SCAMADVISER

whoscall

The State of Scams in Hong Kong 2024

GASA

Global Anti-Scam Alliance

Fraudsters target 1-in-6 as Hong Kong in 12 months

SCAMADVISER whoscall GASA Global Anti-Scam Alliance

The **2024 State of Scams in Hong Kong** report, a study conducted by the Global Anti-Scam Alliance (GASA), reveals the challenges facing Hongkongers, with frequent scam encounters and significant financial losses. Through the participation of 511 Hongkongers, the study sheds light on the risks faced by the people of Hong Kong and highlights areas for improvement in combating those who seek to defraud.

Despite increasing awareness of scams and their evolving nature, **91% of Hongkongers reported encountering scams at least once per month**, an 8% increase compared to 2023. Only 5% of respondents stated that they rarely face scams. Over the last 12 months, **33% of Hongkongers experienced more scam encounters**, indicating that scams are becoming increasingly prevalent in the region. However, **13% of respondents noted a reduction in scam encounters**, suggesting that some preventive measures may be starting to take effect.

Awareness of scammers using artificial intelligence (AI) is widespread, particularly regarding AI-generated chat and text. However, there is less awareness of more complex AI-generated images and videos. The majority of scams are delivered via phone calls or text/SMS messages, with a **10% increase in SMS scams since last year**. Instant messaging apps, emails, and social media platforms also serve as common mediums for scams. Platforms like WhatsApp and Facebook are frequently exploited, contributing to the challenges faced by Hongkongers in identifying and avoiding scams.

The financial and emotional impact of scams in Hong Kong is substantial. Only 1% of victims were able to fully recover their losses—a worrying figure that reflects a 2% decrease in successful recovery compared to 2023. The average amount lost per victim was $1,581, and the emotional toll has risen, with 54% of victims reporting a strong emotional impact, a 7% increase from last year.

The underreporting of scams remains a significant issue, with **76% of Hongkongers opting not to report scams to law enforcement**—a 5% increase from the previous year. This trend indicates a growing lack of trust in the ability of authorities to take meaningful action. Many believe that reporting scams will not lead to the recovery of their funds, while others cited the complexity of reporting processes as a deterrent. Among those who did report scams, local police stations and police websites were the primary channels used, followed by anti-fraud apps and banks.

Authority scams are the most common type of scam in Hong Kong, often involving scammers impersonating government officials to create a sense of urgency and fear. Victims shared stories of phone calls from individuals claiming to be mainland Chinese officials, false messages about fines, and even impersonations involving family emergencies to solicit money. Additionally, scams involving fake online shopping and counterfeit products were frequently reported.

Trust in the internet has eroded significantly, with 65% of Hongkongers expressing less trust due to scams. Only 11% reported no loss of trust, indicating the pervasive impact of online fraud on digital confidence. To mitigate risks, 43% of respondents reported checking for the presence of a phone number to verify legitimacy, while others used anti-fraud apps and paid attention to spelling and grammatical errors in communications.

Despite the challenging situation, a hopeful sign is that **78% of those scammed came to their own conclusion that they had been deceived**, often before more significant damage could occur. However, the people of Hong Kong need stronger support from their government, financial institutions, and tech platforms to protect them from the growing threat of scams. With only 17% of participants rating government efforts to combat scams positively and 41% expressing dissatisfaction, there is a clear call for action to enhance public safety measures, improve reporting systems, and restore confidence in the fight against fraud.

Jorij Abraham
Managing Director

GASA Global Anti-Scam Alliance

Sam Rogers
Director of Marketing

Hong Kong's Escalating Scam Threats Require AI-Driven Fraud and Consumer Protection Strategies

SCAMADVISER whoscall GASA Global Anti-Scam Alliance

ScamAdviser is a global leader in scam prevention, committed to empowering businesses with its AI-powered Anti-Scam Intelligence (ASI). ScamAdviser provides real-time detection of suspicious activity and scam prevention for websites, calls, messages, and online platforms. With the world's largest scam database, ScamAdviser partners with over 400 organizations to protect more than 1 billion consumers worldwide, helping people confidently navigate the digital world. In this interview, **Aaron Chiou, Product Director of ScamAdviser**, will describe the current state of scams in Hong Kong and the advanced strategies needed for enterprises to protect consumers.

