GASA | netsafe
Global Anti-Scam Alliance

STATE OF SCAMS REPORT 2026



NEW ZEALAND

One in four New Zealand 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 Global Anti-Scam Alliance | netsafe

Summary

Scams remain an everyday reality

Scam exposure remains widespread in New Zealand, with 83% of adults reporting they encountered a scam in the past year. Although exposure levels are stable versus 2025 (82%), scams remain a regular feature of daily life, averaging 88 scam encounters per person annually.

Confidence does not guarantee protection

Nearly three quarters (73%) of adults say they are confident they can recognize scams, yet 44% of those who encountered a scam went on to interact with it. Among those who interacted, 23% ultimately lost money or personal information that resulted in financial loss.

Scam losses top half a billion dollars

New Zealand adults lost an estimated NZD 503.5 million* to scams over the past year, with victims reporting an average loss of NZD 1,623. Financial harm is rarely isolated, with 37% of victims reporting they were scammed more than once.

The damage goes beyond money

The consequences of scams reach well beyond stolen money. Six in ten victims say the experience affected their mental wellbeing, while many report becoming more distrustful of digital platforms, reducing spending, or experiencing a loss of confidence following the incident.

Victims increasingly rely on others to identify scams

Almost half of victims (49%) discovered they had been scammed only after being alerted by a bank, family member, authority, media source, platform, or another external party, up from 37% in 2025. This suggests that self-detection is becoming less common, despite high confidence in scam recognition.

Reporting does not always lead to recovery

While reporting levels are relatively high, outcomes are mixed. Victims are more likely to report scams to commercial organizations than authorities, and only 42% of those who reported losing money say they recovered or were reimbursed for at least some of their losses.

*At a 95% confidence level, estimated losses range from NZD 255.7 million to NZD 751.2 million.

Strengthening Scam Prevention and Support in New Zealand



Brent Carey
CEO

Netsafe

About Netsafe

Netsafe NZ is an independent non-profit organisation supporting people in Aotearoa New Zealand to have safe and positive online experiences. We keep people of all ages safe online by providing free support, advice and education.

Under New Zealand's Harmful Digital Communications Act, Netsafe runs a helpline service 5 days a week to provide expert incident support to people experiencing harm online.

People should be able to look for work, buy something online or respond to a message from their bank without having to become experts in deception. The frequency of scam encounters in Aotearoa New Zealand makes protection a responsibility for every organisation involved in those everyday activities.

At Netsafe, an independent online safety charity, we hear from people trying to understand what has happened and what they can do next. Their experiences show how financial loss can be accompanied by shame, family stress and a lasting loss of confidence. They also reveal where advice is difficult to apply and where routes to help become confusing.

This State of Scams research provides evidence to improve that response. People identify information from banks, payment providers and awareness initiatives as useful in recognising scams. We should build on what people find helpful, while expecting the services they use to provide effective safeguards alongside that advice.

The accounts of convincing messages and apparently genuine situations also deserve attention. People need practical ways to verify what they are being told, especially when familiar names and appearances offer little reassurance. Advice must remain useful in the circumstances people actually face.

What happens after a scam needs the same attention. Someone seeking help should be able to understand where to report, what action may be possible and where further support is available. Confusion about those steps adds to an already difficult experience. A compassionate response should give people useful information and realistic expectations.

Netsafe brings an independent perspective grounded in the harms people report. Our work combines public guidance, research and scam intelligence, including through Re:Scam.org and Netsafe.org.nz/scams. That experience can help banks, telecommunications providers, digital platforms, government and community organisations identify gaps and improve the advice and responses people receive.

The Global Anti-Scam Alliance's research gives us a shared basis for that work. The next step is to turn the findings into practical improvements: stronger prevention, clearer reporting and better routes to appropriate help. People's experiences should inform those decisions, and we should assess whether the changes make a difference.

Making this work reliable and accessible requires sustained investment. Netsafe welcomes partners willing to fund and test improvements in independent guidance, the use of scam intelligence and pathways to support. Success should be judged by whether people can find appropriate help, understand their next steps and participate online with greater confidence.

If we ask people to report scams, we owe them a response they can understand and use.

Our global research surveyed 58,900 respondents across 42 countries

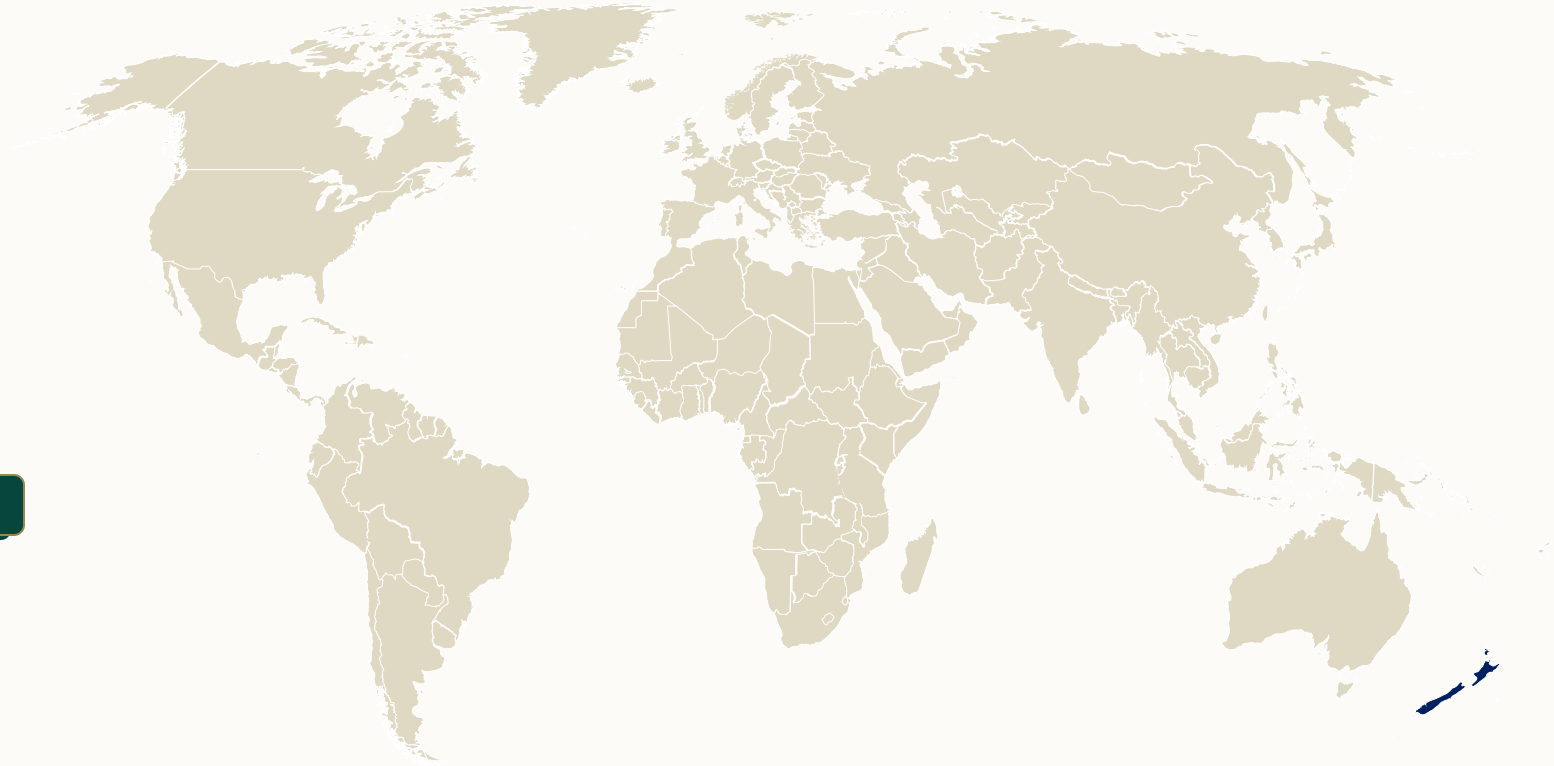
GLOBAL COUNTRIES

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
Spain
Sweden
Switzerland
Taiwan
Thailand
Türkiye
UAE
UK
United States
Vietnam

OCEANIA

Australia
New Zealand

The data in this report will focus on findings within **New Zealand**



GASA Global Anti-Scam Alliance | netsafe

Who we spoke to in New Zealand

Sample size | 1,180 people

Audience | Adults aged 18+ living in New Zealand

Weighting | Nationally representative of the New Zealand adult population on age, gender and region

Methodology | 15-minute online survey

Sample source | Online research panel

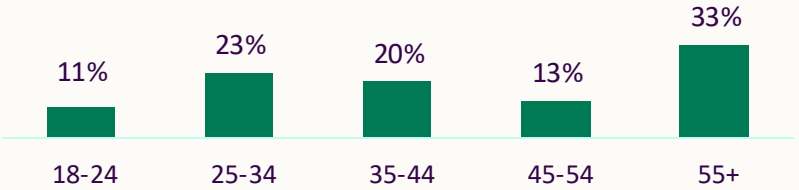
Fieldwork | 16th March – 13th April 2026

Base: All respondents (Base = 1,180)

GENDER



GENERATION / AGE



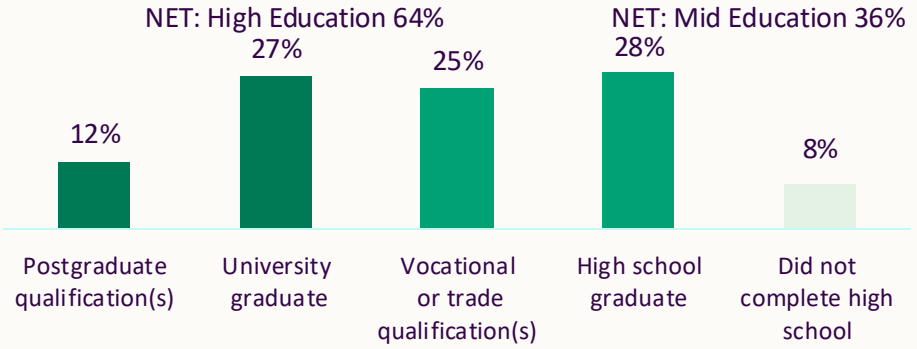
WORKING STATUS



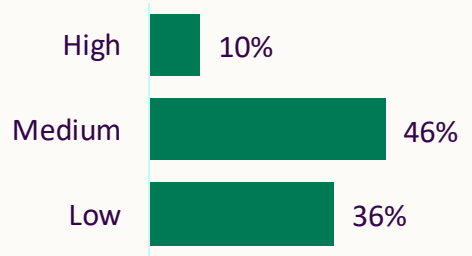
PARENTAL STATUS



EDUCATIONAL STATUS



HOUSEHOLD INCOME



GASA Global Anti-Scam Alliance | netsafe

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 New Zealand, 90 of 1,180 respondents reported losing money to scams, equating to an estimated 310,125.97 affected adults nationally.

