost, please consult the appendix.

CONVERSION RATES

The following conversion rate was used in this report:
1 USD equals 56 PHP

This rate was taken between 16 March 2026 - 13 April 2026

Click here to see full overview of available value lost statistics

The Scam Funnel in Philippines

58% are confident they recognize a scam

Total participants (1,160)

84% encountered a scam*

Top reasons for not interacting with scams
53% Message or request did not seem legitimate
47% I searched online and found warnings about it
43% The request felt too good to be true

20% of parents say their child has been scammed too

44% interacted with the scammer
(60% among those that encountered a scam)

Top reasons for not giving money
53% request was suspicious
45% links, attachments, or websites looked fake or slightly incorrect
38% offer felt too good to be true

15% lost money or data that led to money lost (scammed)
(34% among those that interacted with a scam)

Most common scams interacted with
24% Shopping scam
22% Investment scam
22% Employment scam

82% of those scammed say it impacted their mental wellbeing

38% of those scammed say it happened more than once

4% reported the scam to authorities
(29% among those that lost money to a scam)

12% of those who reported their losses say their money was reimbursed by the organization they reported to

The research covered four key topics

You can navigate through pages and sections of this report using the clickable icons in the navigation bar at the base of each slide.

Use the button to return to this page.

Click to navigate through sections

SCAM ENCOUNTERS

Exploring how often people encounter scams, the platforms and channels scammers use, how frequently scams are reported, and which measures are most effective for recognizing and avoiding them.

SCAM INTERACTIONS

Understanding the full range of consumer interactions with scams, from initial engagement to sending money or personal information, and identifying the factors that prevent financial loss.

COST OF SCAMS

Assessing the true cost of being scammed, including financial, emotional and behavioral impacts, as well as the techniques scammers use that work and the risk of revictimization.

SCAM PREVENTION

Examining the self-protection tactics consumers rely on, and their perceptions of how public bodies and commercial organizations should help prevent and resolve scams.

Throughout this report, comparisons to the Asian average have been made either in brackets (X%) or alongside the country level data as follows:



Similarly, any comparisons made from this year and last year will be made either in brackets (X%) or displayed as follows:



To find out more about the report and its authors:

ABOUT THE REPORT

ABOUT THE AUTHORS

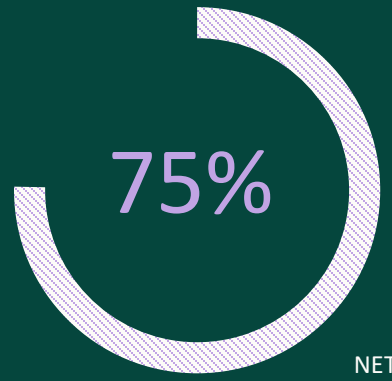
GASA Global Anti-Scam Alliance | Gogolook |



SCAM ENCOUNTERS

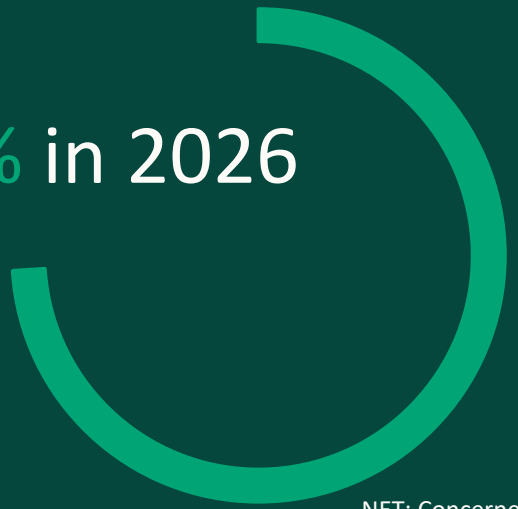
Exploring how often people encounter scams, the platforms and channels scammers use, how frequently scams are reported, and which measures are most effective for recognizing and avoiding them.

Three in four remain concerned about being scammed in Philippines



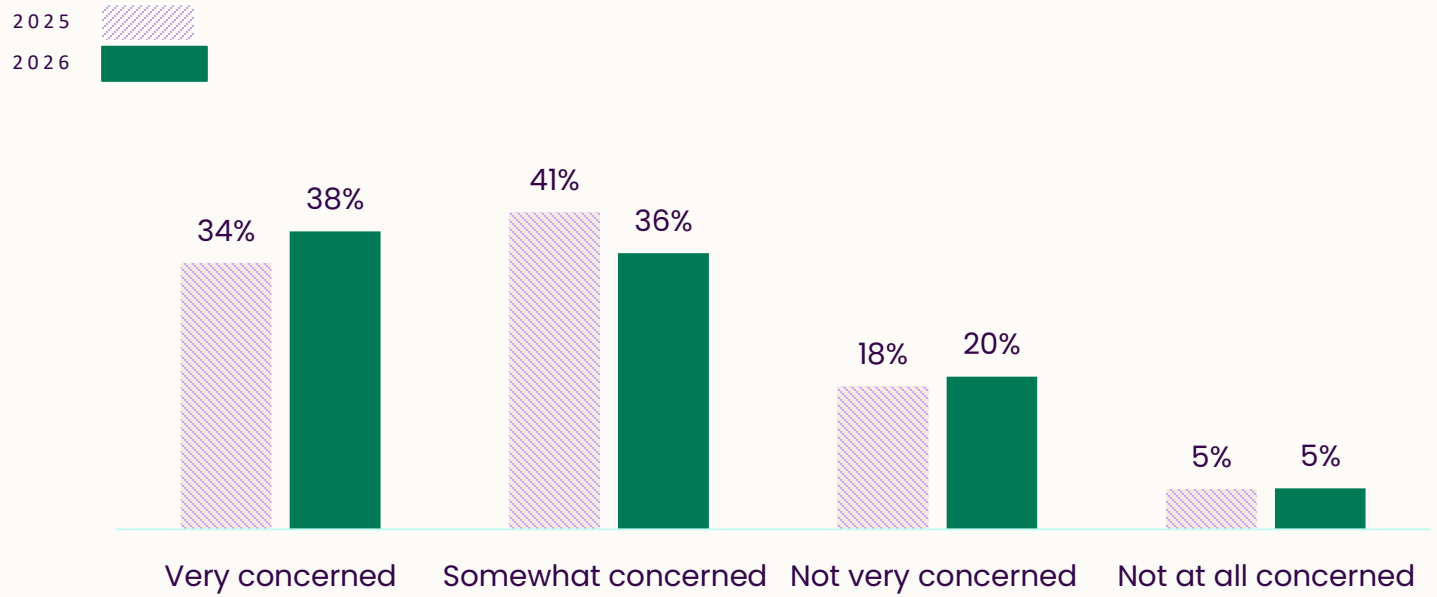
NET: Concerned

are concerned about being scammed in 2025 vs



NET: Concerned

Proportion concerned about being scammed in 2025 vs 2026



Q1B. How concerned were you about being scammed this time last year, and how concerned are you about being scammed today [=2026] / this time last year [2025]? Base: All respondents (1,160)

Nearly three in five Filipino/a adults are confident in their ability to spot scams

Confidence in recognizing scams

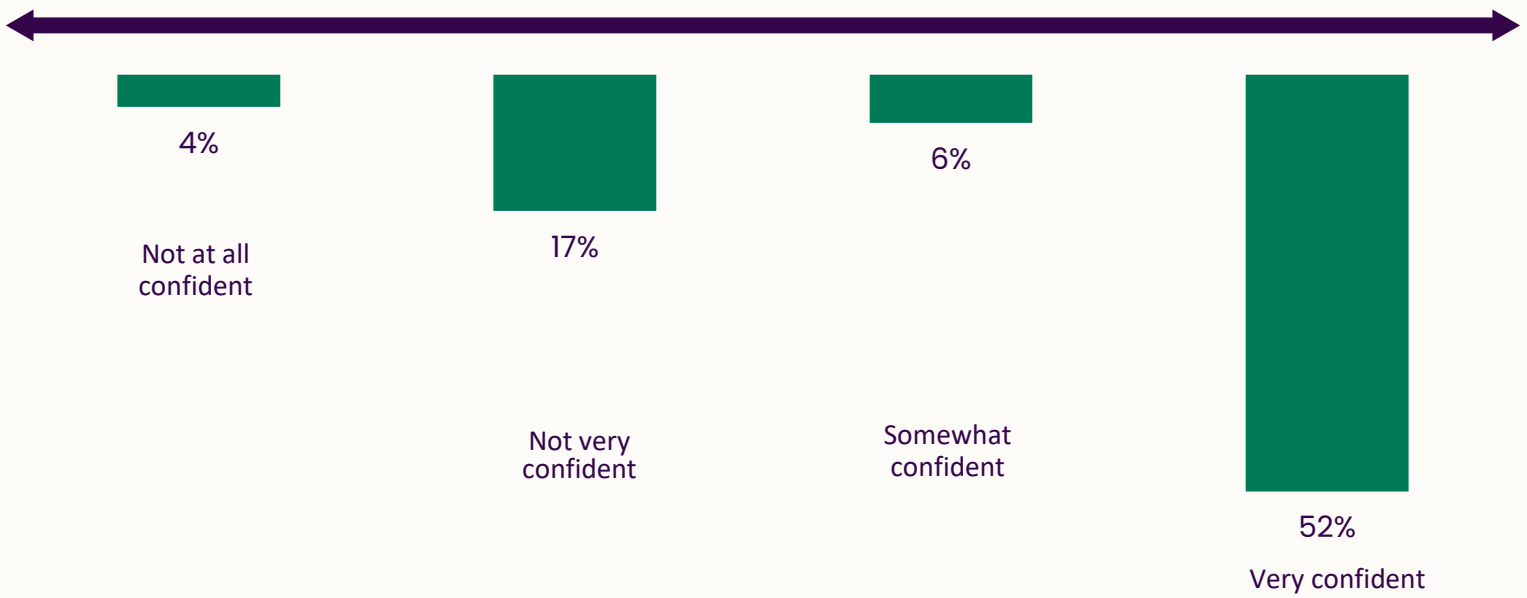
Scam-recognition confidence in Philippines skews strongly toward **18-24** year olds (64%) working (61%). By comparison, lack of confidence is much higher among **women (24%) Gen X (27%), those aged 55+ (32%),** currently not working (30%), those living in rural areas (25%) and with a mid education levels (29%).

21%

Do **not feel confident** in their ability to recognize scams

58%

Do **feel confident** in their ability to recognize scams



Q1A. How confident are you, if at all, that you can recognize scams? Base: All respondents (1,160)

More than eight in ten Filipino/a adults encountered a scam in 2026 – showing an increase from 2025

Prevalence & frequency of encountering a scam

84%

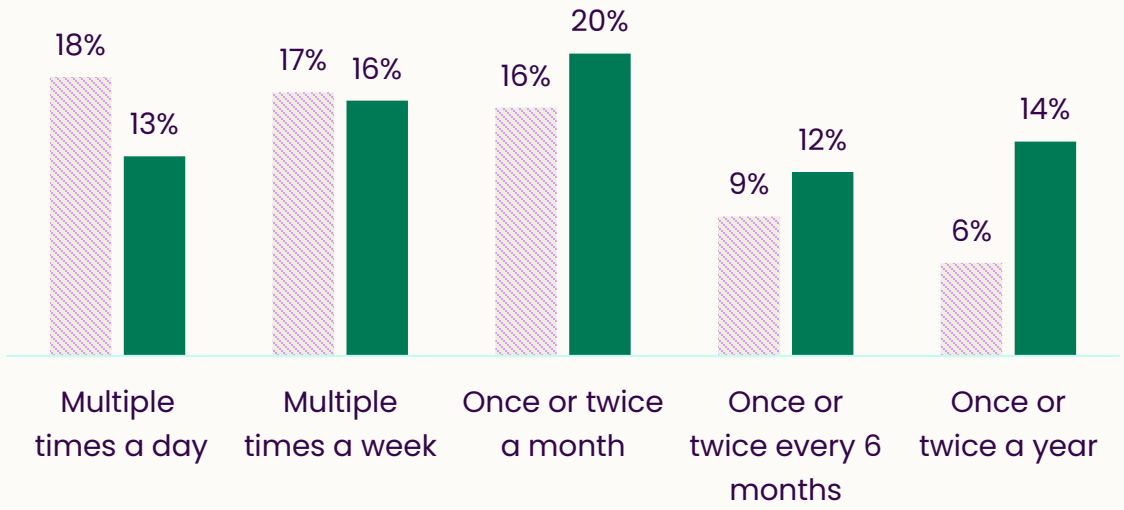
Of Filipino/a adults encountered a scam in 2026

Vs.

77%

Who encountered a scam in 2025

Scams are most commonly encountered on a **monthly** basis



Which equates to

151

scam encounters on average per person, per year, in **Philippines**

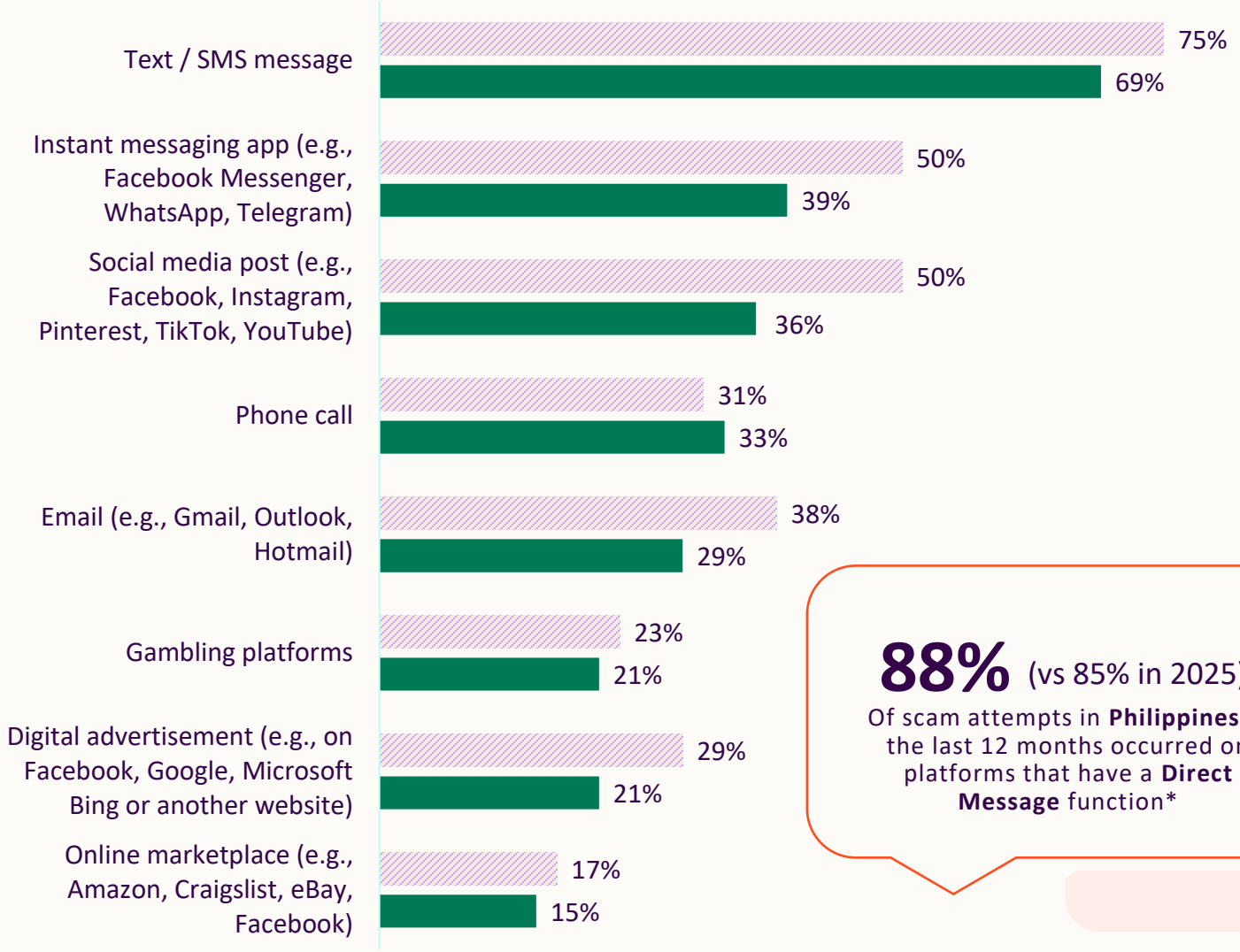
2025
2026

Q2. How often, if ever, do you encounter scam attempts? Base: All respondents (1,160)

SMS and text messages remain most common scam contact channel in the Philippines

Communication platforms where scams were encountered – top 8





88% (vs 85% in 2025)
Of scam attempts in **Philippines** in the last 12 months occurred on platforms that have a **Direct Message** function*

Q3. You said you have encountered a scam in the last 12 months. Through which communication channel(s) did scammers approach you in the last 12 months? Base: All who have encountered a scam (864)
*Platforms with a direct message function include Text / SMS message, Instant messaging app (e.g. Facebook Messenger, WhatsApp, Telegram), Online Community or Forum (e.g. Discord, Reddit), Dating site or app (Match, Tinder), Video gaming (Roblox, Steam, Xbox, PlayStation, Online marketplace (e.g. Amazon, Craigslist, eBay, Facebook).