How significant has the issue of scams become in Hong Kong? The issue of scams in Hong Kong has grown significantly, with 91% of Hongkongers encountering scams at least once per month—an 8% increase from the previous year. Even more concerning is the financial losses due to scams, which now total $1.5 billion, equivalent to 0.4% of Hong Kong's GDP. The rise of AI has further complicated the scam landscape. Reports show that Hongkongers have a good understanding of the threats posed by generative AI, which may help them better protect themselves, however, the question may land on how to identify these threats.

What types of scams have trended in Hong Kong recently? The issue of scams in Hong Kong has grown significantly, with 91% of Hongkongers encountering scams at least once per month—an 8% increase from the previous year. The rise of AI has further complicated the scam landscape. Reports show that Hongkongers have a good understanding of the threats posed by generative AI, which may help them better protect themselves, however, the question may land on how to identify these threats.

What types of scams have trended in Hong Kong recently? Recent trends in scams in Hong Kong show that authority scams are the most common type encountered, where scammers impersonate government officials or other authoritative figures to deceive victims. Additionally, scams delivered via phone calls, text/SMS messages, and instant messaging apps have seen significant increases, with a 10% rise in text message scams compared to the previous year. Popular platforms for these scams include WhatsApp and Facebook, a growth of 5% more Facebook scams reported in 2024 compared to 2023.

Which actions have been taken by the government and other organizations to protect consumers from scams? Any best practices from which we can learn? In Hong Kong, many people still fall victim to scams due to their inability to recognize scam schemes, compounded by a lack of trust in and unfamiliarity with reporting channels. Only 1% of victims have been able to fully recover their losses. To address this issue, Hong Kong has actively invested in anti-scam initiatives and educational campaigns. The Hong Kong Police Force has partnered with tech companies to develop a caller ID app that helps users identify scam calls. They are actively promoting its use while continuously updating and optimizing the app to keep pace with evolving scam tactics.

Hong Kong Telecom has also integrated a caller ID service into its offerings, providing consumers with a safer communication environment by helping them identify and block potential scam calls. This service enhances security and supports broader efforts to combat scam in Hong Kong.

What further actions could give consumers the upper hand in fighting scams? To give consumers the upper hand in fighting scams, expanding public education on AI-driven scam tactics is essential. Further integration of advanced caller ID services, such as real-time scam detection from Hong Kong Telecom is helpful in enhancing user protection. Simplifying the reporting process through apps and offering incentives for reporting would encourage more victims to come forward. Finally, stronger legal frameworks and international cooperation to combat cross-border scams would create a more robust defense against scammers. Collaboration between sectors is key to significantly bolstering consumer protection against scams.

Aaron Chiou
Product Director

SCAMADVISER

Whoscall's Role in Combatting Hong Kong's Growing Scam Crisis

Whoscall, powered by Gogolook, is a cutting-edge digital anti-scam tool designed to protect users from scams across various channels, including phone calls, text messages, and links. In the Hong Kong 2024 State of Scams report, GASA interviewed William Wu, HK VP of Technology at Gogolook, to share insights on the in-depth analysis of the evolving scam landscape in Hong Kong, to equip consumers with the knowledge and tools they need to stay one step ahead of scammers.

How big has the problem of scams become in Hong Kong?

In Hong Kong, the problem of scams has reached critical levels. In the first seven months of 2024, the total financial loss from various scams exceeded 5.1 billion HK dollars (approximately US$653 million) according to police research. During this period, Hong Kong reported 24,407 scam cases, which is a 12 percent increase compared to the same timeframe in 2023.

Which scams have been trending in Hong Kong over the past?

In fact, scam syndicates constantly adapt their methods to maximize profits. The number of scam cases has risen significantly, the main reason is the increased number of phone scams. Recently, we have identified a new type of scam involving scammers impersonating customer service. For example, scammers often pose as staff from online shopping or payment platforms, claiming the victim has subscribed to an auto-renewing service. They instruct the victim to click a link and enter bank details, which allows the scammers to steal money. In addition to phone scams, romance scams now use deep fake technology. 62.3% of scams are Internet-related.

Which actions have been taken by the government and other organizations to protect consumers from scams? Any best practices from which we can learn?

The Hong Kong Police Force (HKPF) has developed a website (CyberDefender) and an app (Scameter) for anti-scam purposes. This system integrates various data sources from leading cybersecurity service providers around the world. Gogolook serves as a key scam data partner, helping safeguard Hong Kong users from scam calls and malicious URLs.