Multiplying this by the average loss (NZD 1623.40) produces an estimated total loss of NZD 503,458,493.37

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 1.63 NZD

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

The Scam Funnel in New Zealand

73% are confident they recognize a scam

Total participants (1,180)

83% encountered a scam*

Top reasons for not interacting with scams
54% message or request did not seem legitimate
44% the contact came from an unknown source
42% notice mistakes in spelling or grammar

11% of parents say their child has been scammed too

33% interacted with the scammer
(44% among those that encountered a scam)

Top reasons for not giving money
32% responses were inconsistent or didn't make sense
29% request was suspicious
25% the offer felt too good to be true

8% lost money or data that led to money lost (scammed)
(23% among those that interacted with a scam)

Most common scams interacted with
15% Shopping scam
13% Impersonation scam
12% Investment scam

60% of those scammed say it impacted their mental wellbeing

2% reported the scam to authorities
(24% among those that lost money to a scam)

42% of those who reported their losses say their money was reimbursed by the organization they reported to

37% of those scammed say it happened more than once

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.

GASA | netsafe
Global Anti-Scam Alliance

Throughout this report, comparisons to the Oceania 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



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.

Concerns around being scammed remains stable in New Zealand



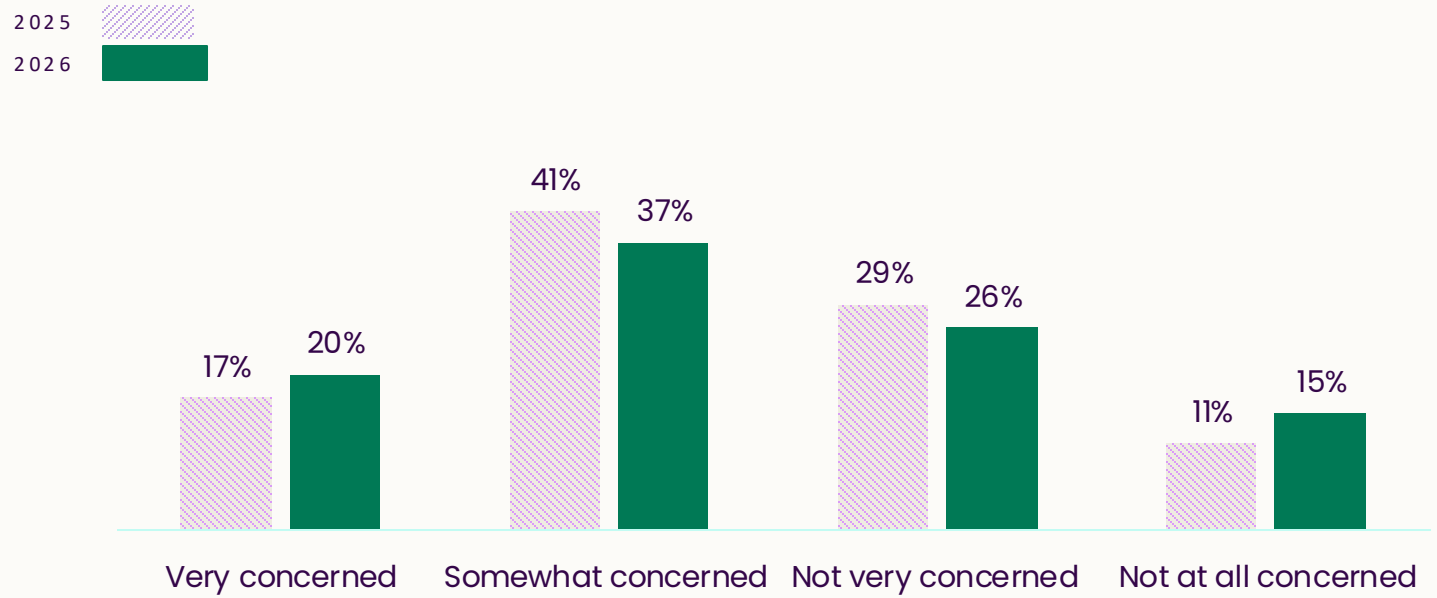
NET: Concerned

are concerned about being scammed in 2025 vs



NET: Concerned

Proportion concerned about being scammed in 2025 vs 2026



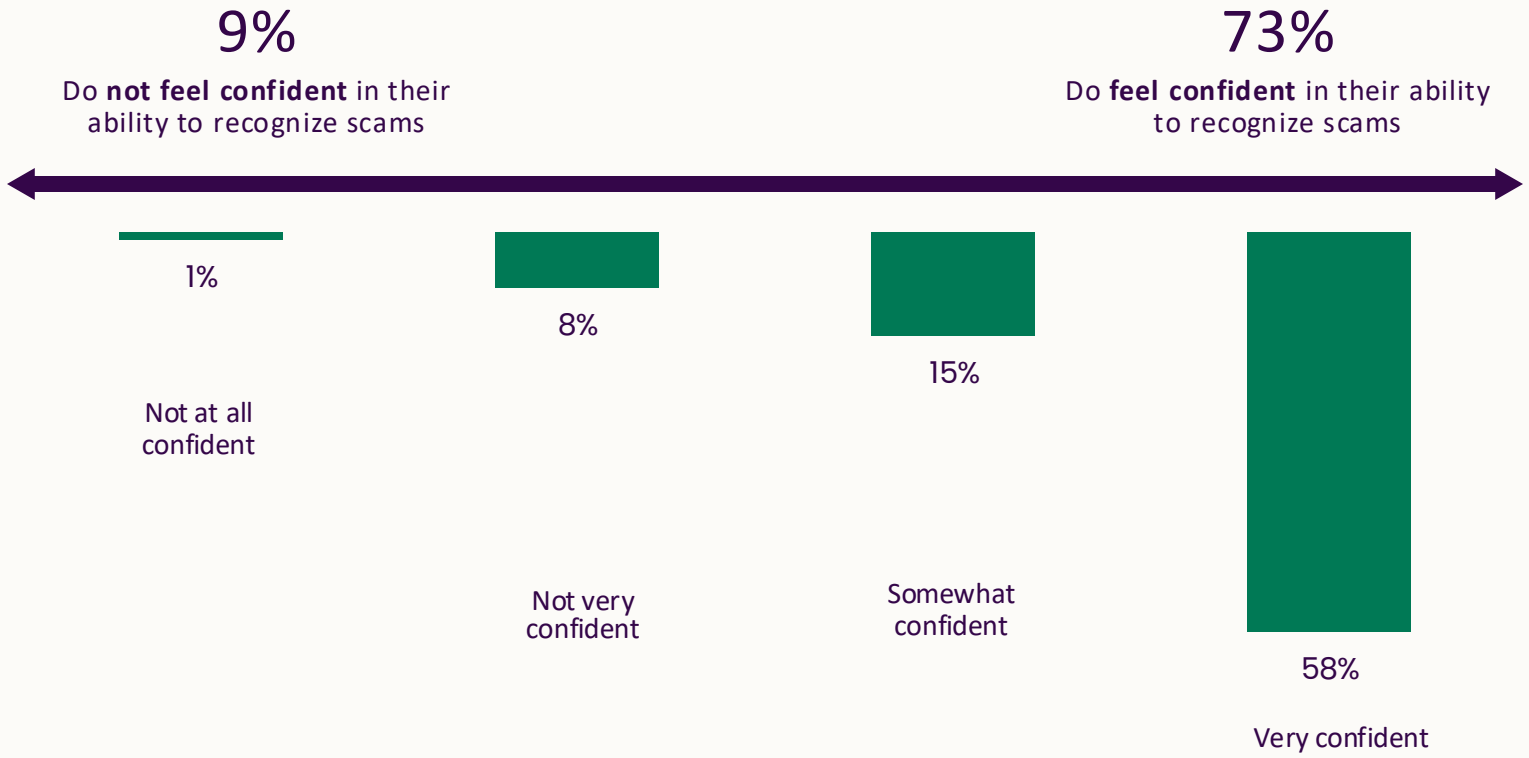
Q1B. How concerned were you about being scammed this time last year, and how concerned are you about being scammed today [=2026] / this time last year [2025]? Base: All respondents (1,180)

GASA Global Anti-Scam Alliance | netsafe

Three in four New Zealand adults are confident in their ability to spot scams

Confidence in recognizing scams

Scam-recognition confidence in New Zealand skews strongly toward **women (76%),** those with a higher education (75%) and parents (75%). By comparison, lack of confidence is much higher among **those aged 45-54 (14%)** or with a low education (16%).



Q1A. How confident are you, if at all, that you can recognize scams? Base: All respondents (1,180)

Four in five New Zealand adults encountered a scam in 2026 remaining stable year-on-year despite a shift towards less frequent exposure

Prevalence & frequency of encountering a scam

83%

Of New Zealand adults encountered a scam in 2026



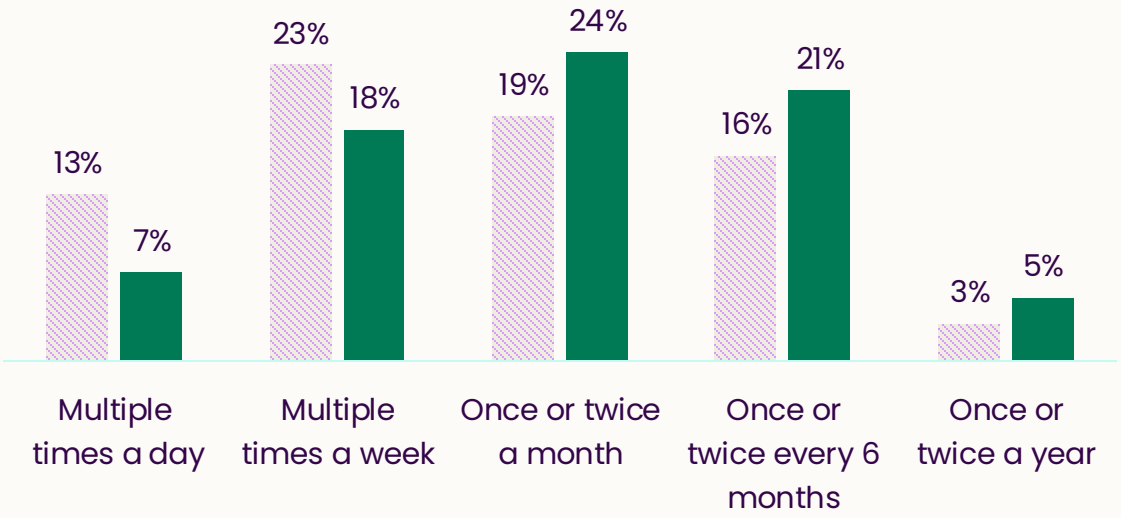
Vs.