Facebook and Gmail are the platforms where victims are most likely to encounter scams

Top 10 online platforms that victims report were used by scammers to contact them in the last 12 months in Philippines



58%



33%



29%



23%



19%



12%



12%



10%



9%

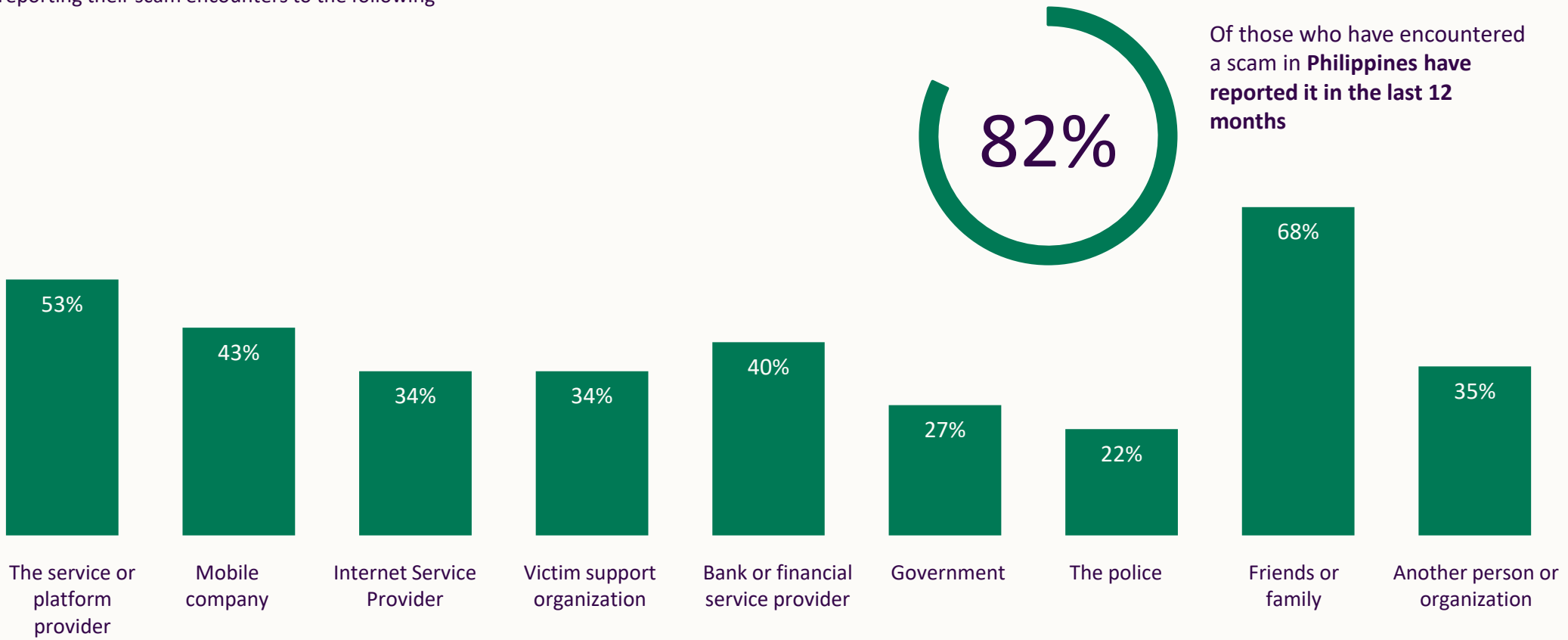


7%

Q4. You said you have encountered a scam in the last 12 months. Through which, if any, of the following global service or platform(s) did scammers contact you in the last 12 months? All who have encountered a scam (n=864)

Filipino/a adults are three times more likely to report a scam encounter to their friends or family as they are to the police

Proportion reporting their scam encounters to the following



Q5. You said you have encountered a scam in the last 12 months. How many times, if any, have you reported a scam encounter to the following in the last 12 months? Base: All who have encountered a scam NET: Has reported a scam attempt at least once (864)

Filipino/a adults report most frequently that the media (i.e news coverage and social media post) have been most effective in helping them recognize or avoid scams

Most effective strategies to recognize or avoid scams





Q25. Which of the following have been most effective in helping you recognize or avoid scams? Select all that apply. If you haven't received any information on how to recognize or avoid scams select N/A. Base: All respondents (1,160)



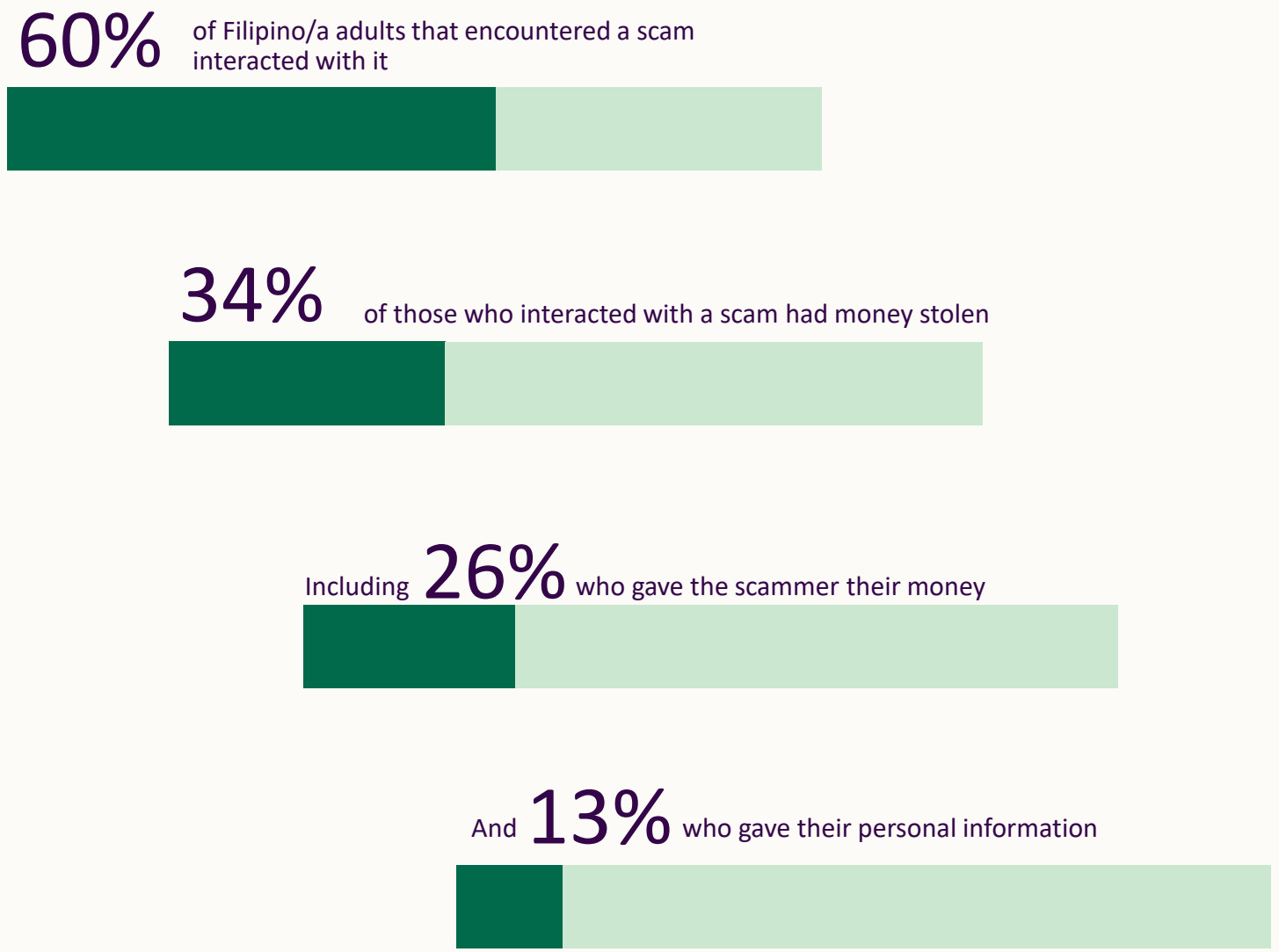
SCAM INTERACTIONS

Understanding the full range of consumer interactions with scams, from initial engagement to sending money or personal information, and identifying the factors that prevent financial loss.

Three in five Filipino/a adults that encounter a scam attempt go on to interact with it

One in three who interact with a scam have money stolen, either by giving the scammer money, personal information, or both

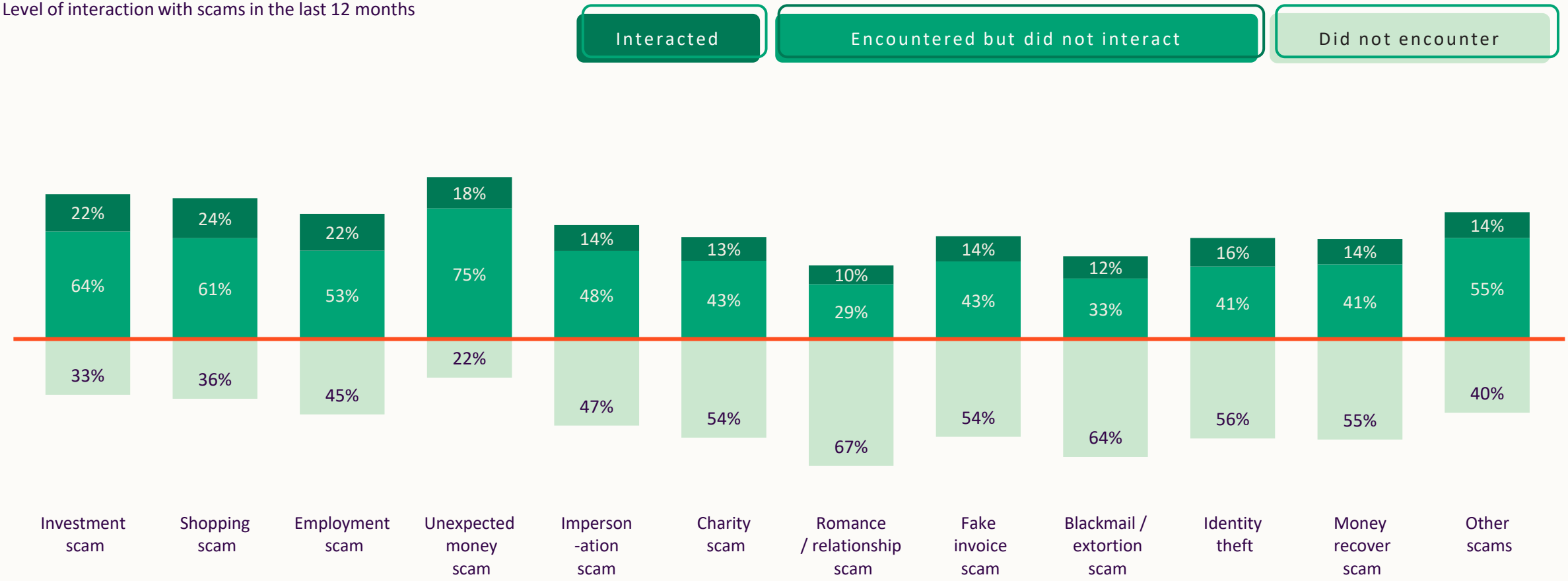
How victims move through the scam funnel



See footnotes for question text and base size. Note: bottom 3 datapoints are taken from Q7A which is a multiple-choice question.