Multiple measures have been rolled out by HKPF including collaboration with the banking industry to intercept fraudulent payments. Collaboration with the telecommunications industry blocking scam calls and suspending phone numbers related to fraudsters. HKPF also collaborated with five major catering groups to educate the citizens about the new modus and how to protect themselves.

HKPF targets students, staff and immigrants about the scam awareness and asks them to install Scameter+ App to prevent it . On the other hand, Police had mounted joint operations with law enforcement agencies against laundering of crime proceeds and receiving of fraudulent payments through stooge accounts.

HKPF e-Report Centre allows citizens to report technology crime or deception on the HKPF website., while the Office of the Communications Authority(OFCA) promotes people of Hong Kong to use scam blocking services provided by telecoms or APPs including Whoscall and Call Defender.

What action would you like to see taken that could give consumers the upper hand in the fight against scams?

To effectively combat scams, a collaborative approach is essential, focusing on technology development, public education, and stronger law enforcement, with a focus on tackling AI-driven scam. Ongoing scams have eroded public trust, leading people to avoid calls from unknown numbers, including legitimate ones. To restore this trust, we should implement technology that identifies important calls, ensuring that crucial communications aren't overlooked.

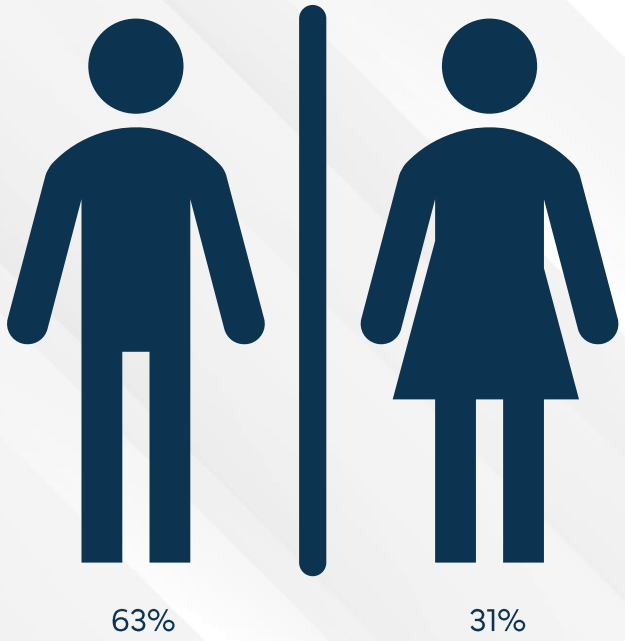
William Wu
HK VP Technology
Gogolook

511 Hongkongers completed the State of Scams survey

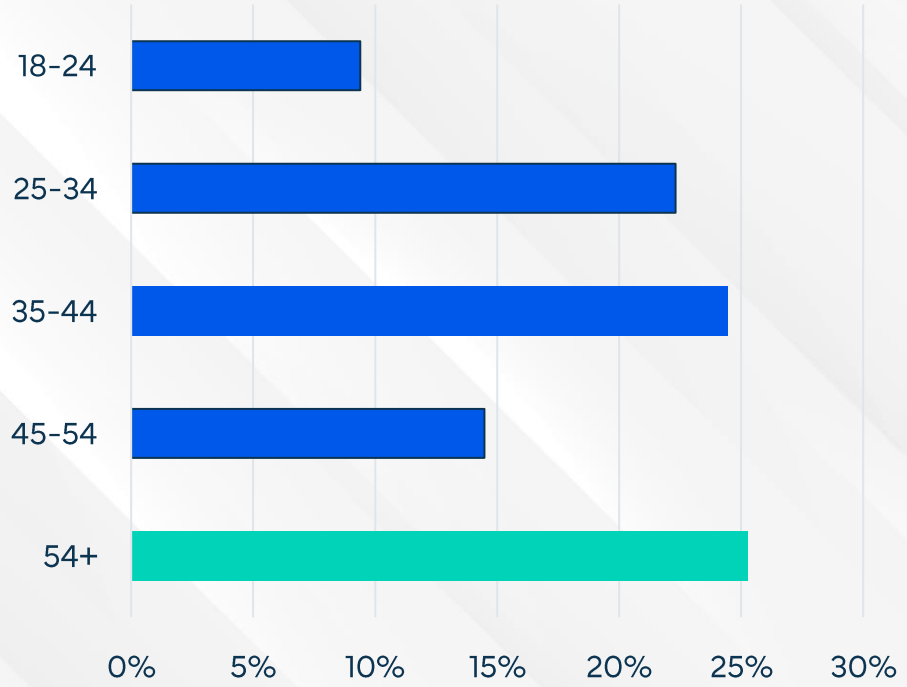
SCAMADVISER whoscall

GASA Global Anti-Scam Alliance

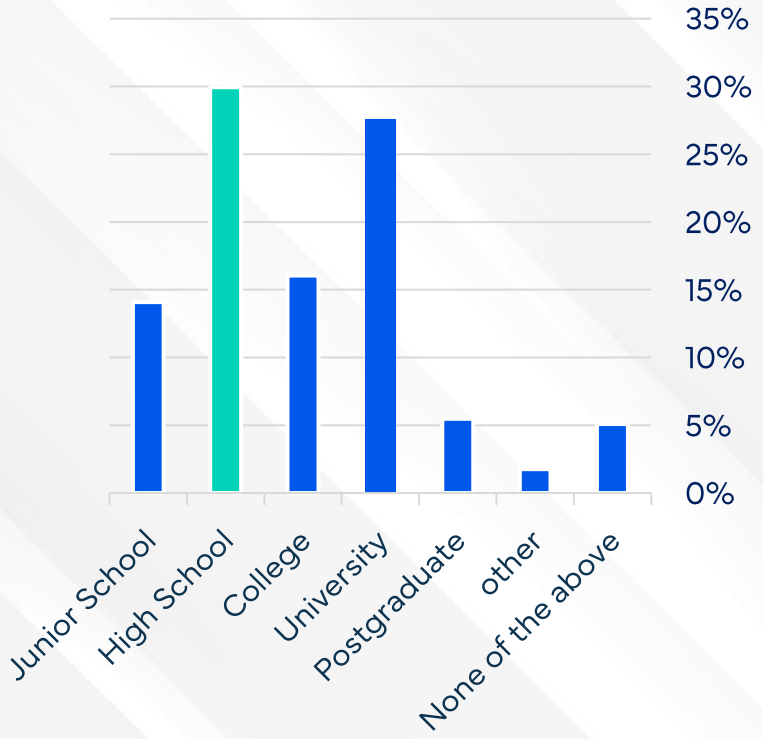
Gender



Age Range

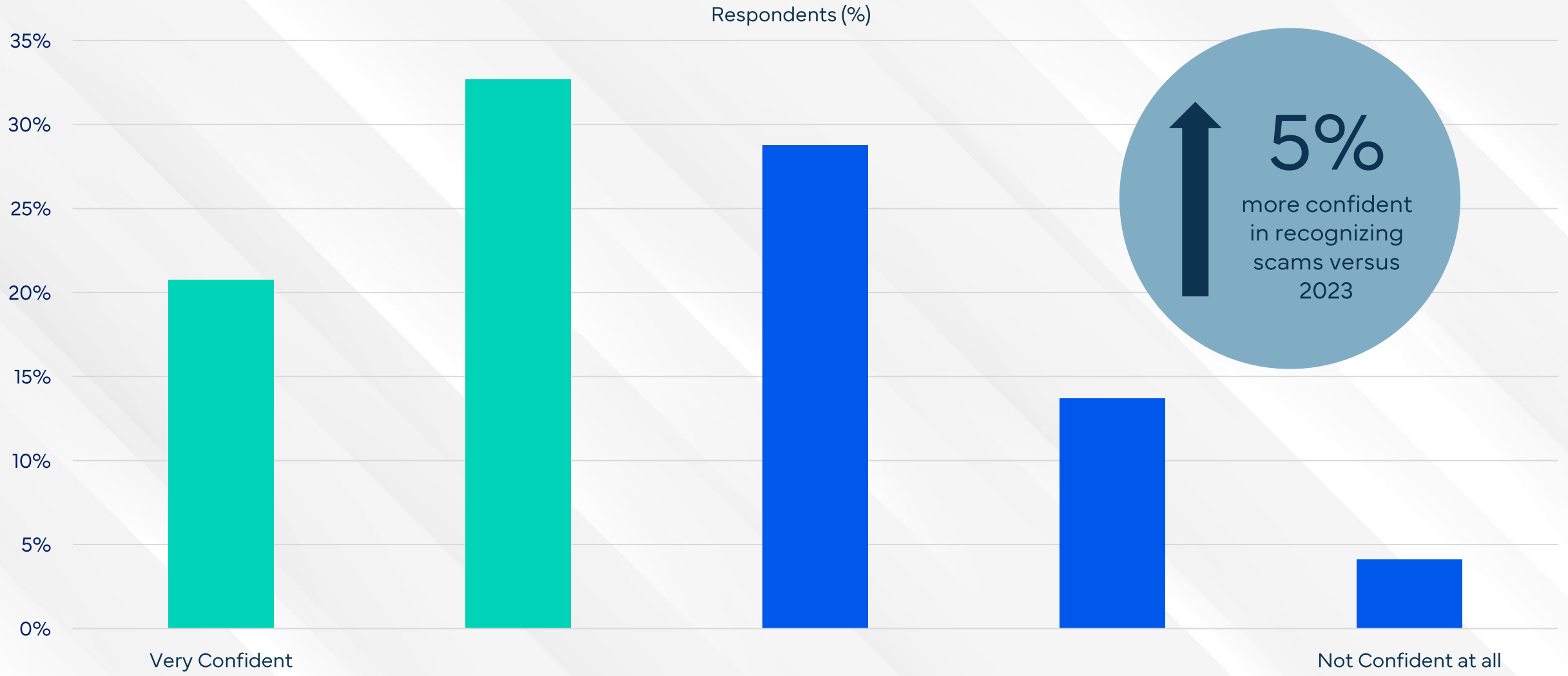


Education



The demography of respondents to the State of Scams in the Hong Kong 2024 survey consists of more men than women. A large proportion were over 54 years with high school education.

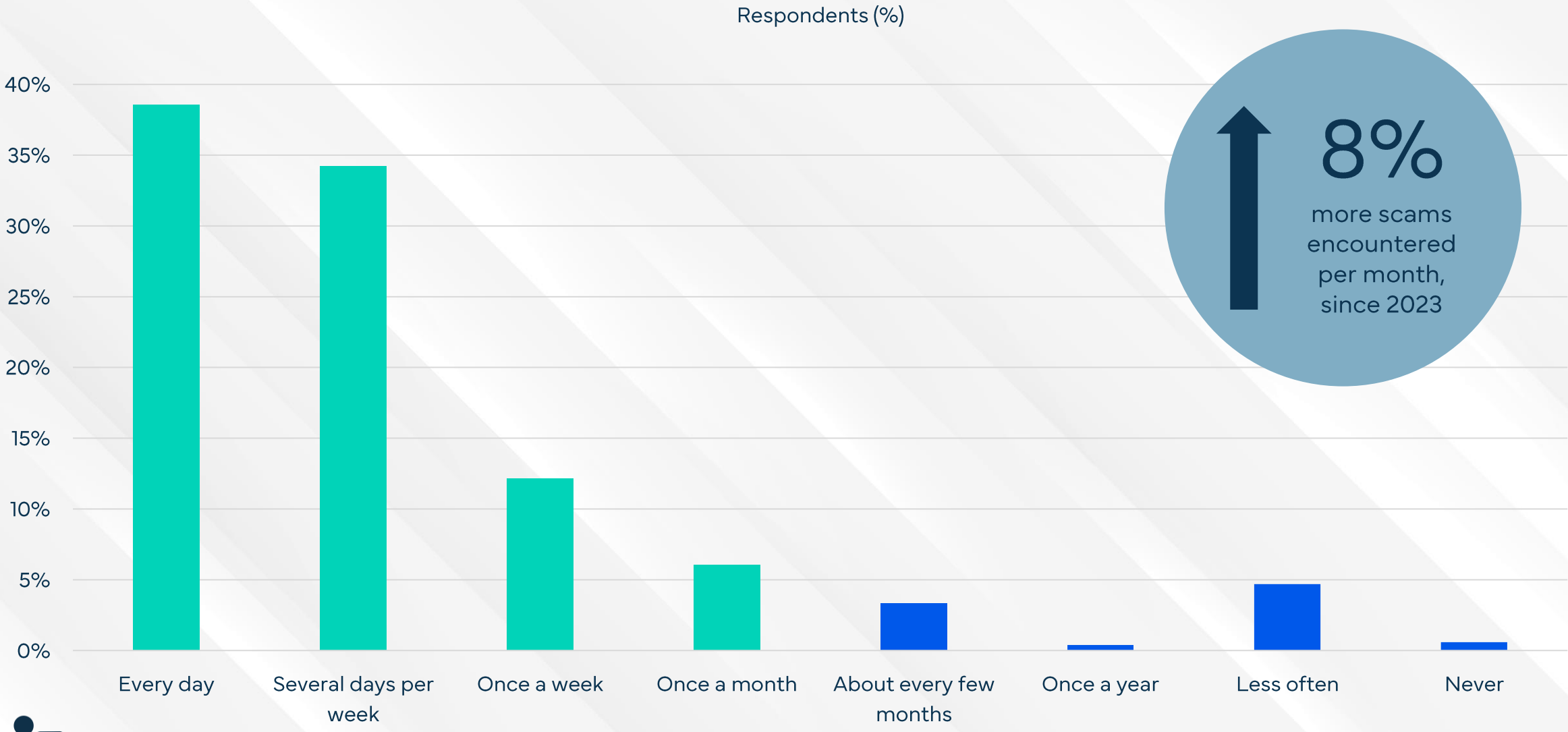
53% of Hongkongers are confident in their ability to recognize scams