82%

Who encountered a scam in 2025



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



Which equates to



scam encounters on average per person, per year, in **New Zealand**

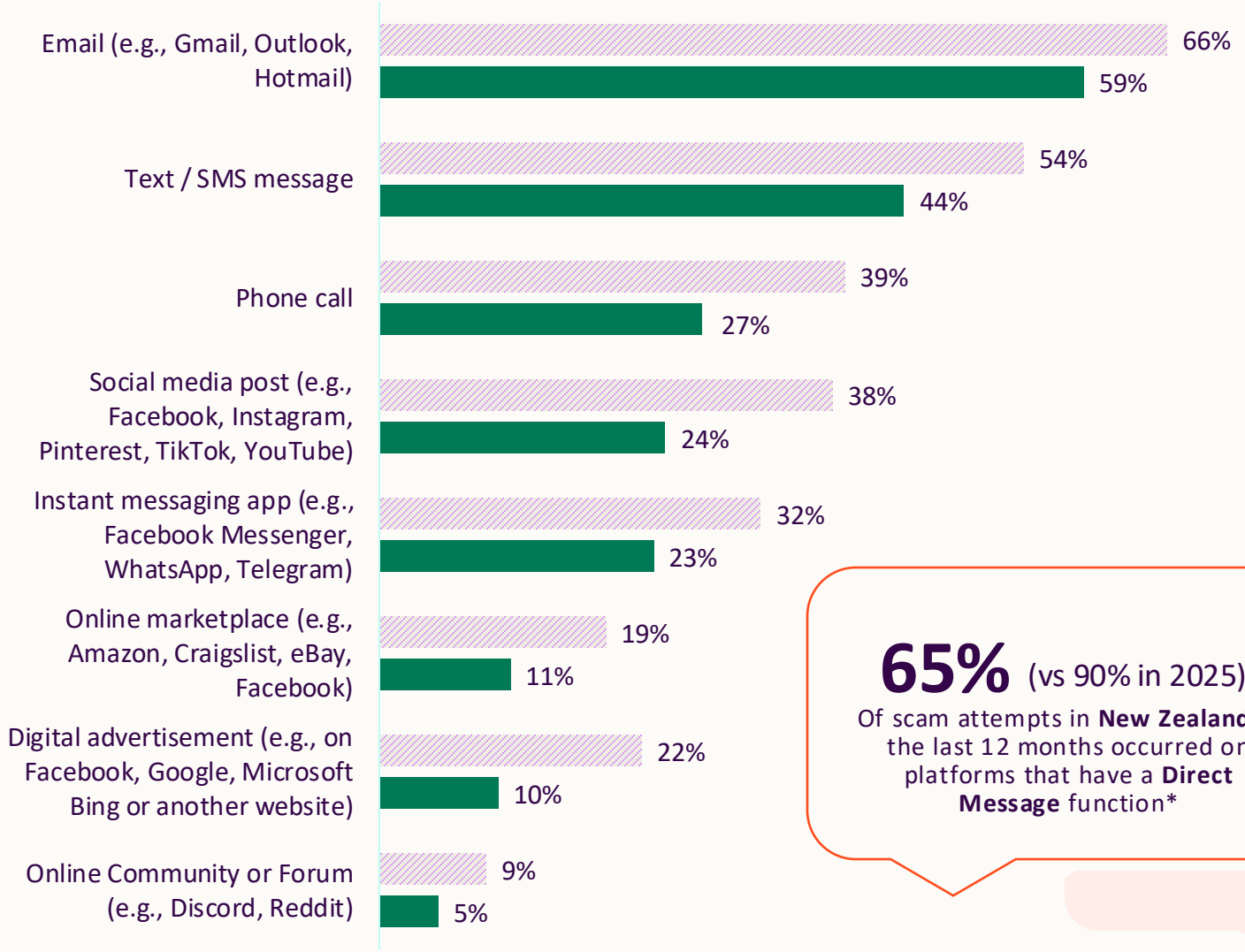


Q2. How often, if ever, do you encounter scam attempts? Base: All respondents (1,180)

Email continues to be the primary route for scam attempts in New Zealand, followed by text messages

Communication platforms where scams were encountered – top 8





65% (vs 90% in 2025)
Of scam attempts in **New Zealand** 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 (884)
*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).

Gmail and Facebook 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 New Zealand

Gmail 38%

facebook 35%

WhatsApp 17%

Instagram 8%

Google 6%

YouTube 6%

Telegram 6%

X 3%

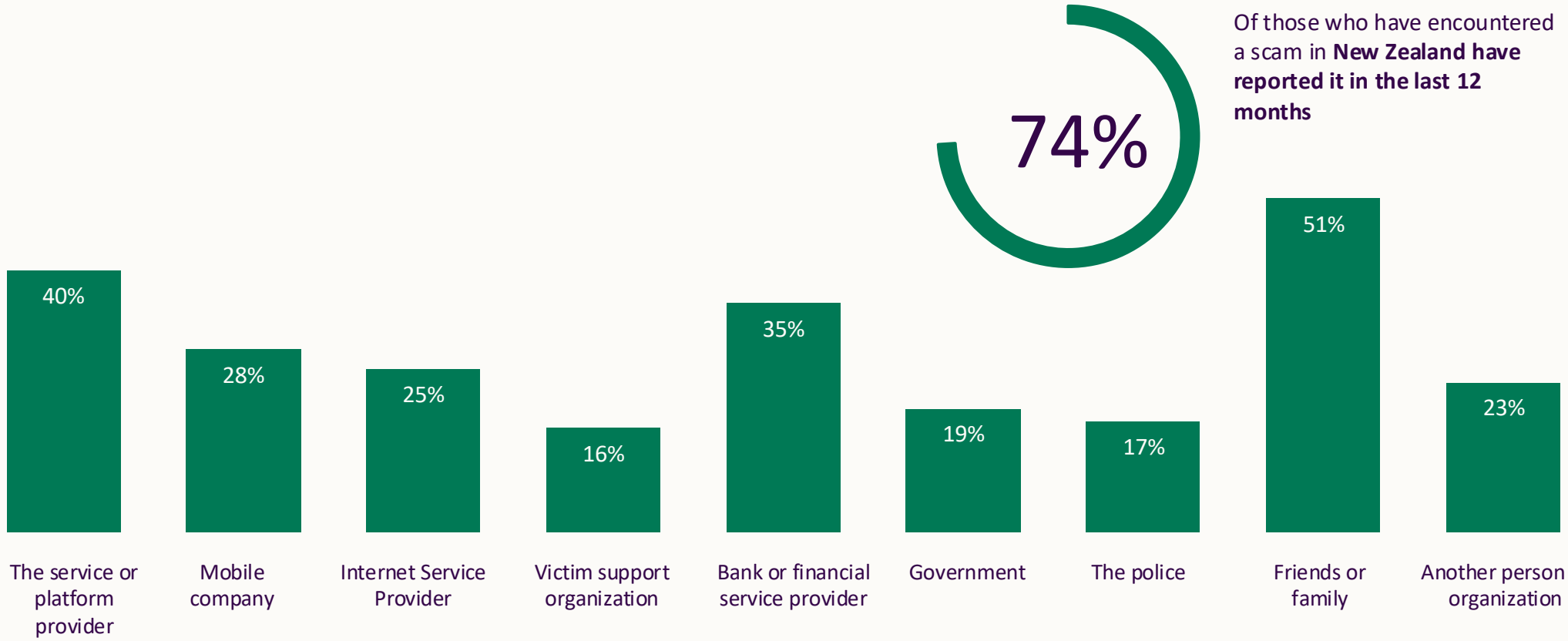
snapchat 3%

LinkedIn 2%

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=884)

New Zealand adults are three times as 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



Of those who have encountered a scam in **New Zealand have reported it in the last 12 months**

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 (884)

New Zealand adults report that information from banks or payment providers and personal experience has 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 (1,180)



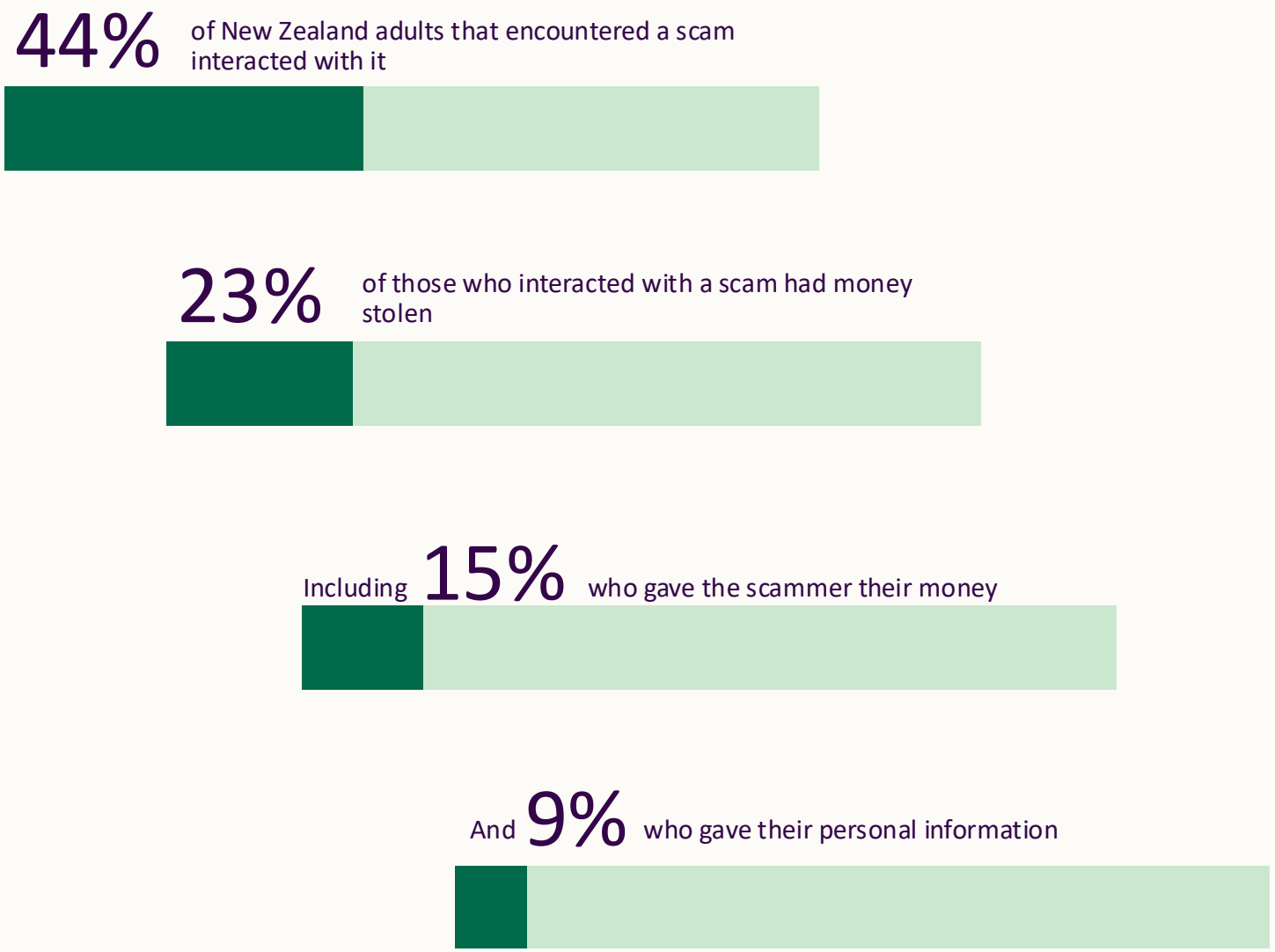
SCAM INTERACTIONS

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.