Filipino/a adults most commonly interact with shopping, investment and employment scams

Level of interaction with scams in the last 12 months



Q6. Scams are becoming increasingly sophisticated, meaning anyone could be affected. Between 2024 and 2025 it is estimated that 202.3 billion people interacted with scam encounters. We'd like to understand how, if at all, you interacted with scams you encountered in the last 12 months. Interacting with a scam can range from simply opening or reading a message to replying, picking up a call, clicking links, visiting fake websites, or engaging in back-and-forth communication. You said you experienced scam encounters in the last 12 months. To what extent, if at all, did you interact with the following types of scams? Answer based on your interactions with the scammer before you realized it was a scam or tried to verify whether it was legitimate. Investment scam: A scammer approaches you with a supposedly lucrative investment opportunity, often promising guaranteed returns or no risk, and asks you for money or financial details to "secure" the investment. Base: All who have encountered a scam (864)

The main reason Filipino/a adults give for not interacting with scams is that the message did not seem legitimate and online searches led to warnings being discovered about it

Top 10 reasons for not interacting with scam encounters

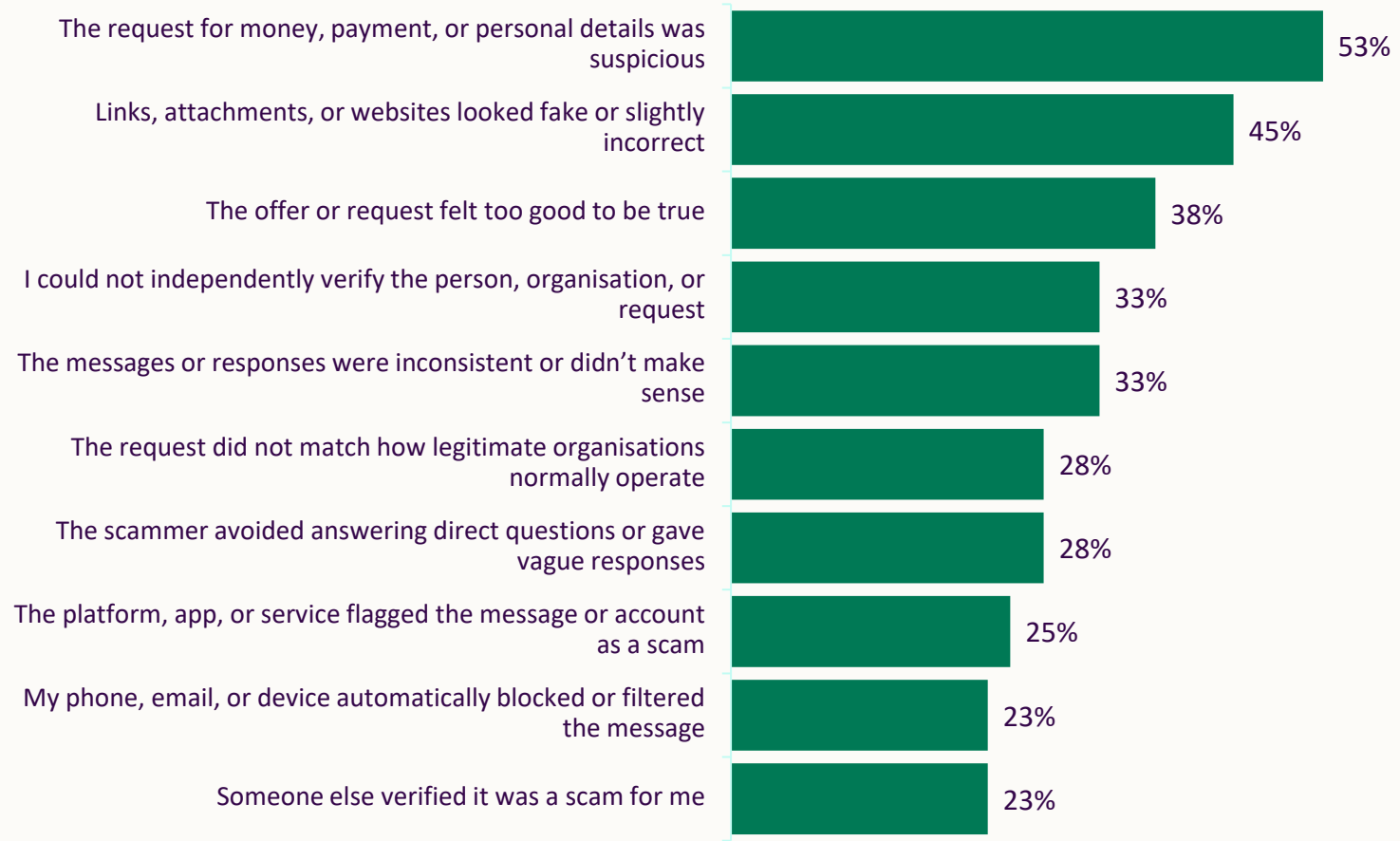
41% of Filipino/a adults say they recognized common scam warning signs



Q8. Thinking about the scams you encountered but did not interact with in the last 12 months, what stopped you from interacting with the scammer? Base: All respondents that did not interact with at least one scam they encountered: (785)

Requests for money, payment, or personal details being suspicious are the main reasons Filipino/a adults do not go on to hand money over to scammers

Top 10 reasons for not giving money to scammers when interacting with scam encounters



Q9. Thinking about the scams you interacted with but did not give money or personal information to in the last 12 months, what stopped you from continuing the interaction? Base: All respondents that did not give money or personal information that led to money lost after interacting with a scam (229)



COST OF SCAMS

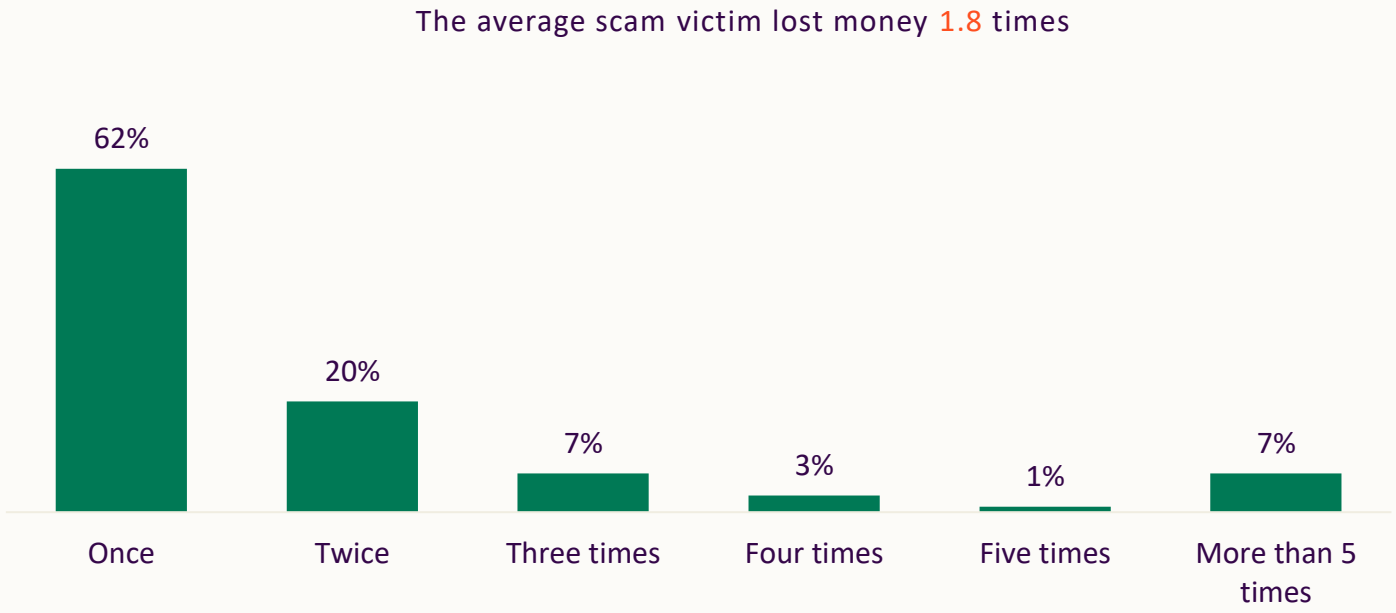
Assessing the true cost of being scammed, including financial, emotional and behavioral impacts, as well as the techniques scammers use that work and the risk of revictimization.

Nearly two in five of those who lost money say it happened more than once

38%

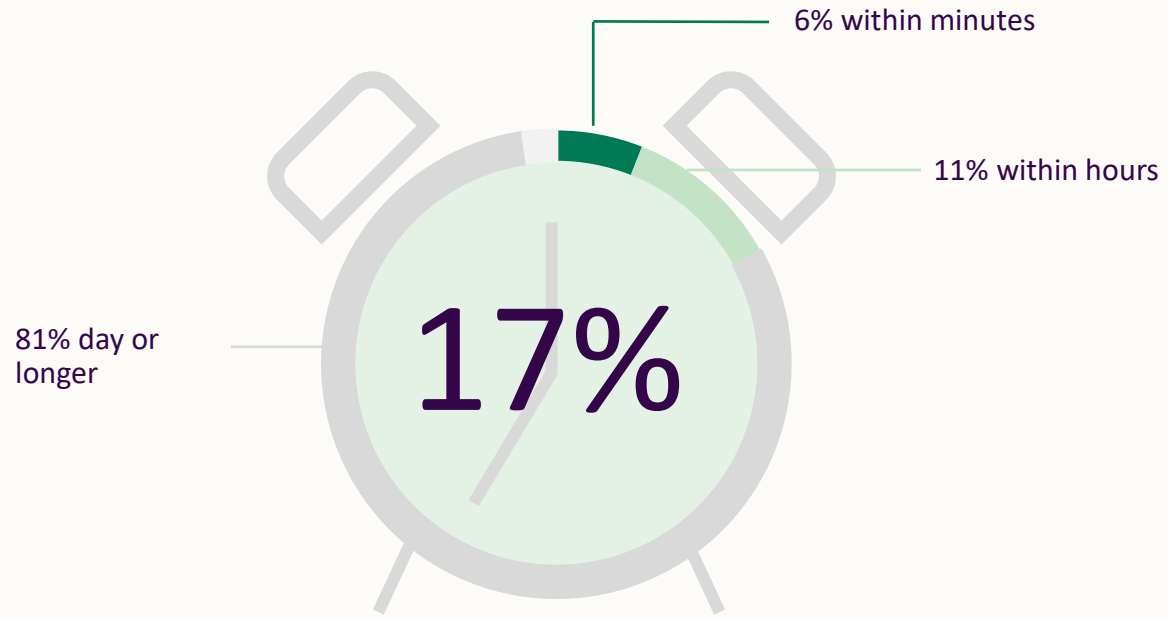
Of **Filipino/a** adults lost money to scams more than once

Prevalence of revictimization



Q10A. You said you have given scammers money or personal information that led to your money being stolen in the last 12 months. How many times has this happened in the last 12 months? Answer based on the number of scam incidents, even if it involved the same type of scam or the same scammer. Do not count multiple payments or transfers made within a single scam incident. Base: All respondents that lost money to a scam (175)

Four in five of those that lost money to a scam say that the scam lasted a day or longer



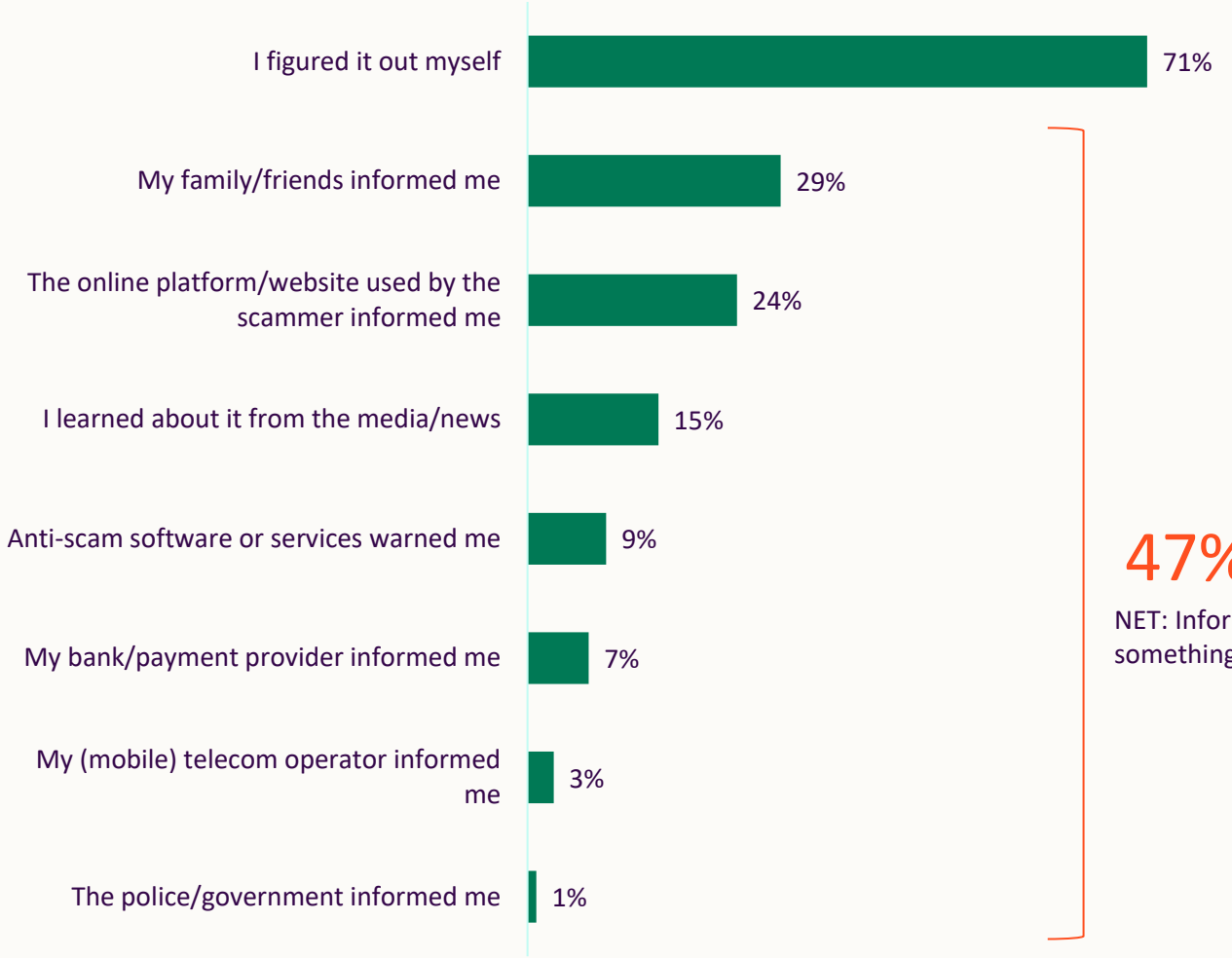
of scams happen within a day of first being contacted by the scammer

Q10B. 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. Only think about the most recent time when you were scammed and lost money. Base: All respondents that lost money to a scam (175)

GASA Global Anti-Scam Alliance | Gogolook

Self-discovery remains the primary way Filipino/a scam victims discover they've been scammed

How victims discovered they were scammed



47% in 2026 compared to 49% in 2025

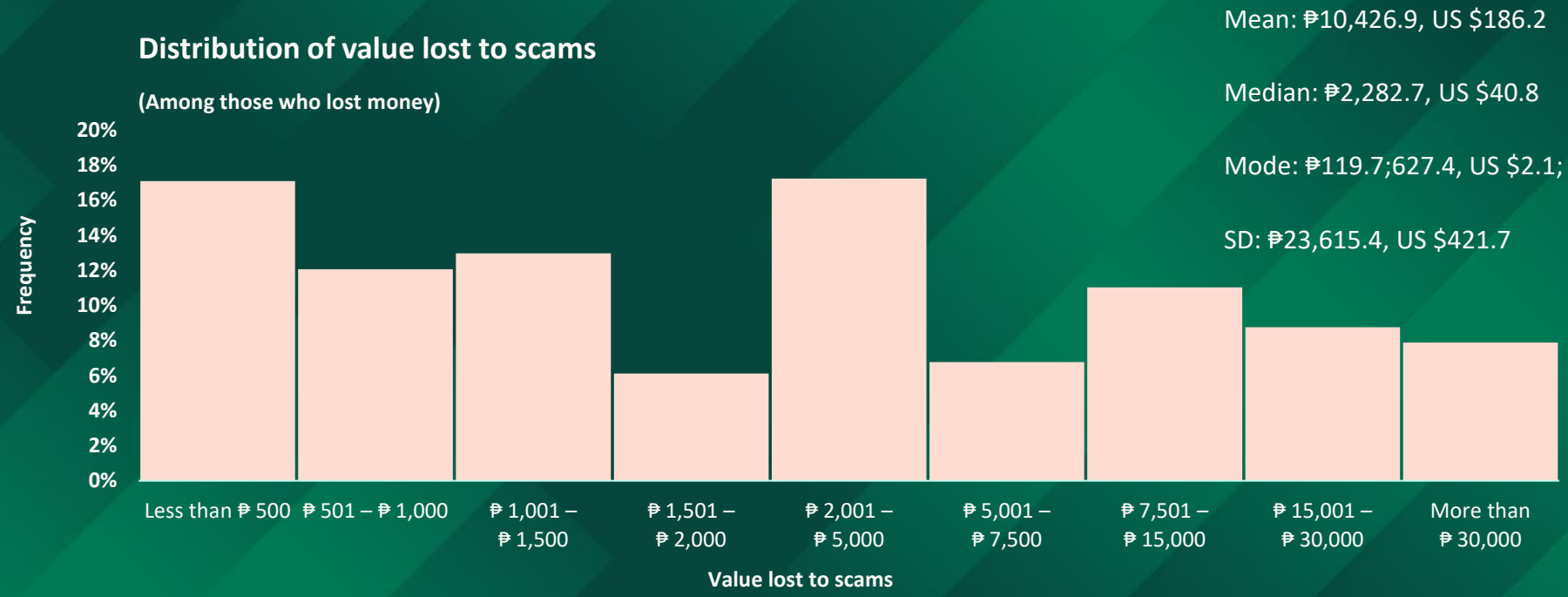
NET: Informed by someone / something else

Q11. How did you discover you were scammed? Continue to think about the times you've been scammed and lost money in the last 12 months Base: All respondents that lost money to a scam (175).