Only 18% of respondents are not (very) confident in recognizing scams, at all.

Q2 - How confident are you that you can recognize scams?

91% of Hongkongers encounter scams at least once per month

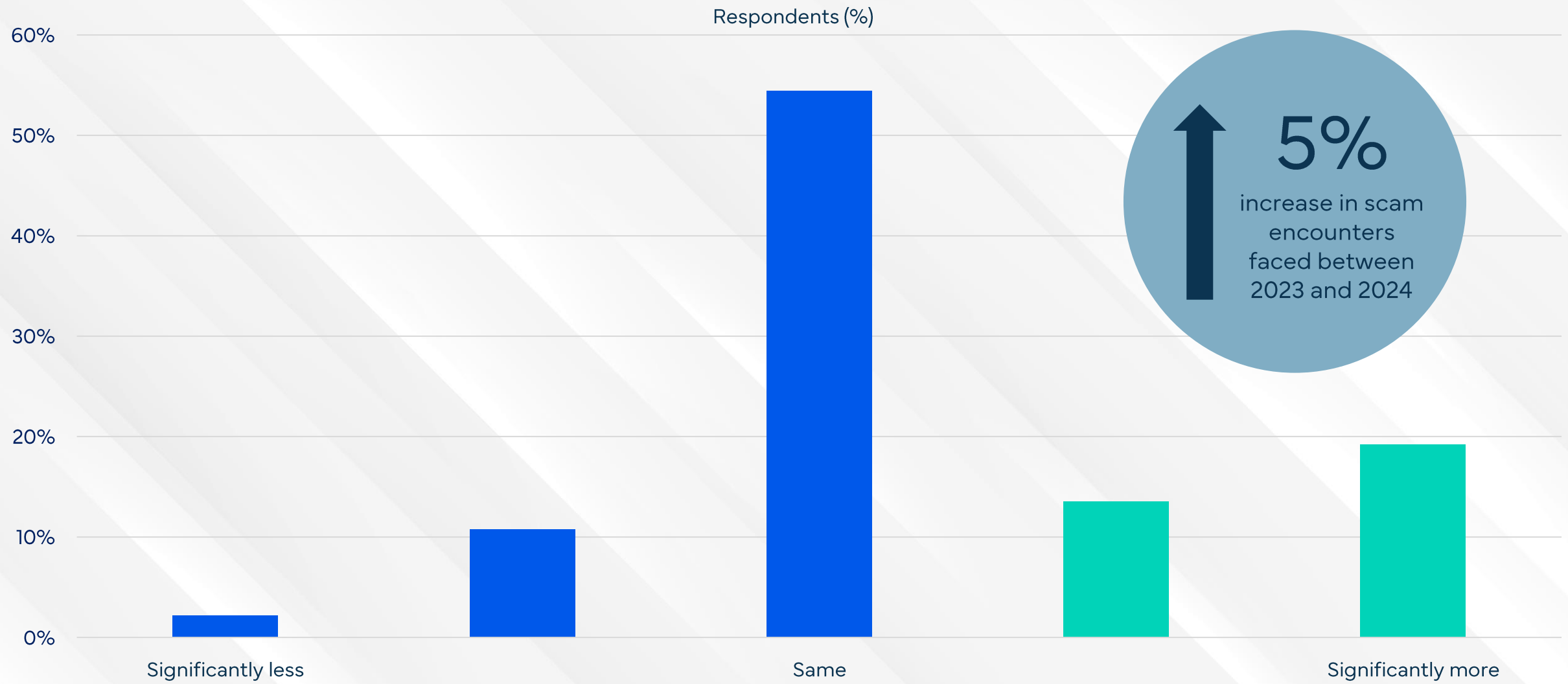


8%
more scams encountered per month, since 2023

5% of Hong Kong survey respondents revealed that they are rarely confronted by scams..