Two in five New Zealand adults that encounter a scam attempt go on to interact with it

Nearly one in four who interact with a scam have money stolen, either by giving the scammer money, personal information, or both

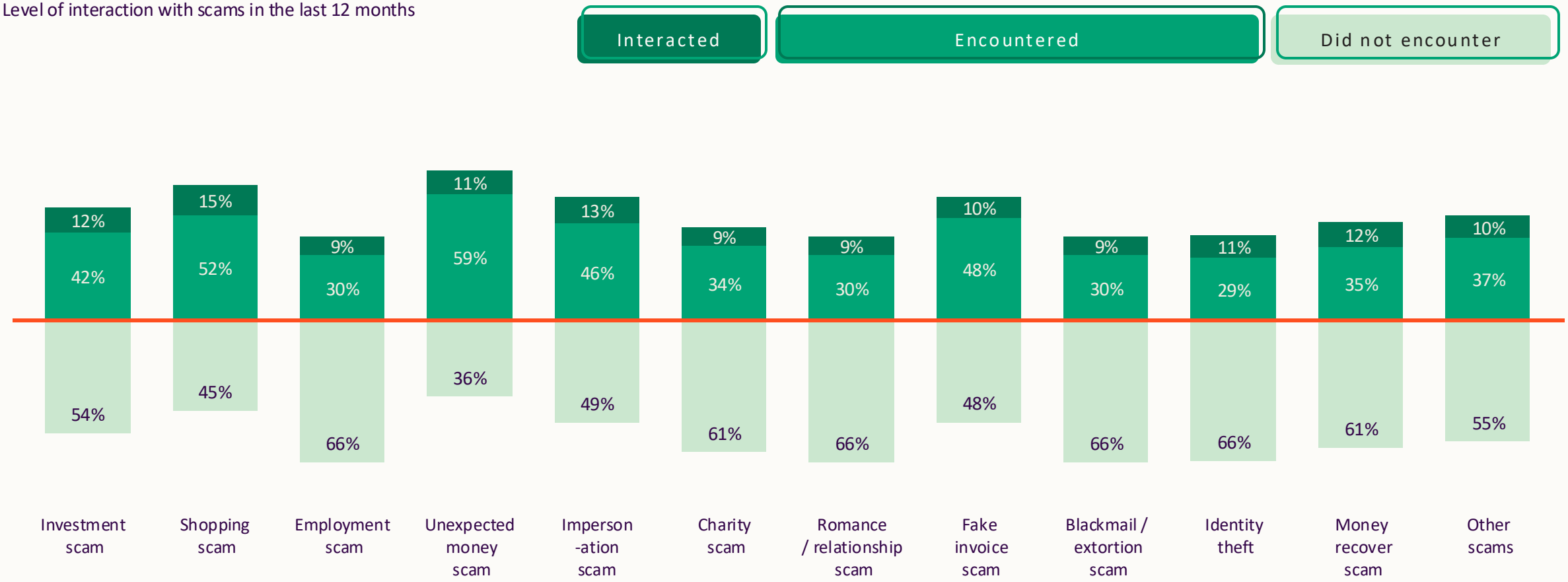
How victims move through the scam funnel



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

New Zealand adults most commonly interact with shopping, impersonation and investment 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 (884)

The main reason New Zealand adults give for not interacting with scams is that they recognize the message or request as not legitimate

Top 10 reasons for not interacting with scam encounters

42% of New Zealand 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: (814)

The inconsistency of message or responses from scammers are the main reasons New Zealand 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 (254)



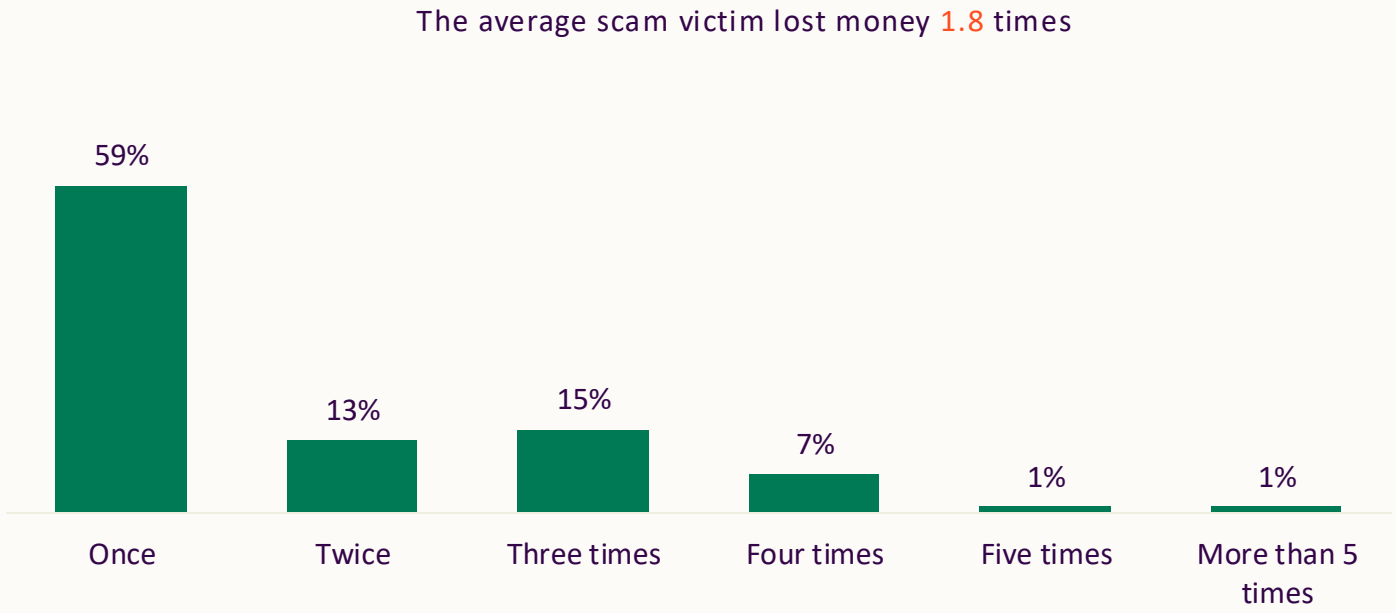
COST OF SCAMS

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

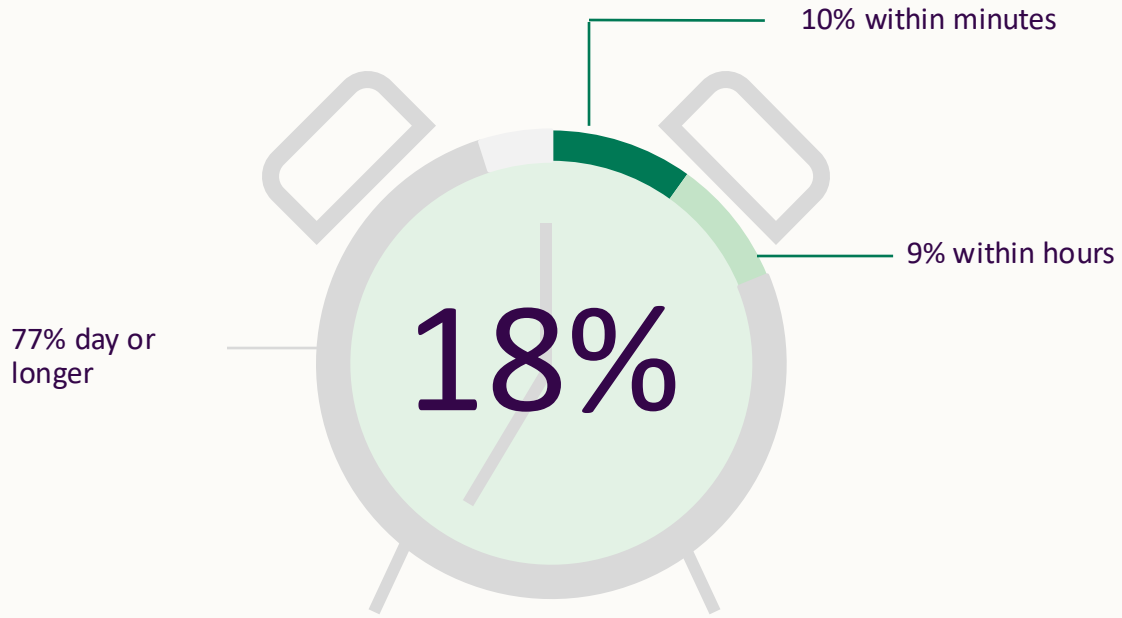


Prevalence of revictimization



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 (90)

Three in four New Zealand adults that lost money to a scam say that the scam lasted a day or longer