Filipino/a adults lost ₱121,8 billion in the last year with an average loss of ₱ 10,426.9

(US $2.18 billion)

(US $186.2)



Mean: ₱10,426.9, US $186.2

Median: ₱2,282.7, US $40.8

Mode: ₱119.7;627.4, US $2.1; $11.2

SD: ₱23,615.4, US $421.7

See appendix . Base: All respondents that lost money to a scam (n=175).

Click here to see full methodology for average loss calculations

A trusted contact became a scam

I was convinced to send ₱6,000 through GCash after receiving a message from what I believed was a friend's account. It was only later that I learned the account had been hacked and I had actually been dealing with a scammer

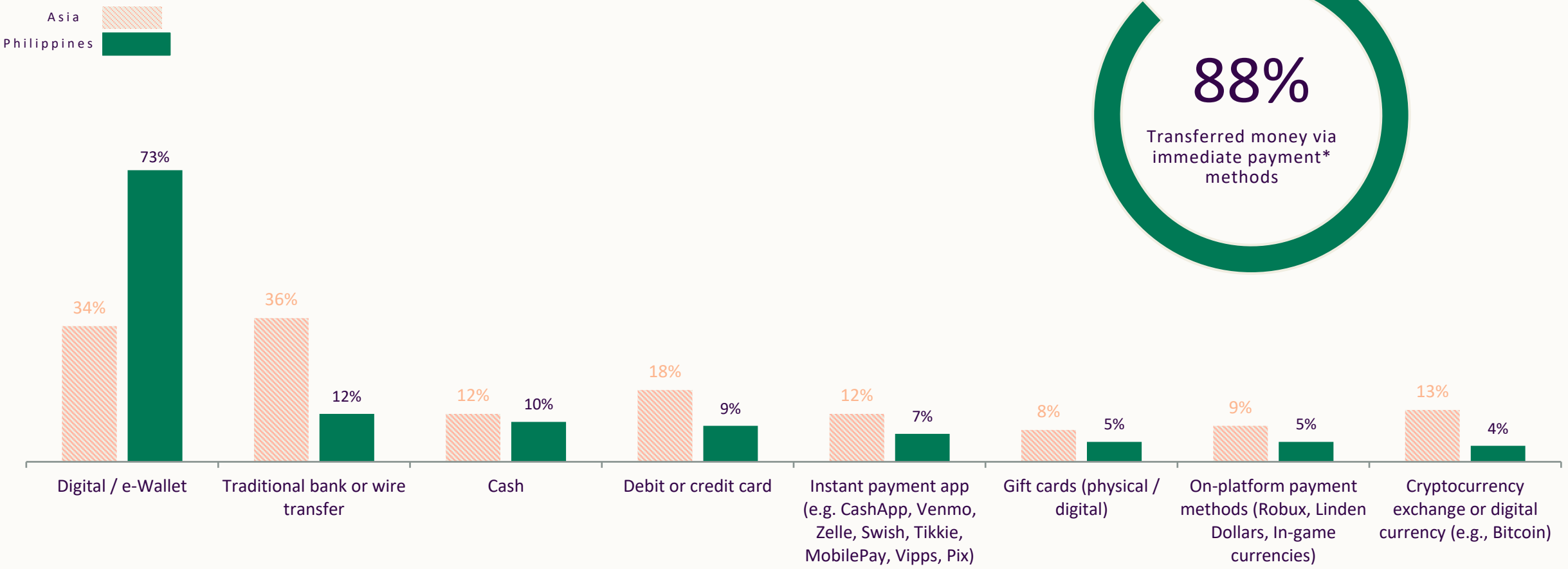
The dream job that cost thousands

There was an employment opportunity in the United States, but I was asked to pay $1,900 to the agency first. Thankfully, my parents and relatives warned me that it was a scam before I sent more money

D12D. Please describe the scam you experienced in the last twelve months where you lost money. If you have been scammed multiple times, describe the scam where the most amount of money was stolen. Base: All respondents that lost money to a scam (n=141)

Most dominant way Filipino/a victims send money to a scammer is through digital / e-wallets

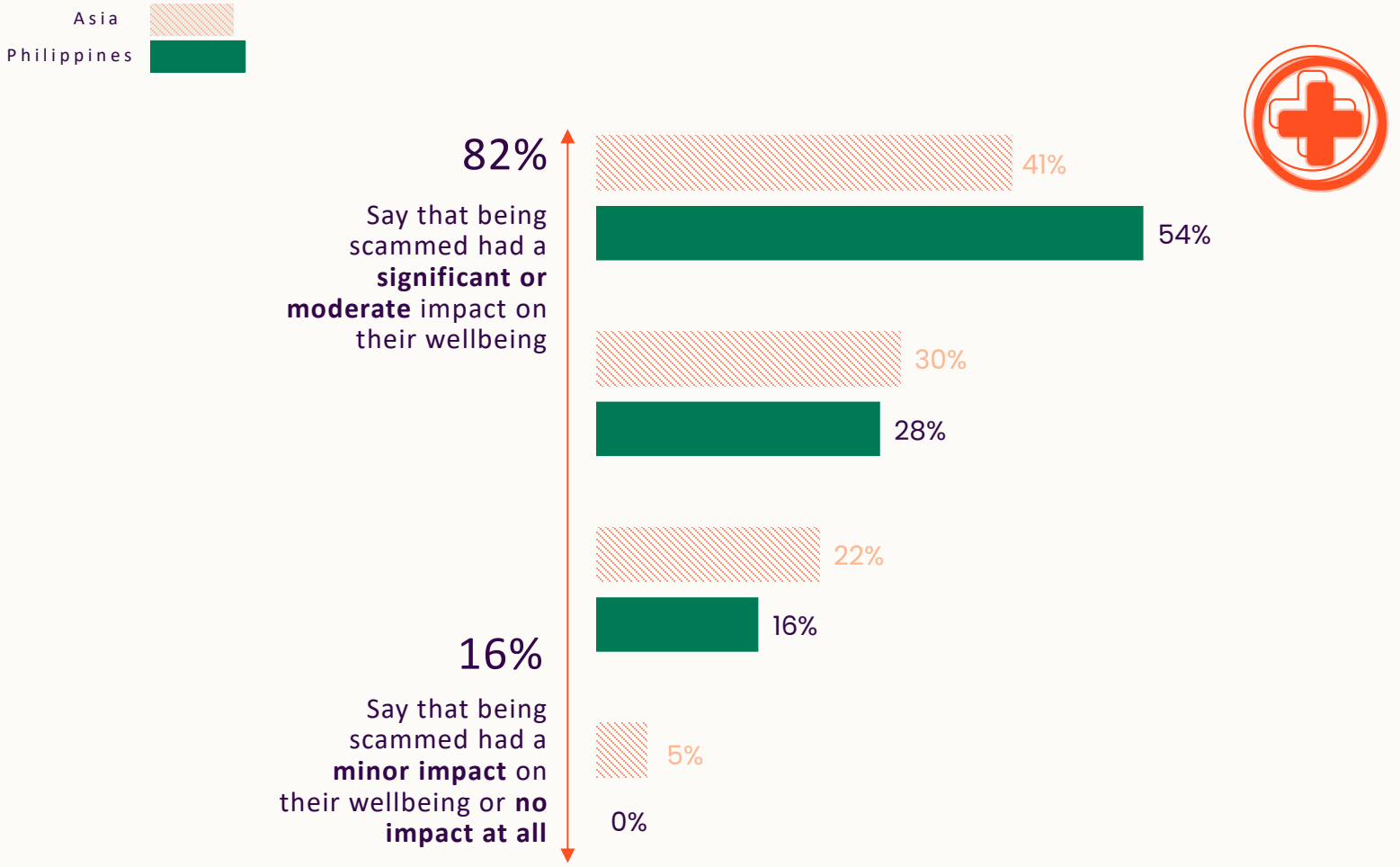
Top 8 payment channels scammers received the payment



Q13. How did the scammer receive your money? Continue to think about the times you've been scammed and lost money in the last 12 months. . Base: All respondents that lost money to a scam (Asia n=1761 | Philippines (175) | *Immediate payment include Instant payment app, gift cards, digital / e-wallet, cryptocurrency exchange and on-platform payment methods

Four in five victims say being scammed impacted their wellbeing – a sharp increase from last year

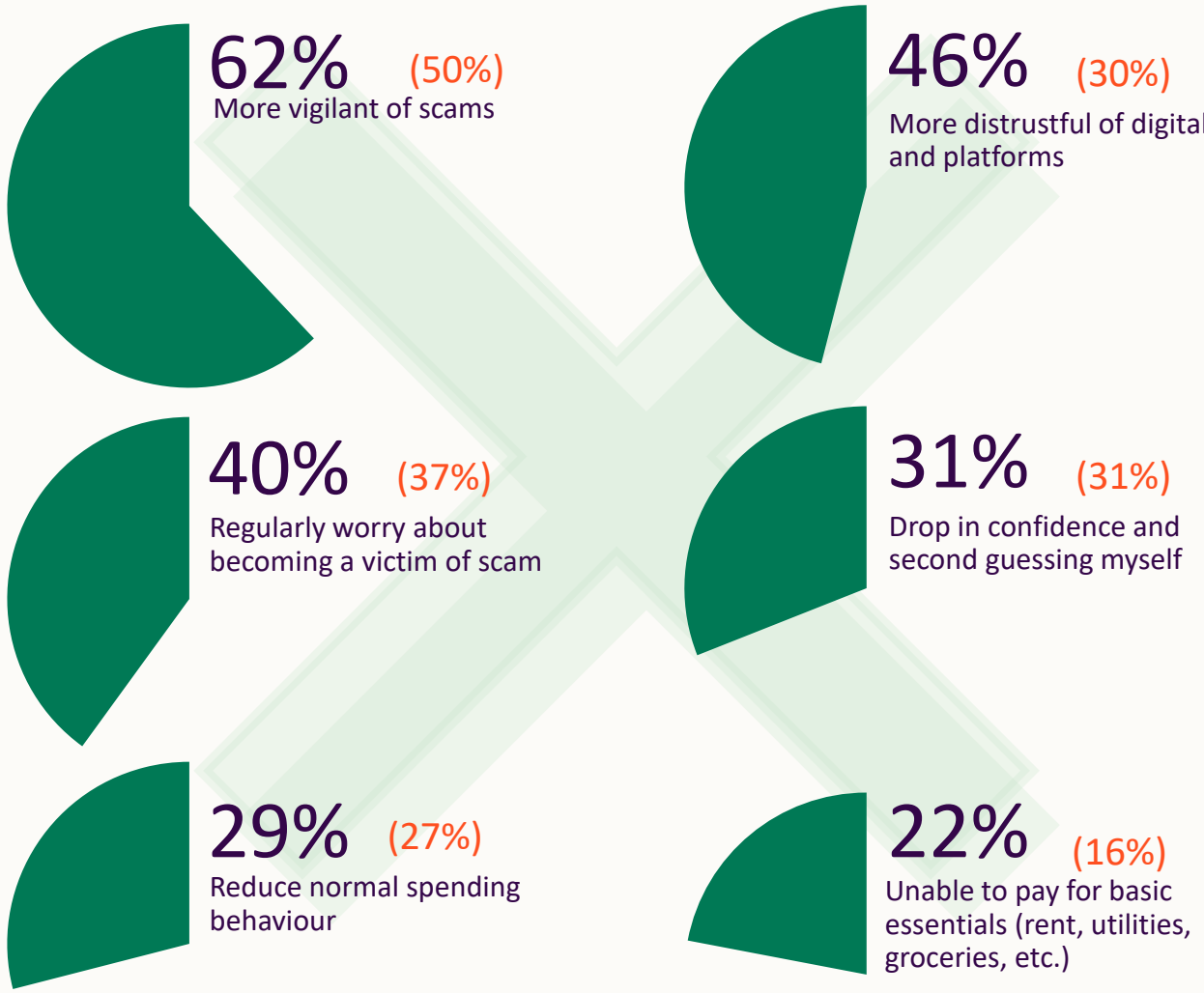
Impact of being scammed on wellbeing



Q14. To what extent did the scam impact your mental wellbeing? Continue to think about the times you've been scammed and lost money in the last 12 months. Base: All respondents that lost money to a scam (Asia n=1761 | Philippines (175)

One in five of those who lost money to a scam is unable to pay for basic essentials as a consequence of being scammed

Impact of scams on victims and their family – top 6



(X%): Asia

Q15. How has the scam(s) impacted you and your family? Continue to think about the times you've been scammed and lost money in the last 12 months. Base: All respondents who lost money to a scam (Asia n=1761| Philippines (175)

Filipino/a victims say scammers were successful because…

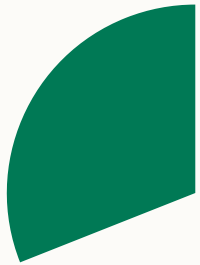
Reasons why scams were successful – top 6



39% (29%)
I trusted the person or message at the time



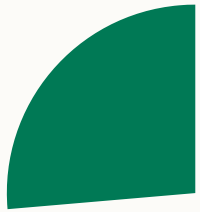
38% (33%)
The situation was convincing and realistic