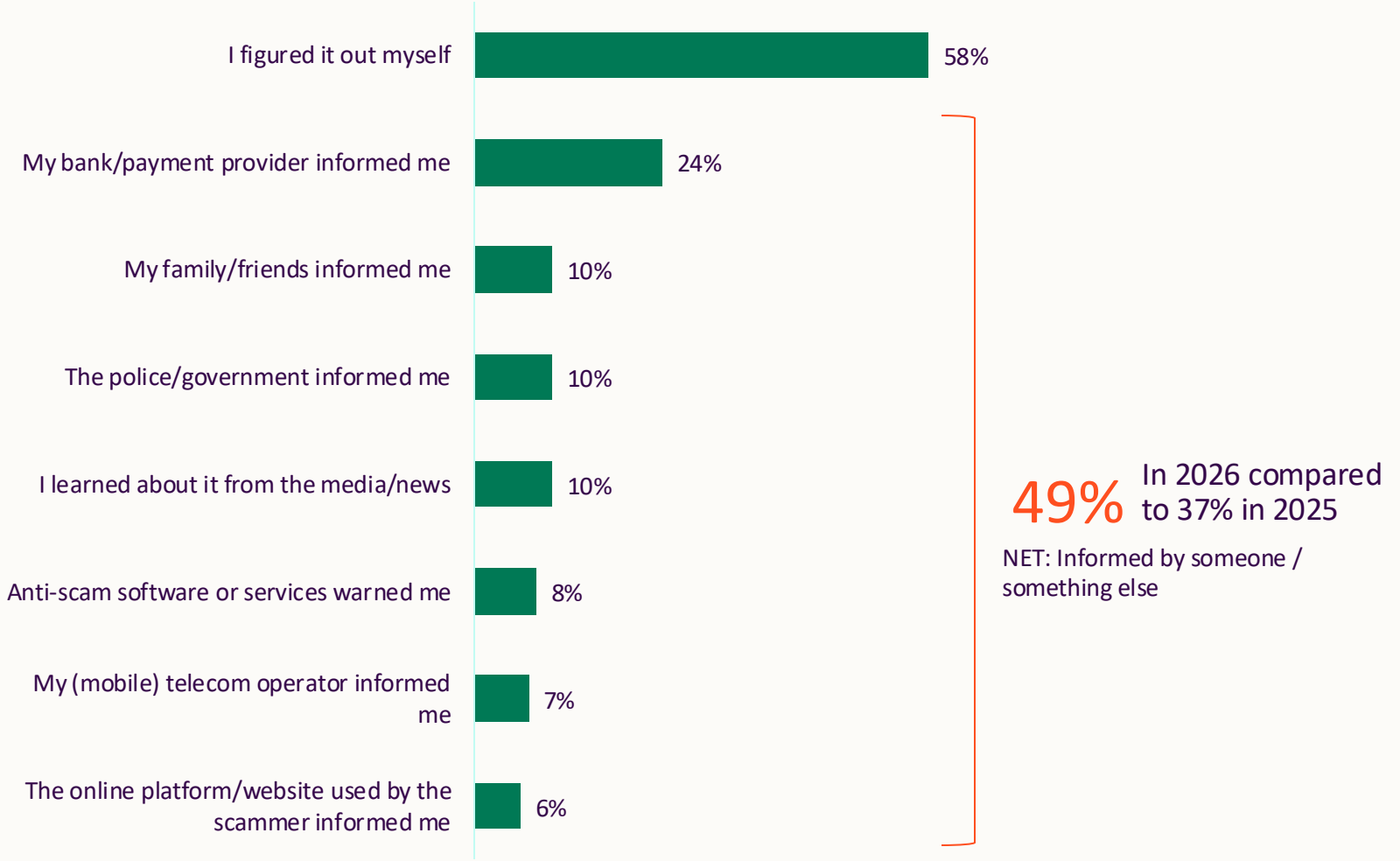


of scams happen within a day of first being contacted by the scammer

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 (90)

There's a rise in New Zealander scam victims discovering they've been scammed after being informed, and a drop in them figuring it out themselves

How victims discovered they were scammed



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 (90).

(US$ 308.9 million)

New Zealand adults lost NZD 503.5 million in the last year with an average loss of NZD 1,623.40

(US$ 996)

*Estimated Scam Losses (95% Confidence Interval)

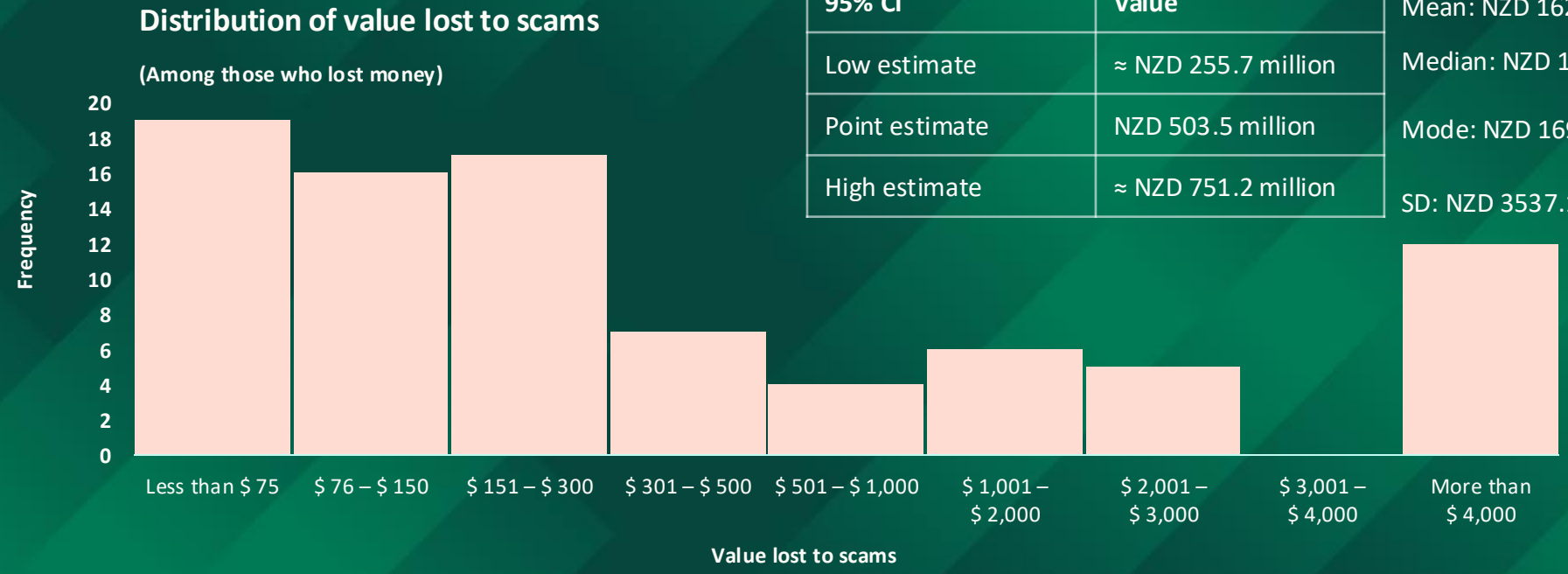
95% CI	Value
Low estimate	≈ NZD 255.7 million
Point estimate	NZD 503.5 million
High estimate	≈ NZD 751.2 million

Mean: NZD 1623.40

Median: NZD 193.70

Mode: NZD 169.3

SD: NZD 3537.10



Click here to see full methodology for average loss calculations

See appendix . Base: All respondents that lost money to a scam (n=90).

I Really Believed He Was a Government Official

A message appeared on Facebook asking me to call a number because of a scam. I was told the caller was a government official investigating my bank. He said the bank staff were the scammers and that they needed my help to catch them. They said they would set up a dummy account in my name. I stupidly believed them. They moved money from my savings account and attempted to transfer it overseas. Even when my bank questioned the transactions, I still believed the bank was the enemy. Thankfully, the bank got the truth from me and stopped the payment. The man had a British accent and was very well spoken. I really believed he was a government official.

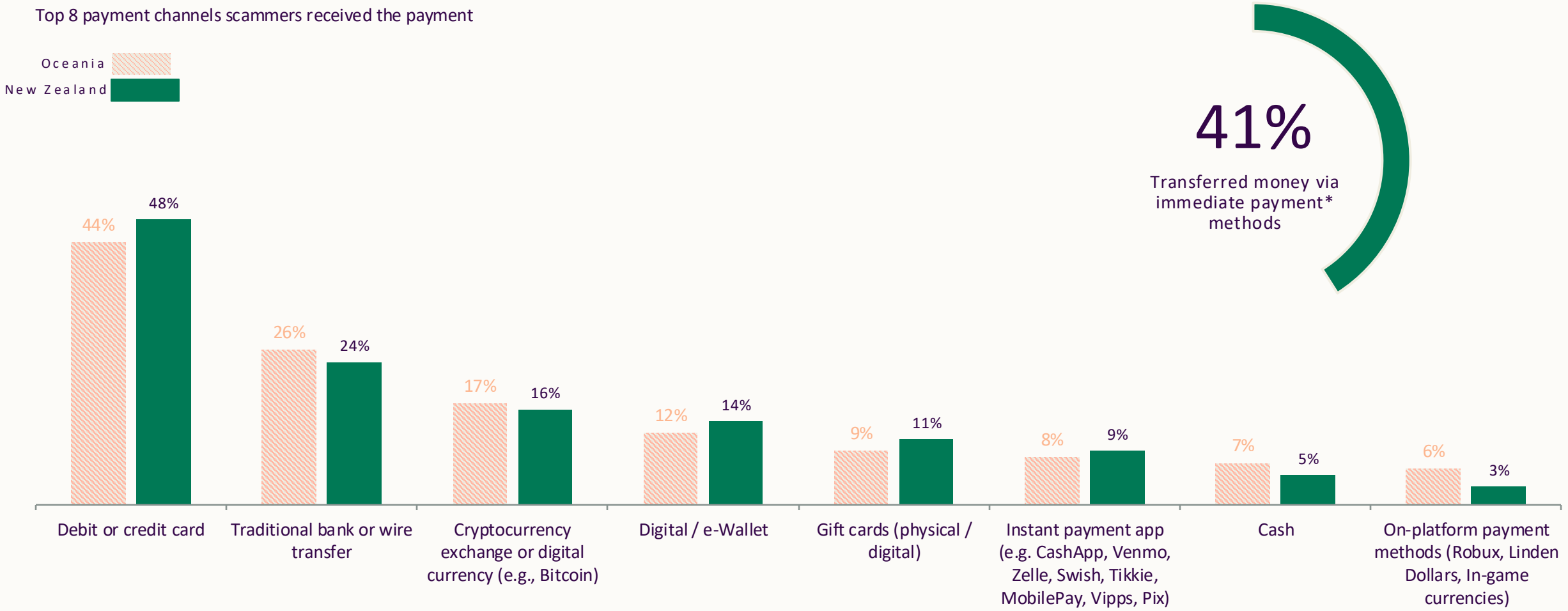
I Thought It Was My Bank

I clicked on a link that I thought was from my bank and logged in. They stole my login details and entered my account. They then transferred money to their own account. This was flagged straight away and my bank called me. I then had to wait a week while the bank and police retrieved my money. My account was frozen until then.

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=90)

Most common ways of a victims send money to a scammer are through debit or credit card, bank transfer or a cryptocurrency exchange

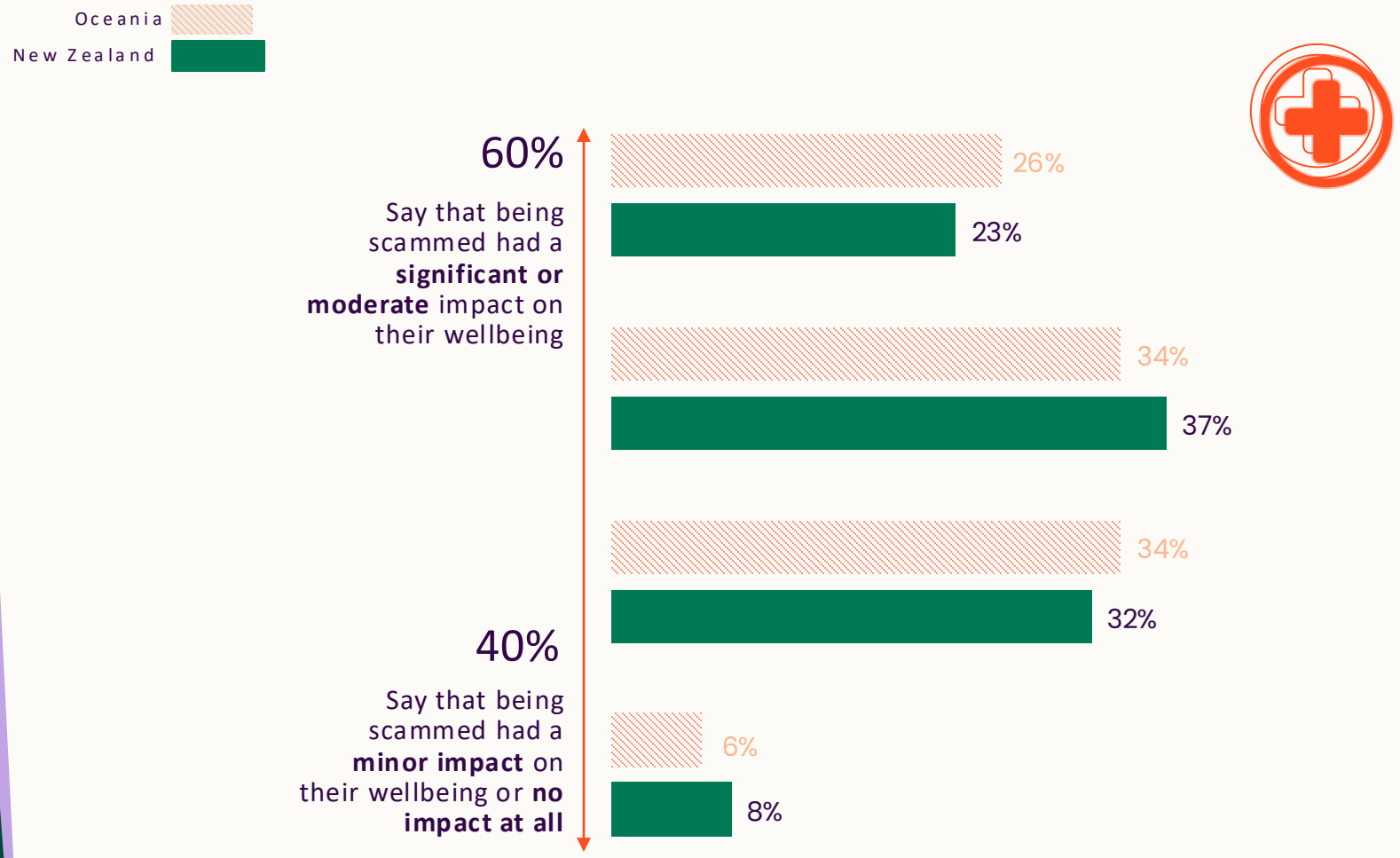
Top 8 payment channels scammers received the payment



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 (Oceania n=175 | New Zealand (90) | *Immediate payment include Instant payment app, gift cards, digital / e-wallet, cryptocurrency exchange and on-platform payment methods

Three fifths of victims say being scammed impacted their wellbeing

Impact of being scammed on wellbeing

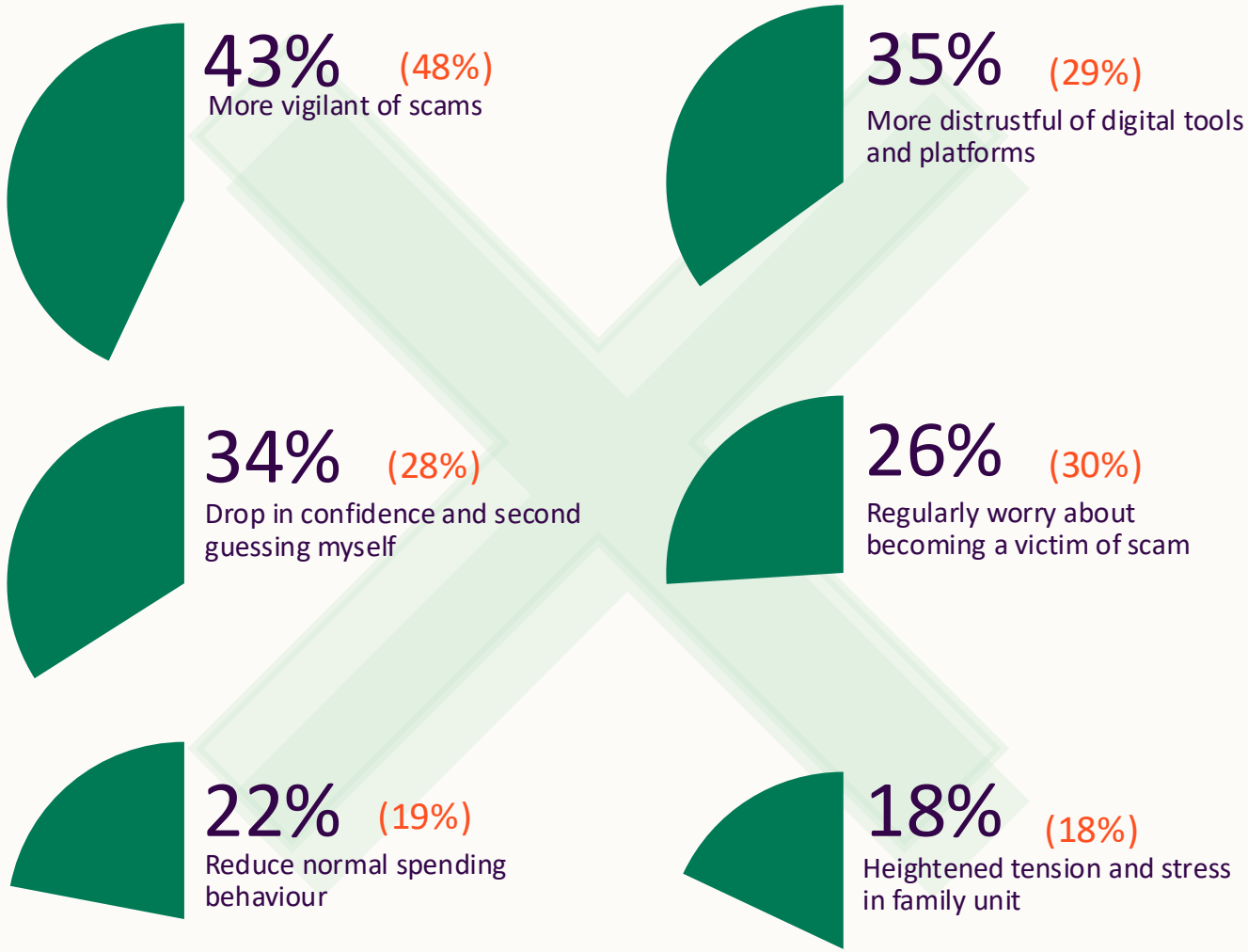


Q14. To what extent did the scam impact your mental wellbeing? Continue to think about the times you've been scammed and lost money in the last 12 months. Base: All respondents that lost money to a scam (Oceania n=175 | New Zealand (90)

GASA Global Anti-Scam Alliance | netsafe

Over a third of those who lost money to a scam experienced drop in confidence

Impact of scams on victims and their family – top 6

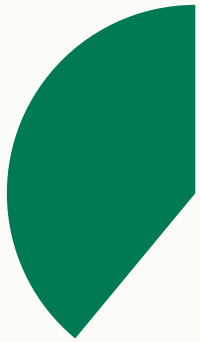


(X%): Oceania

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 (Oceania n=175 | New Zealand (90)

New Zealander victims say scammers were successful because...

Reasons why scams were successful – top 6



39% (36%)
The scam communication looked genuine e.g. realistic emails



37% (32%)
Scammer pretended to be a legitimate organization



34% (32%)
The situation was convincing and realistic



29% (23%)
The offer was too attractive to ignore



22% (26%)
The scammer seems trusted



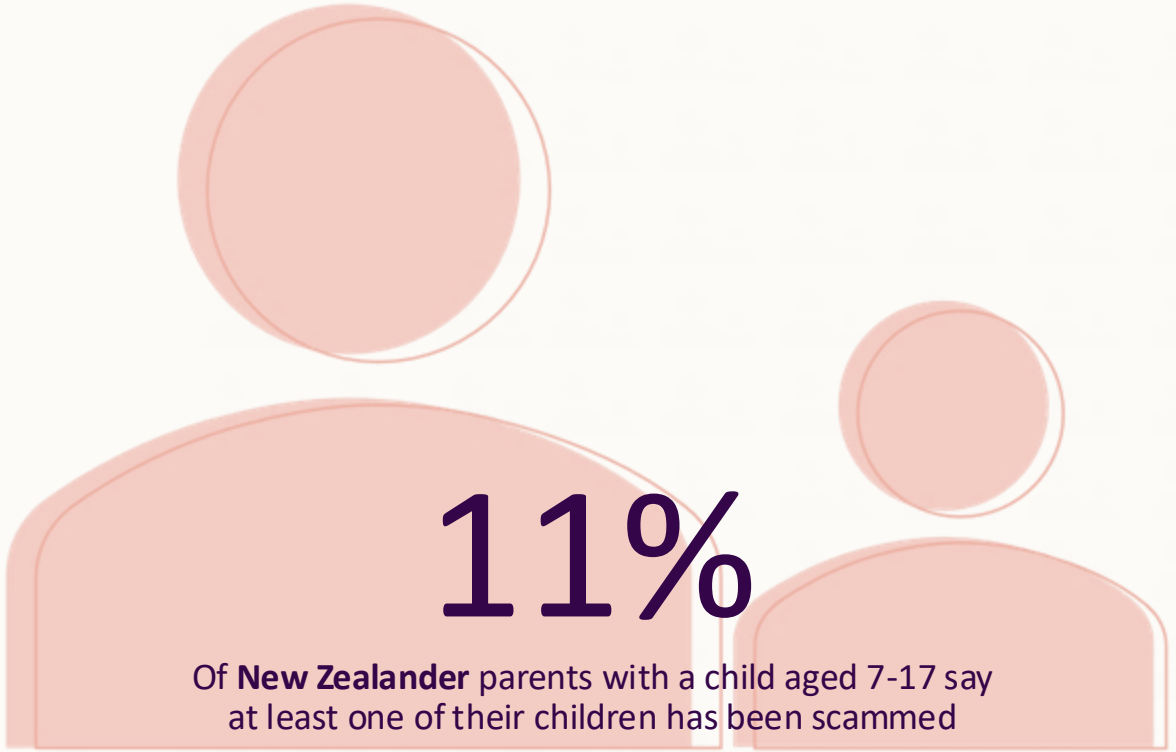
21% (22%)
Thought the scammer offered a good deal