31% (29%)
The scam communication looked genuine e.g. realistic emails



30% (24%)
The offer was too attractive to ignore



29% (28%)
Scammer pretended to be a legitimate organization



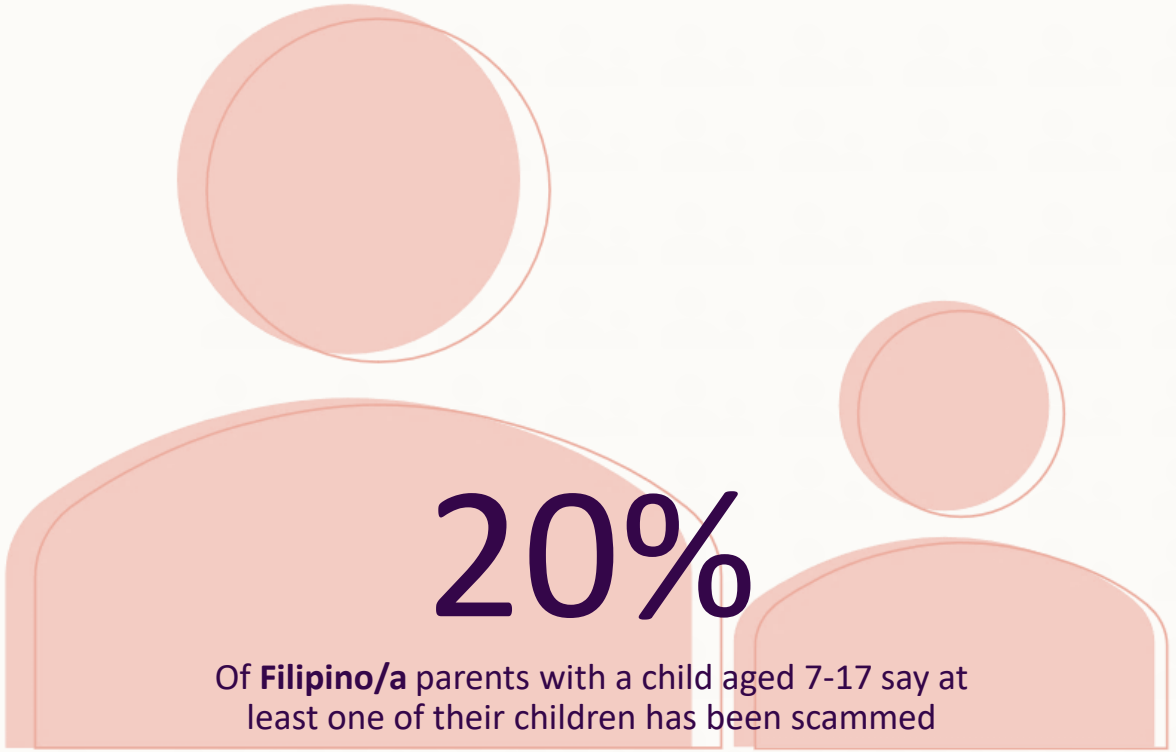
25% (23%)
Thought the payment was secure or protected

(X%): Asia

Q16. How do you think the scammer was able to steal your money? Select all that apply. Continue to think about the times you've been scammed and lost money in the last 12 months. Base: All respondents who lost money to a scam (Asia n=1761 | Philippines (175)

One in five parents say their children have experienced at least one scam

Proportion of parents reporting scam experiences among their children



20%

Of **Filipino/a** parents with a child aged 7-17 say at least one of their children has been scammed

Q19. Have any of your children between the age of 7-17 been scammed? As a reminder, scams are fraudulent or deceptive acts to obtain money and/or personal information. Base: All respondents with children aged 7-17 (384)

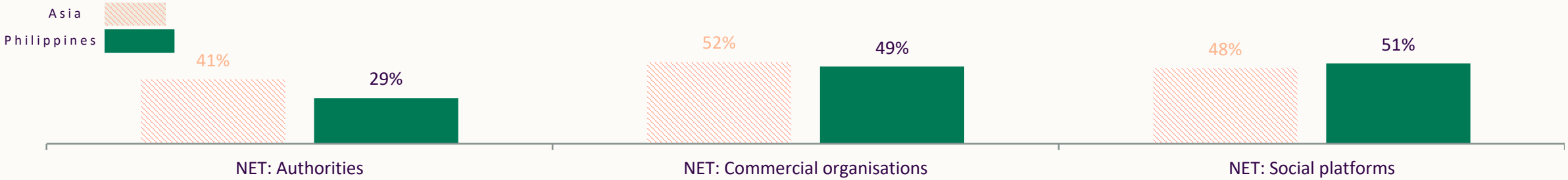


SCAM PREVENTION

Examining the self-protection tactics consumers rely on, and their perceptions of how public bodies and commercial organizations should help prevent and resolve scams.

Scams were most likely to be reported though social channels, followed by commercial platforms of anti-scam website and banks

Channels / organizations scams reported to – top 10

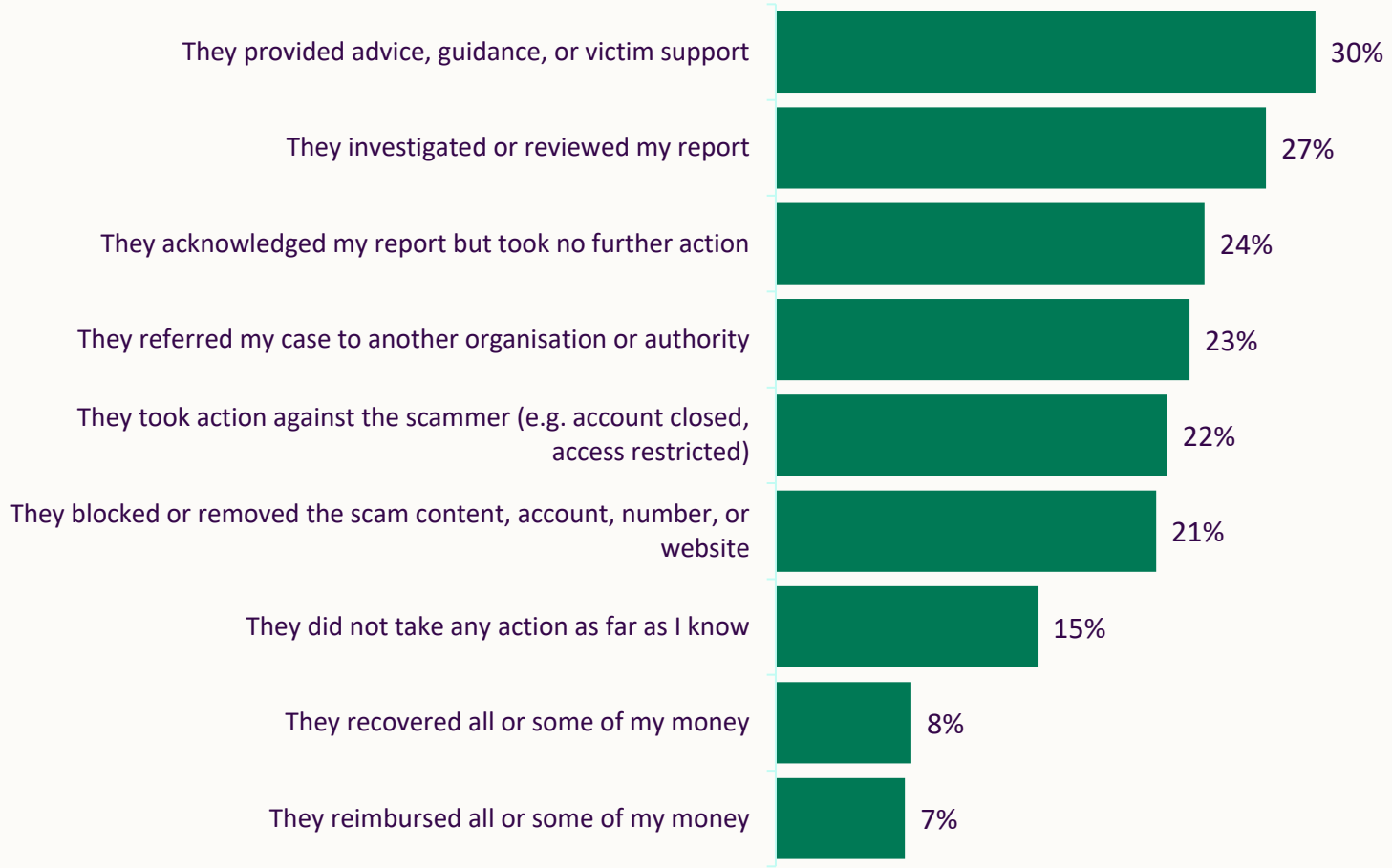


Local or national Police	15%	Anti-scam app/website	19%	Family and Friends	38%
National reporting website	8%	My bank/payment provider	19%	Social platform	24%
Financial regulator	8%	Internet service provider or hosting company	13%	Online review site	8%
Consumer protection authority or organization	5%	E-commerce /marketplace	11%		
		Telecom / mobile operator	10%		
		Cryptocurrency exchange	4%		

Q17. Who did you report the scam to? Continue to think about the times you've been scammed and lost money in the last 12 months. If you did not report the scam, select N/A.As a reminder your answers are anonymous. We appreciate your open and honest answers. Base: All respondents who lost money to a scam ((Asia n=1761| Philippines (175)

Only one in eight scam victims who report their money loss are able to recover any money

12% of those who reported their losses had money recovered or reimbursed



NET: Action taken across: National reporting website, Financial regulator, Local or National Police, Consumer protection authority or organization, E-commerce /marketplace, Online review site, Social platform, Internet service provider or hosting company, bank / payment provider, Cryptocurrency exchange, Telecom / mobile operator, The anti-scam app / website

Q18. When you reported the scam to the following organizations, what action, if any, was taken by the organization? Base: All respondents that lost money in a scam and reported it to an organization NET All organizations (125)

Across Asia, scams go unreported predominantly due to practical barriers and confusion

Asian barriers to reporting scams

16%

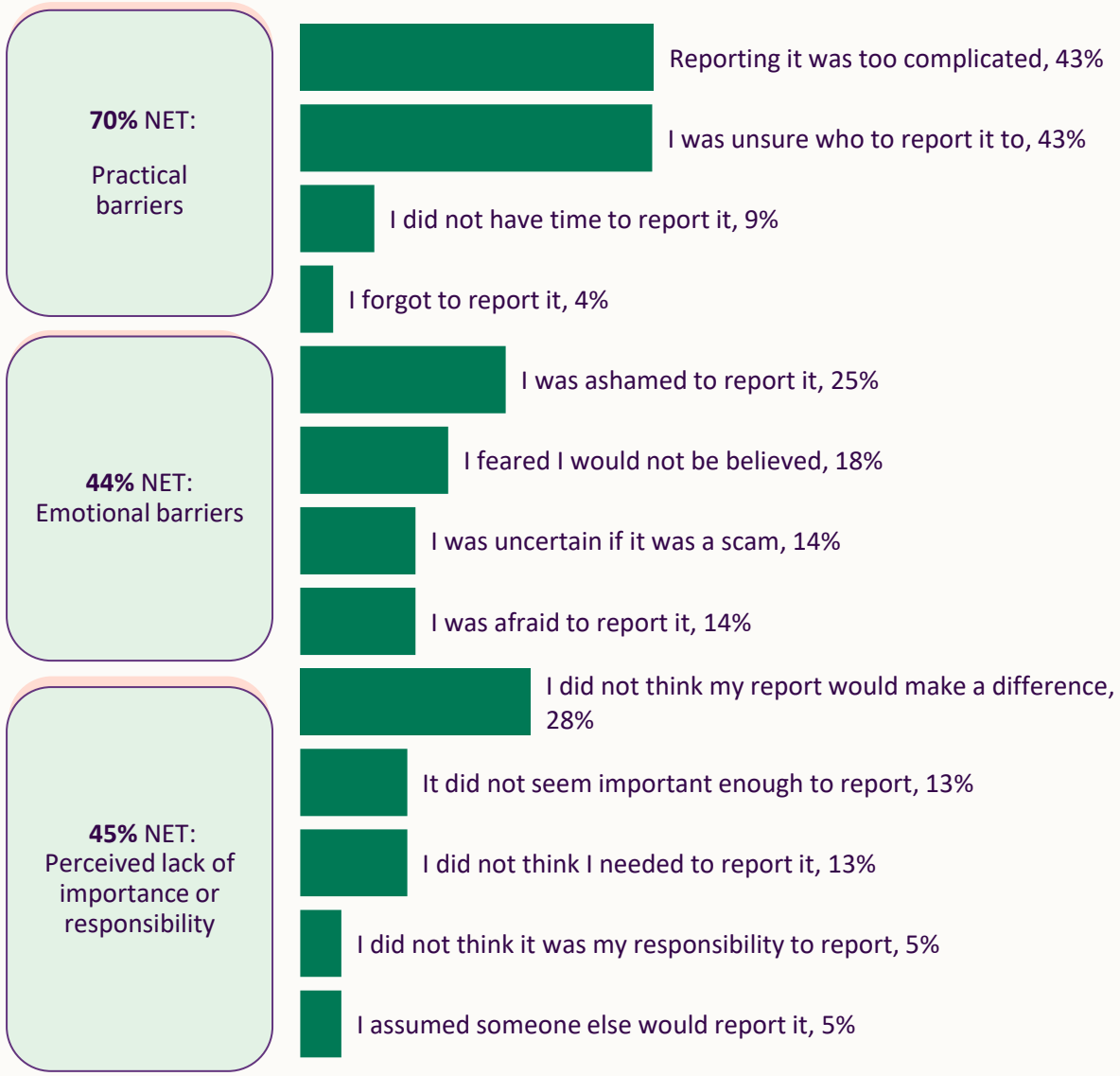
Of those experiencing a scam in the last 12 months and lost money Asian did not report it

4%

Say there was no reason for them to report the scam

28%

Did not think their report would make a difference



Q17. Who did you report the scam to? Base: All respondents that lost money to a scam (Asia n=120) | Q20. What reasons might you have to not report a scam?. Base: All respondents that did not report the scam to an organization (Asia n=431).

Half of Filipino/a adults, follow the rule if too good to be true to be vigilant and check for review on the same or other website

Steps taken to check legitimacy of offer





Q24. What steps do you take to check if an offer, messages, or requests are real or a scam? Base: All respondents (1,160)

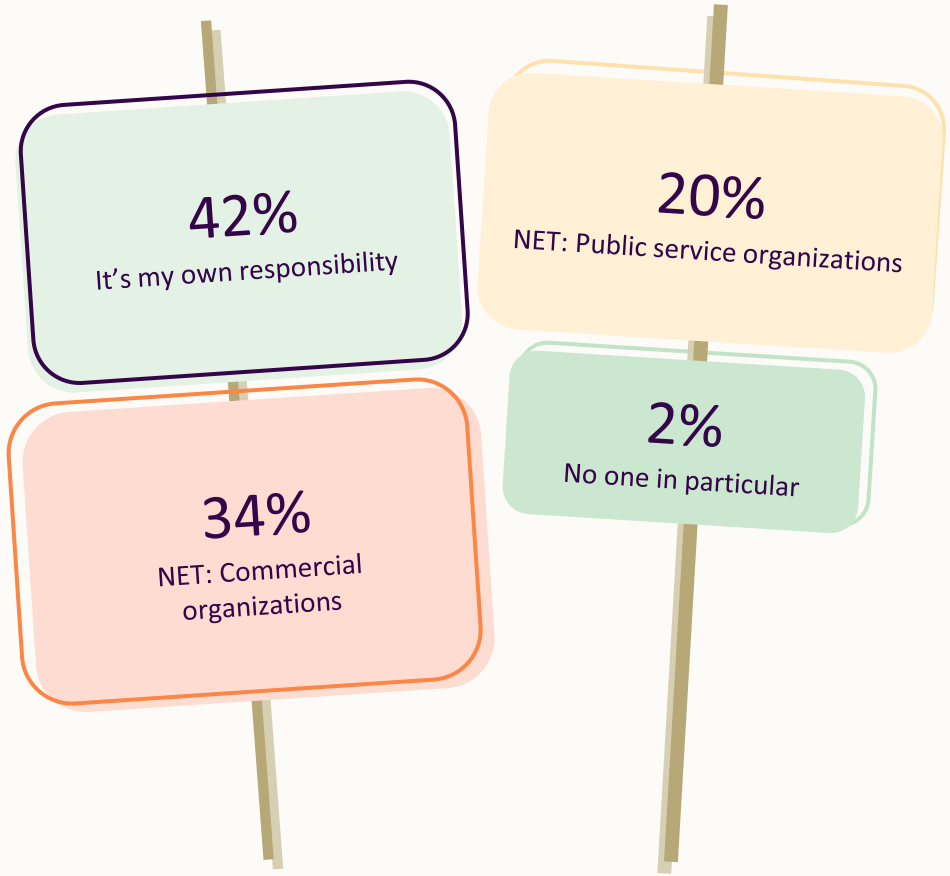
Filipino/a adults see themselves as primarily responsible for staying safe from scammers, followed by online platform providers and government

Responsibility for keeping people safe from scammers ranking:

- 42% My own responsibility
- 16% The online platform used by the scammer
- 14% The government
- 8% The website provider / hosting company used by the scammer
- 7% My telecom or mobile operator
- 6% The police
- 3% My bank/payment method or cryptocurrency exchanger
- 1% Charities or consumer support associations
- 1% Insurance companies

Most responsible

Least responsible



Q21. Who do you think should be most responsible for keeping people safe from scammers? Base: All respondents (1,160)

Online platforms and website providers fail to meet expectations relative to the responsibility assigned to them.

Responsibility for keeping people safe from scammers ranking:

- The online platform used by the scammer
- The government
- The website provider / hosting company used by the scammer
- My telecom or mobile operator
- The police
- My bank/payment method or cryptocurrency exchanger
- Charities or consumer support associations
- Insurance companies

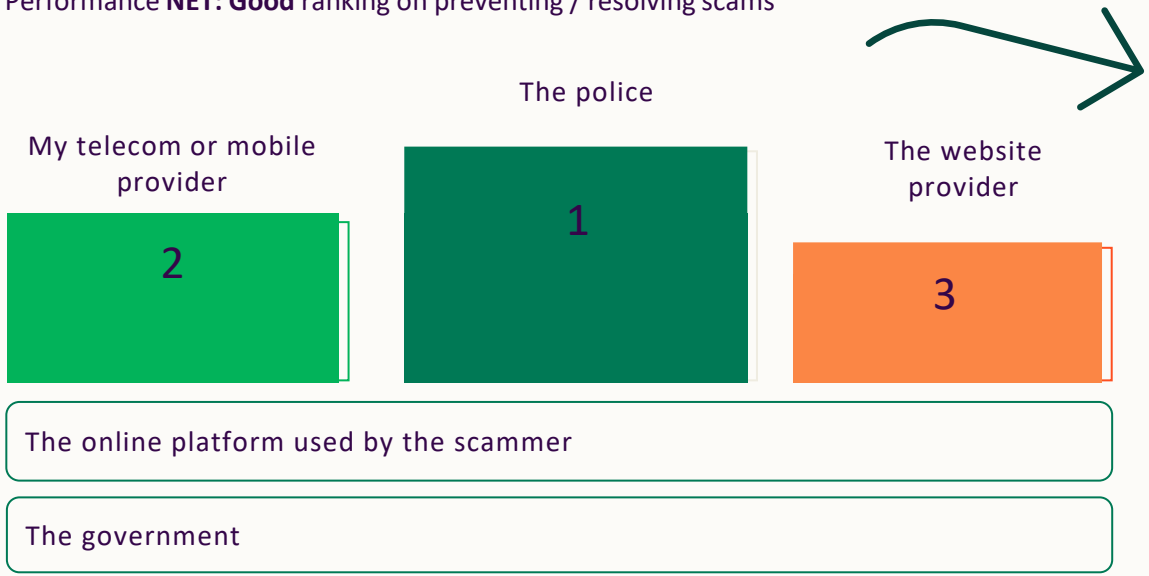
Performance NET: Good ranking on preventing / resolving scams:

- Insurance companies*
- The police
- Charities or consumer support associations*
- My bank/payment method or cryptocurrency exchanger*
- My telecom or mobile operator
- The website provider / hosting company used by the scammer
- The online platform used by the scammer
- The government

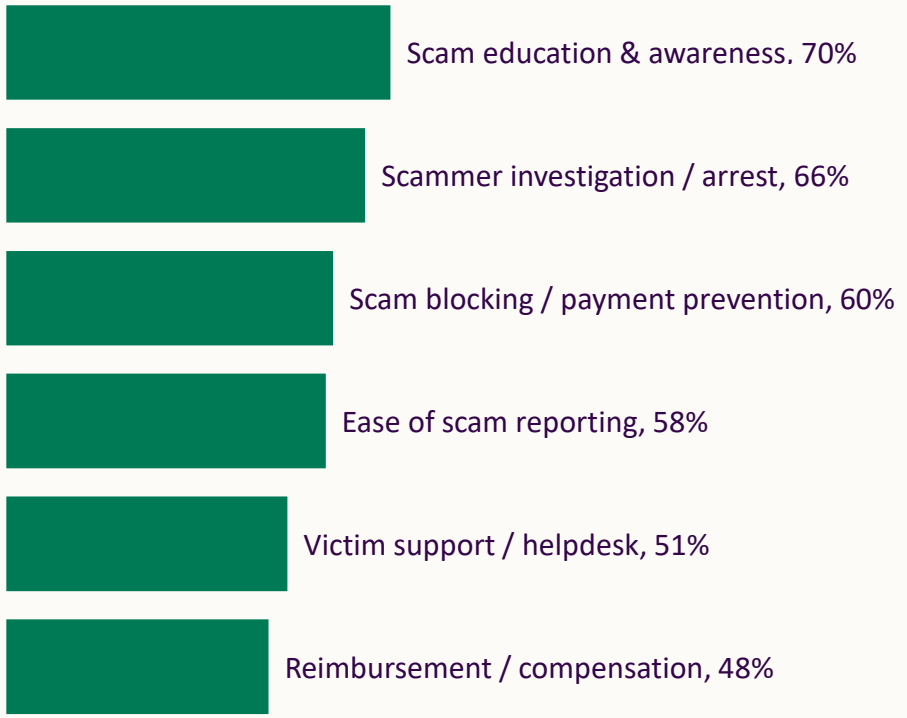
Q21. Who do you think should be most responsible for keeping people safe from scammers? Base: All respondents (1,160) | Q22. You said should be most responsible for keeping people safe from scammers. How do you rate on the following aspects: Base: All respondents that think .. is responsible for keeping people safe from scammers (government n=165 | police n=72 | charities n=17* | online platform 182| website provider n=91 | bank n=32* | telecom operator 80 | Insurance companies 7*) |*low base size

The police is considered strongest in preventing and resolving scams effectively

Performance **NET: Good** ranking on preventing / resolving scams



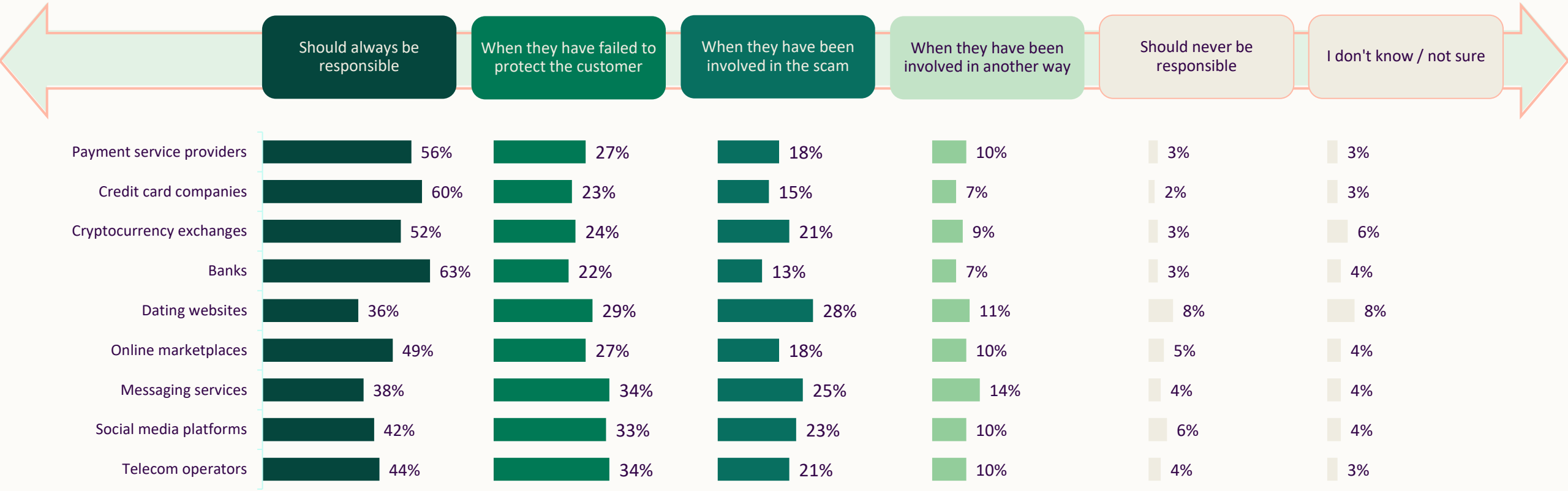
The Police-NET: Good:



Q22. You said .. should be most responsible for keeping people safe from scammers. How do you rate on the following aspects: NET: All aspects Base: All respondents that think .. is responsible for keeping people safe from scammers (government n=165 | police n=72 | charities n=17* | online platform 182| website provider n=91 | bank n=32* | telecom operator 80 | Insurance companies 7*) |*low base size | due to low base size Insurance companies, charities and banks are not included

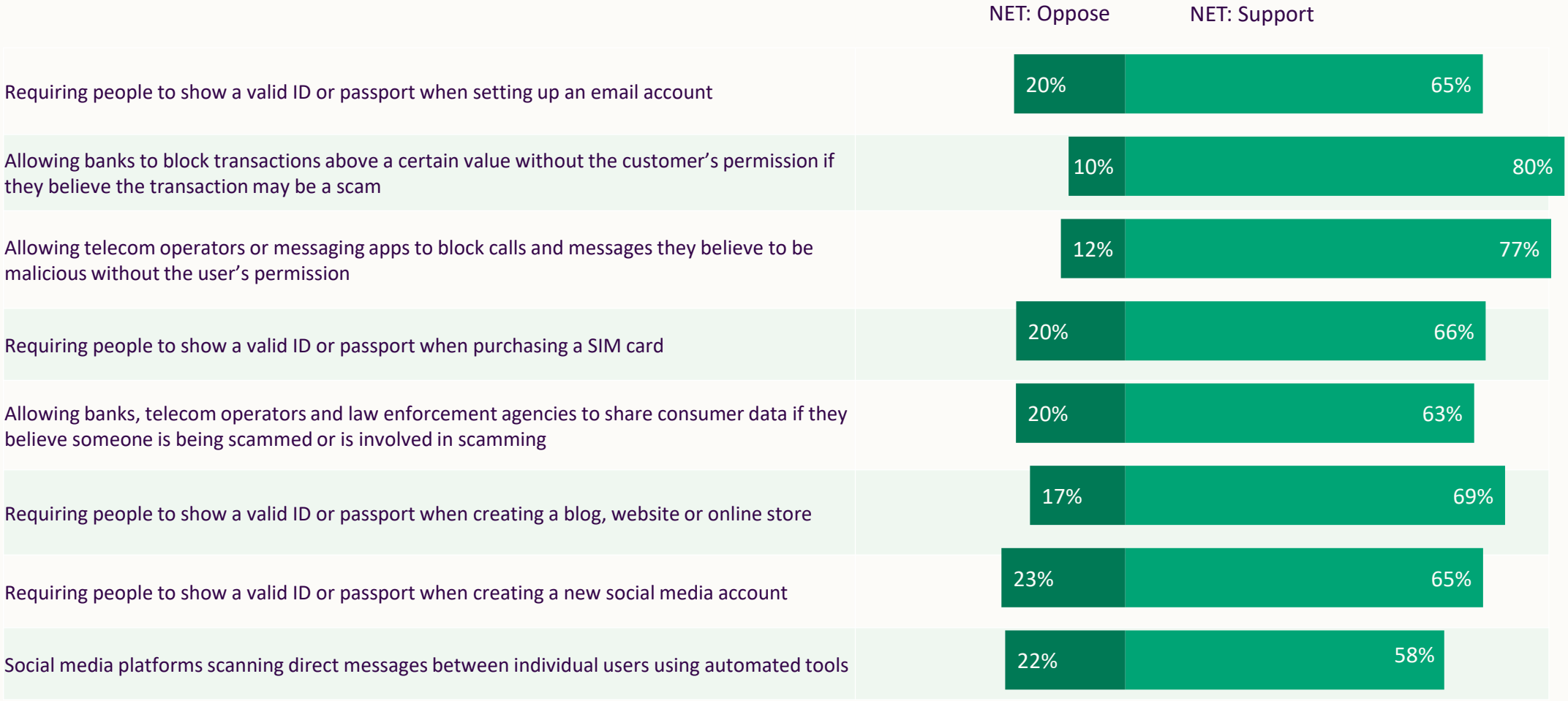
Over half of Filipino/a adults believe banks, credit card companies, payment services and crypto exchanges should always be responsible for reimbursing those experiencing a scam

Level of expected responsibility for reimbursing scams



Q23. If someone is scammed via any of the following platforms / organizations, in what circumstances do you think the platform / organizations should be responsible for reimbursing them? Base: All respondents (1,160)

Over three in four Filipino/a adults support banks and telecom operators in blocking transactions or calls as a scam protection measure