(X%): Oceania

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 (Oceania n=175 | New Zealand (90)

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

Proportion of parents reporting scam experiences among their children



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 (265)

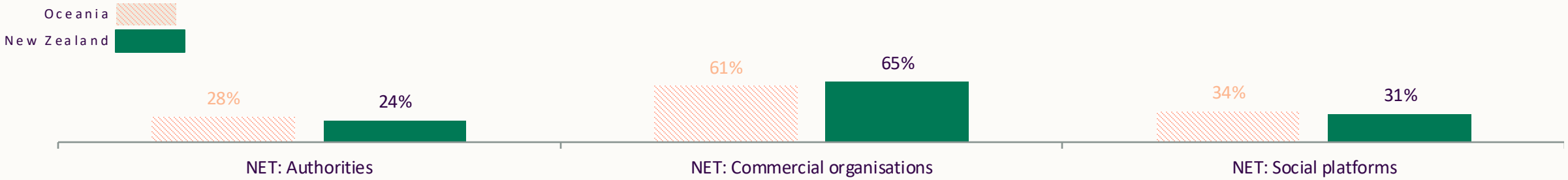


SCAM PREVENTION

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 twice as likely to be reported to commercial platforms than they were authorities

Channels / organizations scams reported to – top 10



Local or national Police	14%	My bank/payment provider	37%	Family and Friends	22%
Financial regulator	9%	Cryptocurrency exchange	14%	Social platform	11%
National reporting website	3%	Internet service provider or hosting company	9%	Online review site	1%
Consumer protection authority or organization	3%	Anti-scam app/website	8%		
		Telecom / mobile operator	7%		
		E-commerce / marketplace	5%		

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 ((Oceania n=1420 | New Zealand (90)

Reports lead to mixed outcomes, with a third being investigated, two fifths are at least partially reimbursed, and one fifth is only acknowledged



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



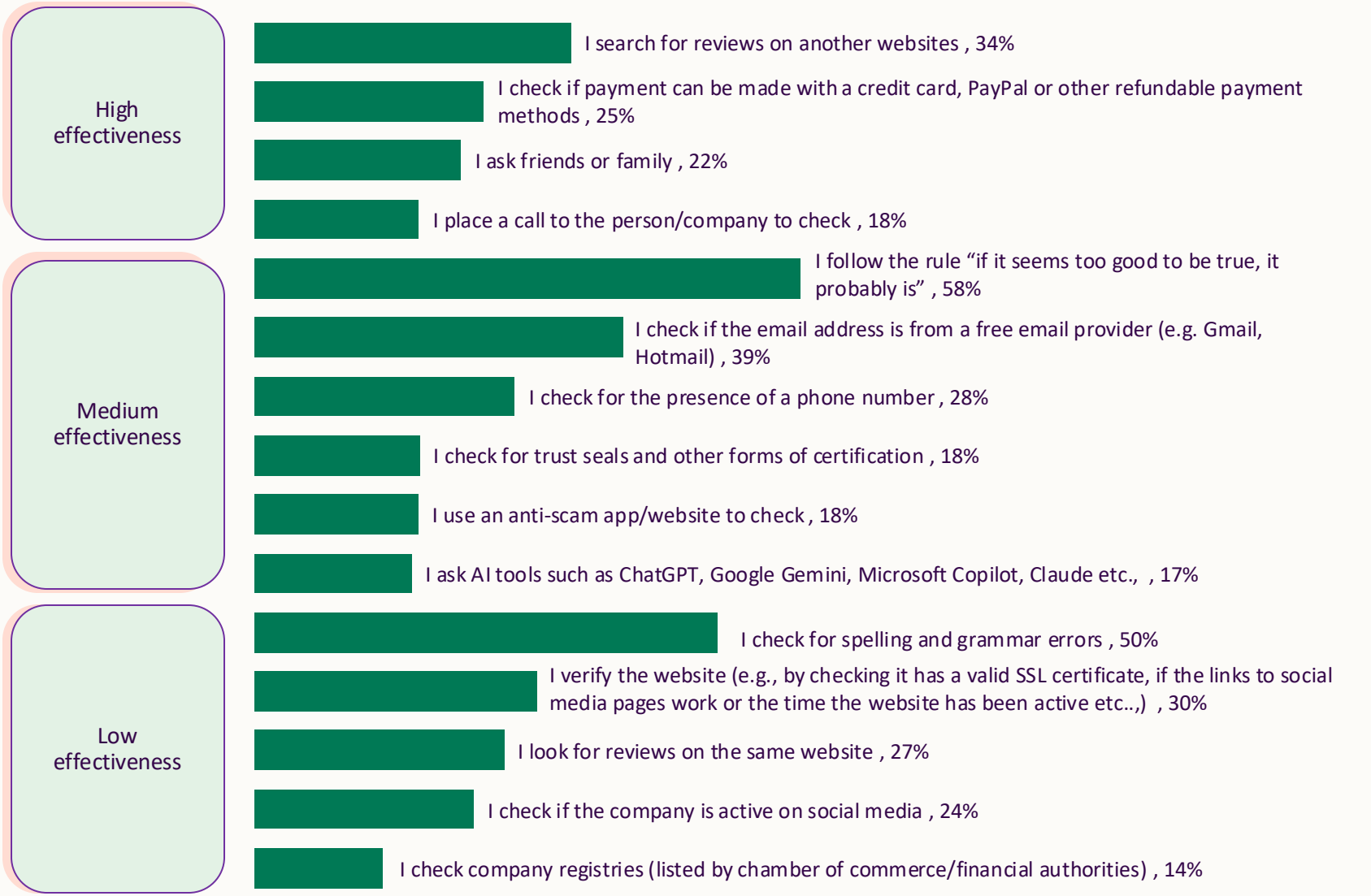
42% of those who reported their losses had money recovered or reimbursed

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 (64)

Across all New Zealand adults, the majority use intuitive "if it seems too good to be true" and grammar checks to verify they are not being scammed

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 (1,180)

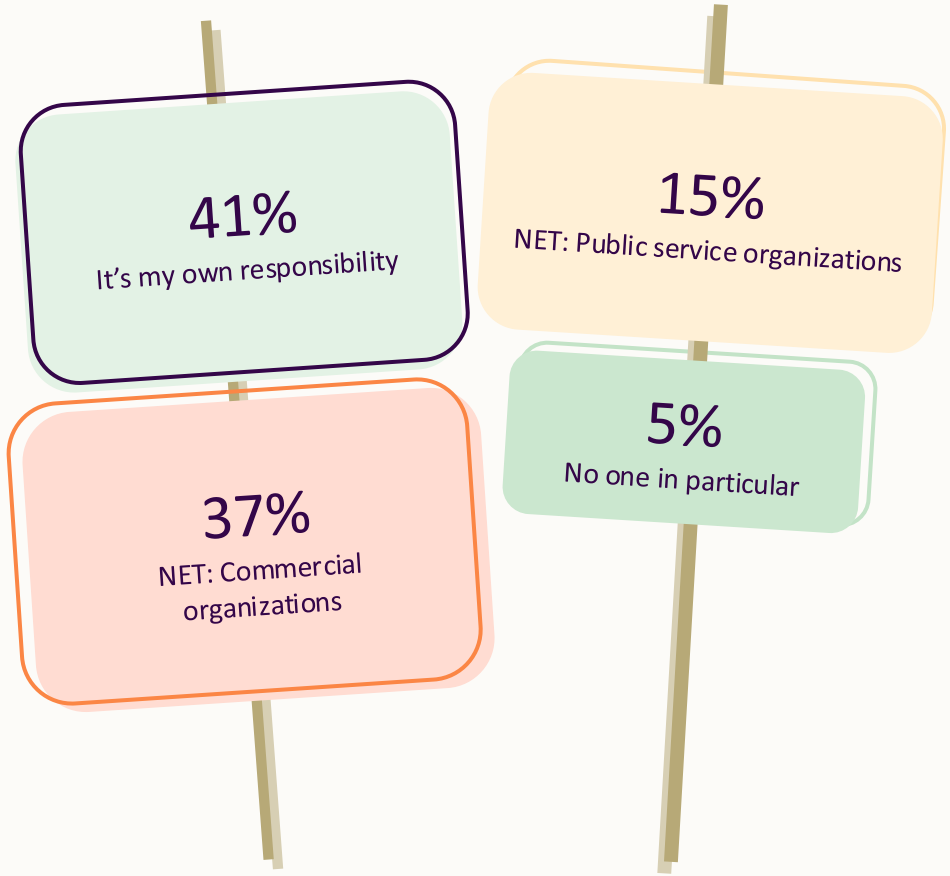
New Zealand adults strongly identify themselves as primarily responsible for protection against scams, followed at a distance by the online platform used by the scammer

Responsibility for keeping people safe from scammers ranking:

- 41% My own responsibility
- 15% The online platform used by the scammer
- 10% The website provider / hosting company used by the scammer
- 9% The government
- 8% My bank/payment method or cryptocurrency exchanger
- 6% The police
- 4% My telecom or mobile operator
- 0% Charities or consumer support associations
- 0% Insurance companies

Most responsible

Least responsible



Q21. Who do you think should be most responsible for keeping people safe from scammers? Base: All respondents (1,180)

Despite this high degree of expected responsibility to protect people from scams, none of the top 3 institutes deliver on effective support in preventing/resolving scams

Responsibility for keeping people safe from scammers ranking:

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

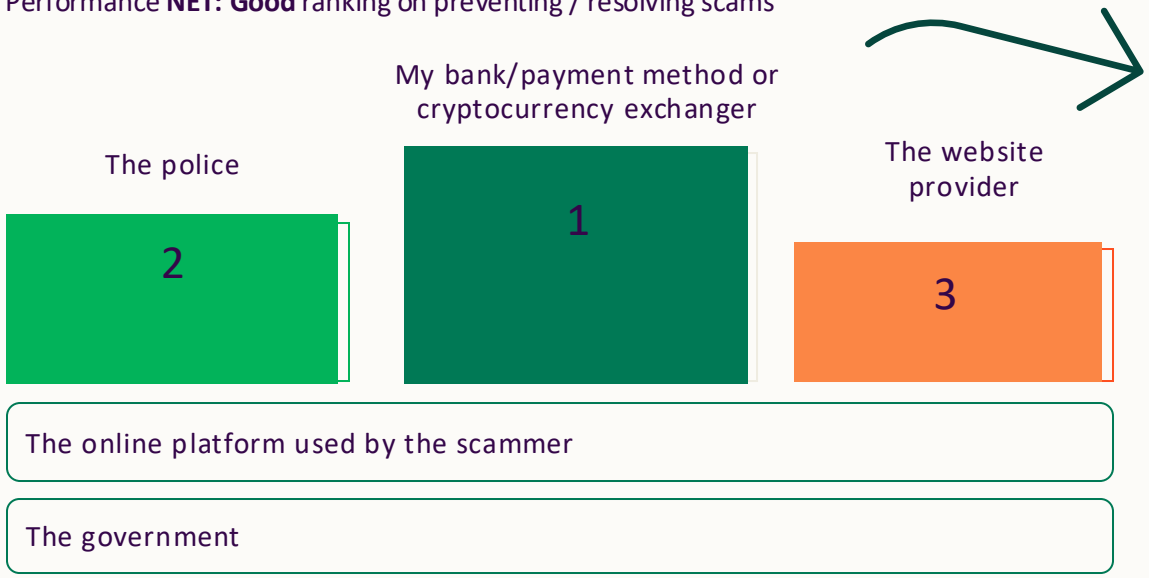
Performance NET: Good ranking on preventing / resolving scams:

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

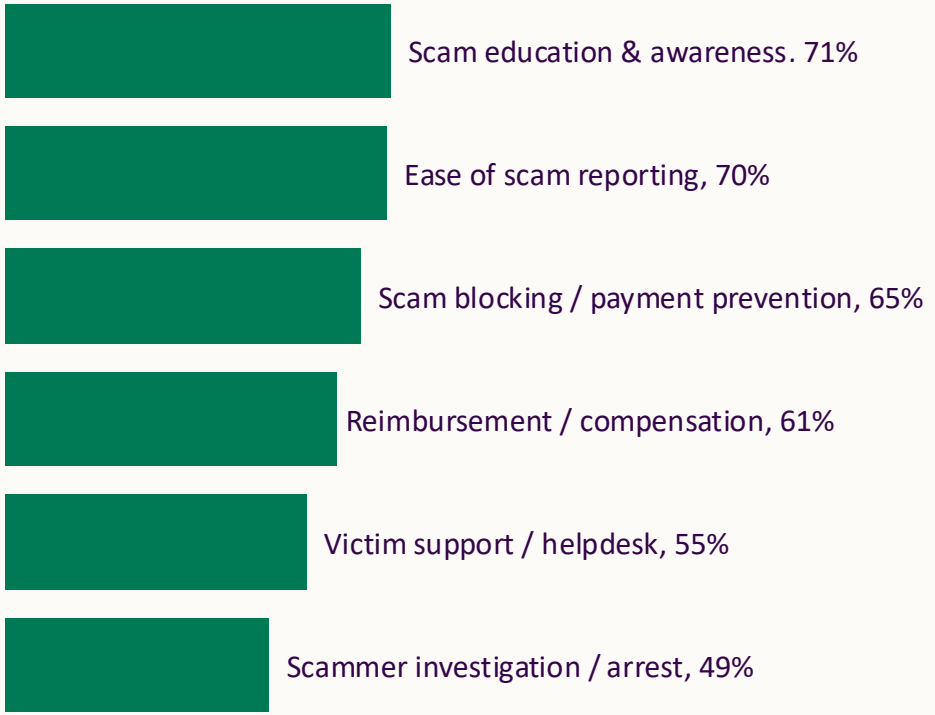
Q21. Who do you think should be most responsible for keeping people safe from scammers? Base: All respondents (1,180) | Q22. You said should be most responsible for keeping people safe from scammers. How do you rate on the following aspects: Base: All respondents that think .. is responsible for keeping people safe from scammers (government n=103 | police n=69 | charities n=5* | online platform 179| website provider n=123 | bank n=91 | telecom operator 43* | Insurance companies 3*) *low base size

Banks/payment method or crypto exchangers are excelling in raising scam awareness and ease of reporting

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



My bank/payment method or crypto exchanger -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=103 | police n=69 | charities n=5* | online platform 179| website provider n=123 | bank n=91 | telecom operator 43* | Insurance companies 3*)) | *charities, insurance and telecom companies and charities not shown due to low base size

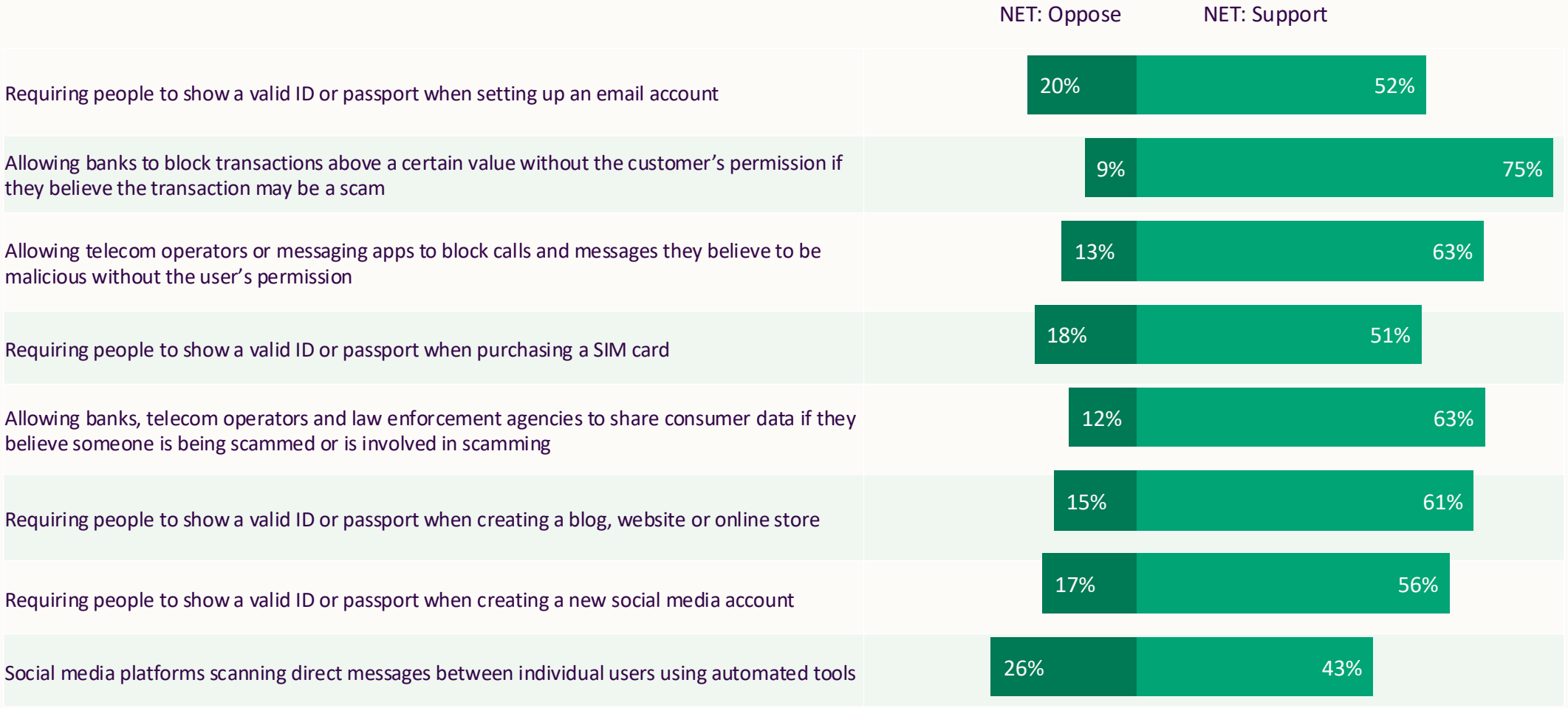
Two in five New Zealand adults believe Banks and Credit Card Companies should always be responsible for reimbursing those experiencing a scam.

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 (1,180)

Coincidingly, strongest support amongst New Zealand adults goes to allowing bank to block transactions 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 (1,180)



ABOUT THIS REPORT

Who are we?

GASA

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

netsafe

Netsafe NZ is an independent non-profit organisation supporting people in Aotearoa New Zealand to have safe and positive online experiences. We keep people of all ages safe online by providing free support, advice and education.

Under New Zealand's Harmful Digital Communications Act, Netsafe runs a helpline service 5 days a week to provide expert incident support to people experiencing harm online.

07 Op Opinium Insights with impact

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

ACCION, Adobe, Aduna, amazon, AnyTech365 AI Powered IT Security, Bitdefender, Capital One, PayPal, Charm, cifas, Citizens, ABN·AMRO, CSC, F-Secure, MEMCYCO, feedzai, FNA, Gen, Gogolook, Google, GSMA, hiya, ibfed International Banking Federation, JPMorganChase, LexisNexis Risk Solutions, LLOYDS BANKING GROUP, Mastercard, Match Group, VISA, McAfee, Meta, Microsoft, TikTok, Nasdaq Verafin, netcraft, TrendLife, OKX, OpenAI, OUTSEER, SCAMADVISER, Scotiabank, TD, Tools for Humanity, THE MEDIA TRUST

Our Corporate Members

Allstate, AnyDesk, Apple, البنك العربي ARAB BANK, Arkose Labs, BANCA BT TRANSILVANIA, BanCoppel, VONAGE Part of Ericsson, BioCatch, CaixaBank, cellcard, Crystal, DANA, EBRAND, FNB, yubo, Globe, indosat OOREDOO HUTCHISON, WORLDLINE, NAVY FEDERAL Credit Union, وزارة الداخلية MINISTRY OF INTERIOR, PAYWARD, pwc, VoiSek, Remitly, Santander, sas, sea, TeamViewer, tieto, true, vodafone, FICO, moomoo



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.

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 online marketplaces, 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