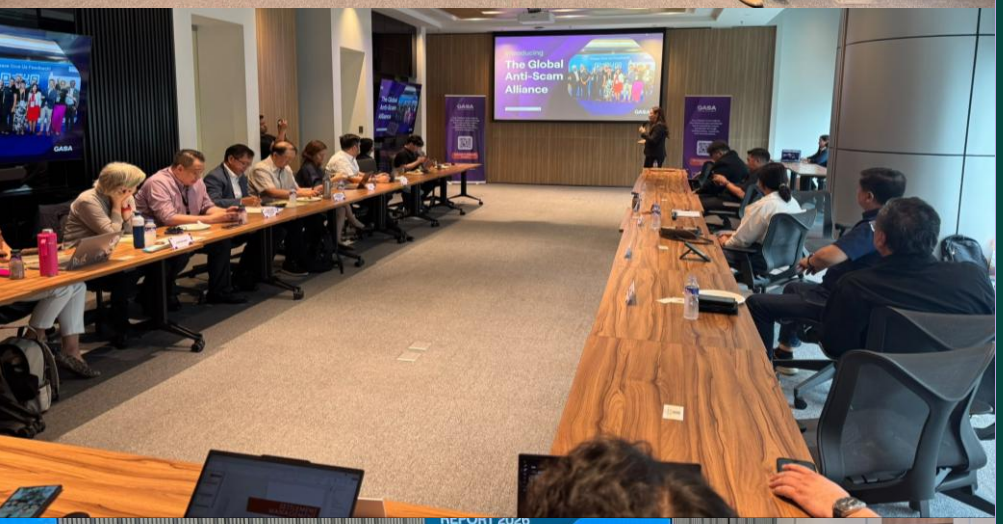
Q26. To what extent do you support or oppose the following measures designed to protect consumers from scams? Base: All respondents (1,160)



Recommendations from Philippines Anti-Scam Roundtables

On 24–25 August 2026, GASA organized two roundtables in the Philippines to discuss interim findings from the State of Scams Philippines 2026 and gather input on recommendations for the report. The sessions brought together anti-scam professionals from around 20 organizations across government, the private sector, civil society, associations, and multilateral organizations. The recommendations encapsulated in this section reflect the key proposals made by participants







Overview

- Scam fighting in the Philippines are an important inflection point. Strong attributes for national scam fighting are in place:
  - Education: Internationally recognized grassroots based Anti-Scam education efforts, e.g. SCAM Watch Pilipinas which won GASA's Scam Fighter Awards 2025 for education
  - Shared Intelligence: Elements of good shared intelligence exists. For example led by BSP-PNPI national mule intelligence and 'Check with SEC'. Next phase is to scale this across sectors
- Silos across key institutionns are an inhibition against faster and coordinated efforts:
  - Victims need to make separate calls to Police hotline and BSP if they wish to take action against scammers and recover funds.
  - Case details of victims are not shared leading to loss of time and frustration on the part of victims
- Higher expectation of institutions and higher willingness for friction:
  - Our survey found that people in the Philippine look to their government to protect them more
  - There was a bigger willingness to accept more friction in banking and telco experiences if it improves protection against scams
- Large migrant worker population a key segment that needs to be protected:
  - Scam compounds lure unsuspecting migrant workers via job scams
  - More can be done to increase awareness and checks to protect outgoing migrant workers against being targeted

Solving scams is a shared effort, and every player has a part that only they can do.

WHAT THE ECOSYSTEM NEEDS

Government & Policymakers

Concern: Economic harm and public trust

Role: Set national strategy and priorities

Regulators & Supervisory Authorities

Concern: Consumer protection and systemic risk

Role: Define standards, rules and accountability

Law Enforcement

Concern: Investigating and prosecuting criminals

Role: Disrupt criminal networks and enforce the law

FIs & Payment Networks

Concern: Financial losses and customer trust

Role: Connect risk signals to detect, respond and prevent scams.

Telcos & Digital Infrastructure

Concern: Abuse of communication channels

Role: Block scam communications and identities

Technologies, Internet and Platforms

Concern: Fraud originating on their platforms

Role: Detect and remove scam content and accounts

Consumer Protection & Civil Society

Concern: Victim support and awareness

Role: Educate consumers and support reporting

International Partners & Intelligence Networks

Concern: Cross-border scam activity

Role: Share intelligence and coordinate action

Each player is strong on its own, but scams exploit the gaps between them. The answer is a connected ecosystem.

Protecting consumers requires three capabilities working together: prevention, intelligence sharing and recovery

WHAT THE ECOSYSTEM NEEDS

A common set of rules, standards and processes so participants can work together consistently and effectively

Shared view of fraud and scam activity across the ecosystem

Fraud & Scam Prevention

Stopping scams earlier through shared intelligence, verification and intervention

Central Fraud & Scam Record

Recovery & Refund

Consistent claims handling, dispute resolution and recovery outcomes when prevention fails

Network-level Intelligence

Transform ecosystem-wide data into insights that help identify emerging threats, trends and vulnerabilities

None of the three works alone: prevention without shared intelligence misses the pattern; intelligence without recovery leaves the victim stranded.

Four areas where public bodies can be hugely effective

ASKS OF PUBLIC BODIES

Scam cost does not land in one place. It shows up in consumer losses, in casework split across several agencies, and in how far people still trust instant payments. Public bodies are essential to implementing ecosystem alignment and collaboration.

01

Nobody shares unless they are made to

Each player sees a small part of the overall scam: the bank sees a payment, the telco sees a spoofed call, the platform sees the advert. Public bodies should establish the legal basis and safeguards for sharing. Industry partners can connect signals and operate shared capabilities.

02

The powers must move as fast as the money

Referrals passed to one agency at a time cannot keep up with money that moves in real time. Funds leave the jurisdiction before anyone can act, and the evidence trail goes with them. Freezing a payment, compelling disclosure and reaching a counterparty need minutes, not days.

03

The floor must be one smaller firms can reach

Large banks can afford strong controls. Smaller banks, e-money issuers and rural providers cannot, and criminals move to wherever protection is thinnest. Obligations should be priced so that everyone ends up protected at the level of the smallest participant as a minimum.

04

Someone has to own it, and pay for it

Successful markets have made progress where the state decided where shared capabilities would sit. The state takes ownership of how that capability is run, pays for the core, and then rolls it out to the industry.

THE BOTTOM LINE

AFASA already gives the Philippines the legal basis. What turns it into a working response is agencies and providers held to the same standards, going after the same people.

Source: Mastercard analysis, drawing on the Philippine roundtables and official sources from Singapore, Malaysia, Australia and the United Kingdom, August 2026

Institutions already pay for scams. Some of that cost is avoidable

ASKS FOR PARTICIPANTS

Participants would see more value in competing over customer experience rather than scam management.

01

Shared signals provide a full picture

Each player sees a small part of the scam: sending bank sees an odd payment, wallet sees a new beneficiary, telco sees a spoofed call, platform saw the advert. No one institution can put that journey together, so every decision is taken on a partial view. A shared signal can change the decision while it is still being made.

02

Alignment can speed up reactions

Separate hotlines, emails and institution-by-institution enquiries are running against instant settlement. The money has usually gone before the counterparty is even identified, and support teams carry the aftermath. What closes that gap is common formats, named contacts and an agreed playbook.

03

Common standards reduce duplicated effort

One taxonomy, sector-wide mule intelligence, standard case handling, tracing past the first receiving account, agreed response times and shared measurement create efficiencies across the entire market. Any institution can buy more controls; none can buy network visibility.

04

What you give, and what you get back

Singapore takes seconded staff and case data and returns a freeze in minutes. Malaysia asks for direct filing and traces across the system in about 30 minutes. Australia wants automated feeds, with duties biting from March 2027. The UK splits reimbursement cost, so the receiving bank has money at stake.

THE COMMERCIAL CASE

Keep competing on the controls your customers see. Anything that depends on seeing past your own customers is cheaper and works better when the market builds it once. This calls for public-private collaboration.

Source: Mastercard analysis, drawing on the Philippine private sector roundtable and official sources from Singapore, Malaysia, Australia and the United Kingdom, August 2026

The routes exist, but a victim still has to know them. Five questions, in the order they are asked

THE CONSUMER VIEW / WHAT DO I DO NOW?

MINUTE ZERO

1. Who do I call first?

In the Philippines: Call the payment service provider the funds were taken from. That is the only place the money can still be stopped.

The gap: A number helps only if victims know it first. Malaysia has one national line; Australia has five.

THE FIRST HOUR

2. Who can recover my money?

In the Philippines: The Coordinated Verification Process under BSP Circular 1215, with industry protocols, is built to trace and return the funds.

The gap: Recovery depends on providers cooperating, without a deadline the victim can enforce.

THE DAYS AFTER

3. Where do I escalate?

In the Philippines: The BSP is the next step if a provider does not help. The police are the final escalation if funds are not recovered.

The gap: An escalation route works only if victims are told it exists and each step is timed.

DAY ONE ONWARDS

4. Who do I report it to?

In the Philippines: Hotline 1326 and the eGovPH e-report channel take the report of the crime, a separate route from recovering the money.

The gap: Victims need to report, whether the money came back or not. Most who stay silent simply do not know where to go.

BEFORE THE NEXT TIME

5. How do I protect myself next time?

In the Philippines: Guidance exists in several places: agencies, providers and campaigns each publish their own advice to the public.

The gap: Nobody is measuring whether any of it changes behaviour. Effectiveness, not volume of material, is the open question.

THE SAME CLOCK, EVERYWHERE

Is it the same everywhere else?

The UK put a deadline and a duty behind recovery; reimbursement rose to 65%. Singapore acts in minutes yet recovers only 15% of losses.

What good looks like: a number known in advance, recovery with a deadline, a timed escalation, reporting that always works, prevention that is tested.

Catching the bad actors matters, but the measure of the framework is whether someone who has just been scammed knows what to do in the first hour without having to work it out.

Sources: BSP Circular No. 1215 and associated industry protocols on coordinated verification; CICC hotline 1326 and eGovPH e-report, Philippine Star, 2026; GASA Southeast Asia scam study, 2025; GASA State of Scams Report 2026 - Malaysia; JCP Law LLC, Singapore Scam Statistics 2025; Frontier Economics, APP Scams Evaluation Final Technical Report, June 2026; ACCC, National Anti-Scam Centre reporting, 2025. Philippine positions reflect participant input at the GASA Manila roundtables, August 2026

Recommendations

GASA organized 2 roundtables on 24 & 25 Aug which were attended by around 20 organizations comprising government agencies, FIs, Telcos, platforms and associations. The following 12 recommendations were made by participants of the roundtables after considering this year's State of Scam Report and current scam fighting efforts in the Philippines:

1 Establish the National Anti-Scam Hub (NASH) as the Central Coordinating Authority

Scam response today remains dispersed across multiple agencies and reporting channels, creating confusion for victims and operational inefficiencies for investigators. NASH should serve as the national coordinating body that receives scam reports, triages cases, assigns actions to relevant agencies, and monitors outcomes. This will provide a single front door for victims while enabling coordinated action across government, financial institutions, telecommunications providers, platforms, and law enforcement.

Additionally, a clear governance and safeguards framework is required to define stakeholder roles, permitted data-sharing purposes, minimum necessary data, access and retention controls, audit requirements, and the treatment of suspicious but unconfirmed indicators. These safeguards should support timely action while protecting privacy and due process and preserving the statutory mandates and independence of participating agencies.

Further, NASH should establish a national scam measurement and reporting framework with common definitions and metrics across participating organizations. Regular publication of aggregated insights would support accountability, inform policy, and strengthen public trust.

2 Implement a Unified National Reporting and Case Management System

One victim report should generate one national case reference shared across all relevant stakeholders. Victims should not be required to repeatedly report the same incident to different organizations. NASH should operate a common case management platform that allows authorized stakeholders to securely access case information, track actions, update investigation status, and coordinate interventions. A shared operational view would significantly improve efficiency, reduce victim fatigue, and accelerate response times.

3 Expand Shared Intelligence Across the Ecosystem

Build upon existing intelligence sharing systems (including BSP mule intelligence and SEC's 'Check with SEC') initiatives to create a broader national intelligence-sharing capability. The Philippines already has strong foundations for information sharing within the financial sector, particularly around mule account detection, suspicious transaction monitoring and organization verification. These are strong building blocks and these capabilities should be expanded to incorporate intelligence from telecommunications providers, technology platforms, e-commerce providers, e-wallet operators, regulators, and law enforcement agencies. A shared intelligence framework would improve the identification of criminal networks, mule accounts, compromised identities, and emerging scam tactics. The "intelligence" or "information" referred will come from different sources.

4 Strengthen Real-Time Intervention and Fund Recovery Capabilities

Reduce the time between scam reporting and intervention. Scammers can move stolen funds within minutes, particularly through e-wallets, digital accounts, and cross-border payment channels. Financial institutions, e-wallet providers, and authorities should strengthen mechanisms for real-time alerts, rapid account freezing, transaction tracing, and coordinated intervention. Success in scam response increasingly depends on speed rather than traditional investigative timelines.

5 Enhance Financial Tracing and Criminal Network Disruption

Follow the money to identify and dismantle organized scam syndicates. Anti-scam efforts should move beyond individual victim cases toward identifying the broader criminal infrastructure that enables scams. Enhanced financial tracing capabilities, network analytics, and cross institutional intelligence sharing can help uncover mule account networks, beneficial owners, facilitators, and organized crime groups. Greater focus should be placed on disrupting criminal ecosystems rather than solely recovering individual losses.

6 Deepen Public-Private Operational Collaboration

Move from information sharing to coordinated operational action. Effective scam prevention requires government agencies, financial institutions, telecommunications companies, technology platforms, e-commerce providers, and cybersecurity organizations to work together throughout the scam lifecycle. Shared operating procedures, escalation protocols, intelligence exchanges, and joint disruption activities should become standard practice across the ecosystem.

7 Strengthen Platform Accountability and Preventive Controls

Stop scams before victims are exposed. Messaging applications, social media platforms, e-commerce marketplaces, and digital service providers should strengthen proactive measures to identify fraudulent accounts, remove malicious content, monitor suspicious seller activity, and disrupt scam campaigns. Stronger verification mechanisms, seller onboarding controls, and faster response times can significantly reduce victim exposure.

8 Scale Preventive Detection Through Shared Infrastructure, Threat Intelligence and AI

Make advanced scam prevention accessible across the entire financial sector. Not all financial institutions possess the resources to operate large fraud teams or deploy sophisticated detection technologies. The Philippines should explore shared industry infrastructure and consortium based capabilities that provide smaller institutions with access to advanced scam detection tools. AI powered analytics can further improve detection of mule activity, synthetic identities, impersonation attempts, social engineering attacks, and emerging scam patterns. AI-powered analytics can improve the detection of mule activity, synthetic identities, impersonation attempts, social engineering attacks, and emerging scam patterns. Beyond transaction monitoring, the ecosystem should leverage shared intelligence to identify and disrupt scam infrastructure, including malicious domains, fraudulent accounts, and other threat indicators, before victims are exposed or losses occur.

9 Improve Consumer Verification and Scam Prevention Tools

Empower consumers to verify before they trust. Preventive tools such as the SEC's "Check with SEC" initiative demonstrate the value of enabling consumers to verify the legitimacy of businesses before transacting. Similar verification capabilities should be expanded across sectors to help consumers identify fraudulent entities, suspicious websites, fake investment schemes, and impersonation attempts before financial losses occur.

10 Create a National Scam Awareness and Education Framework

Deliver consistent, coordinated, and continuous public education. Scam awareness campaigns should be centrally coordinated through NASH to ensure consistent messaging across agencies and industry partners. Standardized educational toolkits, public advisories, reporting guidance, and awareness campaigns can improve public understanding of scam risks, reporting pathways, and protective behaviors. Particular focus should be placed on emerging scam typologies and high-risk demographics.

11 Invest in Specialist Training and Local Response Capabilities

Build anti-scam expertise at both national and local levels. The effectiveness of NASH will depend on the skills of the analysts, investigators, intelligence specialists, and operational staff supporting it. Specialized training should be developed for personnel across BSP, CICC, PNP ACG, NBI, SEC, and financial institutions. Local Government Units (LGUs) should also be equipped to act as frontline anti-scam champions, providing initial victim assistance, conducting preliminary assessments, and escalating cases through standardized processes.

12 Strengthen Cross-Border Cooperation and Protection for Overseas Filipino Workers (OFWs)

Recognize scams as a transnational crime requiring international coordination. Many scam operations and money flows originate outside the Philippines, while OFWs remain a frequent target of scams, recruitment fraud, and other forms of exploitation. NASH should establish formal mechanisms for international information sharing, cross-border investigations, asset recovery efforts, and coordination with Philippine diplomatic and labor offices overseas.

Dedicated protocols should be developed for OFW and migrant-worker cases, including overseas-accessible reporting channels, clear routing between scam, trafficking, and labor-protection pathways, and coordinated procedures for victim assistance, protection, and repatriation where required. A victim-centered approach should be adopted to ensure that individuals presenting with indicators of coercion, trafficking, or exploitation are appropriately safeguarded.

13 Strengthen Victim Support and Recovery Mechanisms

Scam victims often experience financial, emotional, and psychological harm that extends beyond the initial incident. Anti-scam efforts should therefore go beyond investigation and fund recovery to provide a more holistic, victim-centred response. Victims should have access to appropriate financial, legal, psychosocial, and mental-health support services, with additional assistance available for vulnerable individuals. Victim experience and recovery outcomes should be recognized as important measures of success alongside investigations, disruptions, and funds recovered.



ABOUT THIS REPORT

Who are we?

The Global Anti-Scam Alliance (GASA) is a non-profit, bringing together policy makers, law enforcement, consumer authorities, NGOs, the financial sector, cybersecurity, platforms and other commercial organizations to share insights and knowledge surrounding scams.

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

Contact: partner@gasa.org

Gogolook is a leading TrustTech company established in 2012. With "Build for Trust" as its core value, expanding its business from Asia to Europe and America.
A foundation member of the Global Anti-Scam Alliance (GASA), Gogolook has also teamed up with a number of institutes such as the Taiwan National Police Agency, Thai Royal Police, the Philippines Cybercrime Investigation and Coordinating Center, the Fukuoka city and Shibuya city government, and the Royal Malaysia Police to fight scams, dedicated to creating a "scam-free environment."
https://www.gogolook.com/

Mastercard powers economies and empowers people in 200+ countries and territories worldwide. Together with our customers, we're building a resilient economy where everyone can prosper. We support a wide range of digital payments choices, making transactions secure, simple, smart and accessible. Our technology and innovation, partnerships and networks combine to deliver a unique set of products and services that help people, businesses and governments realize their greatest potential.
http://www.mastercard.com/

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

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

Contact europe@opinium.com for inquiries.

About the authors



Jorij Abraham
MANAGING DIRECTOR
GASA
Global Anti-Scam Alliance

Jorij Abraham has been active in the Digital World since 1997. From 2013 to 2017, he was the Research Director of Thuiswinkel.org, Ecommerce Europe (the Dutch & European Ecommerce Association) and the Ecommerce Foundation.

In 2017 he took over ScamAdviser.com and grew it into a place where people can check if something is a scam with more than 7 million users per month.

In 2022 Jorij founded the Global Anti-Scam Alliance (GASA) of which he is the Managing Director.



Brian D. Hanley
CHAPTER DIRECTOR ASIA-PACIFIC
GASA
Global Anti-Scam Alliance

Brian D. Hanley has more than 25 years of experience living and working across Asia and the Pacific (APAC). He currently leads the Global Anti-Scam Alliance (GASA) efforts in APAC, bringing together government, law enforcement, industry leaders and civil society to combat online scams and protect consumers.

Previously he led regional programs in support of independent media and information integrity at Internews and served as a Senior Democracy and Governance Field Advisor with USAID.

He has also held roles in the U.S. Senate and began his international service as a U.S. Peace Corps Volunteer. Brian holds a master's degree in international affairs from Columbia University's School of International and Public Affairs (SIPA).



Molly Maclean
ASSOCIATE DIRECTOR
07 Op Opinium

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

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

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

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, Charm, Confiant, 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, Ministry of Interior, Nasdaq Verafin, netcraft, OpenAI, Scamadviser, The Media Trust, Trend Micro, Visa, Scotiabank

Our Corporate Members

AnyDesk, Arab Bank, Arkose Labs, Banca Transilvania, BioCatch, CaixaBank, cellcard, Chainalysis, Crystal, DANA, EBRAND, FICO, Memcyco, Navy Federal Credit Union, Cyberdefense, Rabobank, React, Remitly, Santander, sea, standard chartered, TeamViewer, tietoevry, true, VoiSek, Vonage Part of Ericsson, Worldline, yubo



APPENDIX

Value lost to scams methodology Q3 (scam encounters)

The next questions are around ‘scam encounters’. A scam encounter includes any situation where you are approached by someone attempting to deceive you for financial gain, regardless of the channel they use to contact you.

Examples of ‘scam encounters’ could include anything from phishing emails (fake emails trying to get your personal details), a fake text message or phone call (someone pretending to be from a trusted company), to a malicious advert (an online ad that leads to an unsafe website).

Q2ASK ALL
SINGLE SELECT RESPONSE
How often, if ever, do you encounter scam attempts?

1. More than three times a day
2. Two to three times a day
3. Once a day
4. Two to three times a week
5. Once a week
6. Once every two weeks
7. Once a month
8. Once every two months
9. Once every three months
10. Once every six months
11. Once every nine months
12. Once every twelve months
13. Less than once every twelve months
14. Never
15. I don't know/not sure

Value lost to scams methodology Q6 (scam interactions)

Q6 ASK ALL WHO HAVE ENCOUNTERED A SCAM IN THE LAST YEAR (Q2=1:12)
SINGLE GRID

Scams are becoming increasingly sophisticated, meaning anyone could be affected. Between 2024 and 2025 there was an estimated 202.3 billion scam interactions.

We'd like to understand how, if at all, you interacted with scams you encountered in the last 12 months. Interacting with a scam can range from simply opening or reading a message to replying, picking up a call, clicking links, visiting fake websites, or engaging in back-and-forth communication.

You said you experienced scam encounters in the last 12 months. To what extent, if at all, did you interact with the following types of scams?

Answer based on your interactions with the scammer before you realized it was a scam or tried to verify whether it was legitimate. 7

ROWS - RANDOMISE

1. Investment scam: A scammer approaches you with a supposedly lucrative investment opportunity, often promising guaranteed returns or no risk, and asks you for money or financial details to "secure" the investment.
2. Shopping scam: A scammer advertises products or subscription services, often through onlinemarketplaces, websites, ads, or social media, and asks you to pay for goods or services that will never be delivered or are not genuine.
3. Employment scam: A scammer poses as an employer or recruiter offering you a job, work from home role, or business opportunity, and asks you for upfront payments or personal/financial information for things like training, equipment, or application processing.
4. Unexpected money scam: A scammer contacts you claiming that you have won a prize, been awarded a grant, inherited money, or are owed a financial payout, and requests fees or personal/financial information to "release" the funds.
5. Impersonation scam: A scammer pretends to be a government/police official, bank representative, or friend or family member and asks you for payments or personal/financial information to resolve a fabricated issue or verify your identity.
6. Charity scam: A scammer pretends to represent a charity or urgent cause and asks you for donations, often using emotional stories or pressure to encourage quick payment.
7. Romance/relationship scam: A scammer builds a relationship with you by pretending to be a romantic interest or claims to be contacting you on behalf of a loved one, then asks you for money or personal/financial information to help with fake emergencies or personal difficulties.
8. Fake invoice scam: A scammer sends you an invoice, bill, or debt notice that looks legitimate and asks you to pay for goods or services that you never ordered, received, or owed.
9. Blackmail or extortion scam: A scammer threatens you or attempts to coerce you, demanding money or personal/financial information in exchange for not carrying out the threat.
10. 1Identity theft: A scammer gets hold of your personal information or gains access to your accounts, such as banking, email, or social media, and uses it without your permission to make purchases, transfer money, apply for loans, or obtain official documents.
11. Money recovery scams: A scammer claims they can help you recover money you previously lost to a scam and asks for additional payments or personal/financial information, ultimately deceiving you again.
12. Weather refund scam: A fictional scam where you are told you qualify for a government "weather refund" for experiencing rainy and sunny weather in the same week.
13. Any other scams in the last 12 months: Any other situation where you are approached by someone attempting to deceive you for personal financial gain in ways not previously listed. [ANCHOR]

COLUMNS - ROTATE

1. I haven't encountered this type of scam in the last 12 months
2. I've encountered this type of scam, but haven't interacted with it (e.g., you saw, received, or became aware of this scam, but did not interact with it)
3. I have interacted with this type of scam on some occasions, but not all (e.g. you responded, clicked a link, followed instructions, or interacted in any other way)
4. I interacted with this type of scam each time I encountered it (e.g. you responded, clicked a link, followed instructions, or interacted in any other way)
5. I don't know/not sure [ANCHOR]

Value lost to scams methodology Q7A (financial loss)

Q7A ASK THOSE WHO HAVE INTERACTED WITH SCAM IN LAST YEAR (SELECTED Q6:3 OR 4)
MULTI SELECT RESPONSE [GU15.1]

Each year, scams are becoming increasingly sophisticated meaning anyone could become a victim. Between 2024 and 2025 it is estimated that 880.1 million people gave money to scammers.
You said you interacted with scam encounters in the last 12 months. During any of these interactions, did you end up giving the scammer your money or personal information?

Answer based on whether you gave the scammer your money or personal information, regardless of whether any of it was recovered or reimbursed.

Select all that apply.

We appreciate your open and honest answers.

Yes, I gave the scammer money (e.g., you sent, paid, or transferred money to the scammer)

1. Yes, I gave the scammer personal information, and it was later used to steal my money (e.g., your information was misused to transfer funds, make purchases, open accounts, or otherwise take money from you)
2. Yes, I gave the scammer personal information, but it was not used to steal my money
3. No, I did not give the scammer any of my money or personal information when interacting with scams [EXCLUSIVE]
4. I don’t know/not sure [ANCHOR, EXCLUSIVE]
5. Prefer not to say [ANCHOR, EXCLUSIVE]

Value lost to scams methodology Q12A to Q12D (financial losses)

Q12A ASK THOSE WHO LOST MONEY TO SCAMMERS (Q7A=1;2)
SINGLE ALTERNATE
You said you have been scammed and lost money in the last 12 months. How much money was stolen from you by scammers during this period, in total?

Answer based on the amount stolen, regardless of whether any of it was recovered or reimbursed.

Do not include any additional money you may have earned through the scam. Think only about the amount directly provided to the scammer from your personal bank account or accessible cash holdings.

If you have been scammed and had money stolen more than once in the last year, answer based on the total amount stolen.

1. From 0 to [roughly equal increment to build up to 50th percentile]
2. [roughly equal increments to build up to 50th percentile]
3. [roughly equal increments to build up to 50th percentile]
4. [roughly equal increments to build up to 50th percentile]
5. [roughly 50th PERCENTILE OF 2025 VALUE LOST]
6. [roughly equal increments to build up to 90th percentile]
7. [roughly equal increments to build up to 90th percentile]
8. [roughly equal increments to build up to 90th percentile]
9. More than [90TH PERCENTILE OF 2025 VALUE LOST]
10. I don't know/not sure
11. Prefer not to say

CLICK HERE TO VIEW ACTUAL VALUES DISPLAYED IN BANDS (ANSWER OPTION 1 TILL 9)

Q12B ASK ALL WHO SELECTED Q12A=5:9 AT Q12A
SINGLE
You said that between [INSERT RANGE ENTERED @ Q12A] was stolen from you by scammers in the last twelve months. Is this the correct amount?

1. Yes, this is how much was stolen from me by scammers in the last 12 months [CONTINUE TO Q12C]
2. No, I entered this incorrectly [SENT BACK TO Q12A TO CORRECT RESPONSE]
3. I don't know/not sure
4. Prefer not to say

Q12C ASK THOSE WHO LOST MONEY TO SCAMMERS (Q7A=1;2), AND ABLE TO GIVE VALUE LOST RANGE Q12A=1;4 OR IF HAVING A HIGHER VALUE LOST (Q12A=5:9) ARE ABLE TO CONFIRM THIS IS CORRECT UPON PROMPTED (Q12B=1)

OPEN NUMERIC
You said you have been scammed and lost money in the last twelve months. Exactly, how much money was stolen by the scammer?

Answer based on the amount stolen, regardless of whether any of it was recovered or reimbursed.

If you have been scammed and had money stolen more than once in the last year, answer based on the total amount stolen.

Enter the exact amount to the best of your memory.

[NUMERIC BOX IN LOCAL CURRENCY]

Q12D ASK ALL WHO GAVE A VALUE AT Q12C ABOVE 50TH PERCENTILE (HIGHER VALUE OF ANSWER OPTION 5 AT Q12A)
SINGLE
You said that [INSERT AMOUNT ENTERED @ Q12C] was stolen from you by scammers in the last twelve months. Is this the correct amount?

1. Yes, this is how much was stolen from me by scammers in the last 12 months [CONTINUE TO NEXT QUESTION D12D]
2. No, I entered this incorrectly [SENT BACK TO Q12C TO CORRECT RESPONSE]
3. I don't know/not sure
4. Prefer not to say

During analysis respondent answers were checked for consistency in answering range of value lost (Q12A) and actual numerical value lost (Q12C).
Additional "sense check" of reported value lost against reported income (D8) and removing respondents who were unable to confirm they have entered the right value lost amount at Q12B and Q12D

DISCLAIMER

This report is a publication by the Global Anti-Scam Alliance (GASA) . 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

It is strictly prohibited to use information published in this report without the authors' prior consent. Any violation of such rule will result in a fine of €25,000, as well as in a further penalty of €2,500 for each day that such non-compliance continues. However, authors allows the use of small sections of information published in the report provided that proper citations are used (e.g., source: www.gasa.org)

Global Anti-Scam Alliance (GASA)

Oder 20 - UNIT A6311
2491 DC The Hague
The Netherlands

General and press queries: partner@gasa.org

X (Twitter): @ScamAlliance

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

GASA
Global Anti-Scam Alliance