Q3 - In the last 12 months, how often have you been exposed to scam attempts? This includes receiving suspicious content, as well as seeing deceitful advertising.

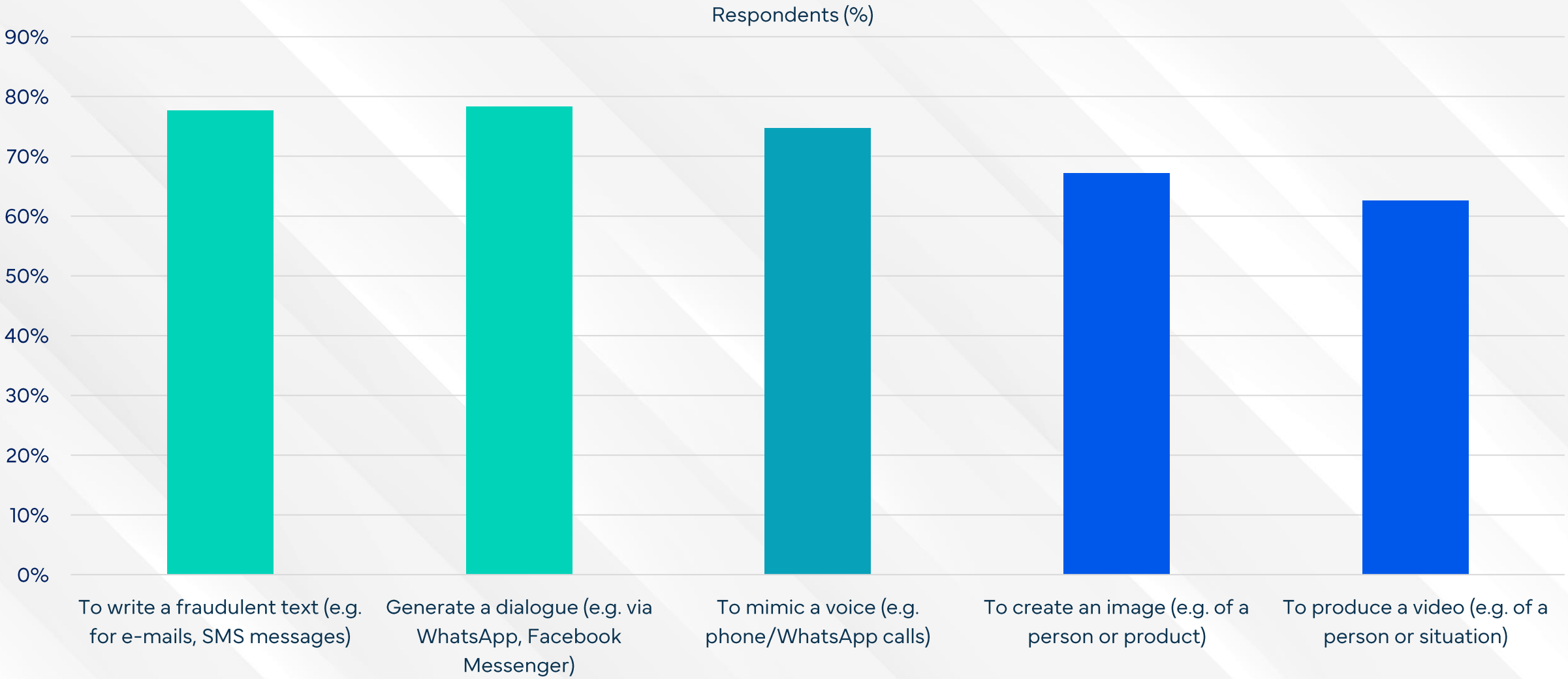
33% of Hongkongers faced more scam encounters in the last 12 months



13% of Hongkonger respondents experienced a reduction in scam encounters in the past 12 months.

Q4 - Compared to the year before, do you feel you have been exposed more or less frequently by an individual/company that tried to deceive you in the last 12 months?

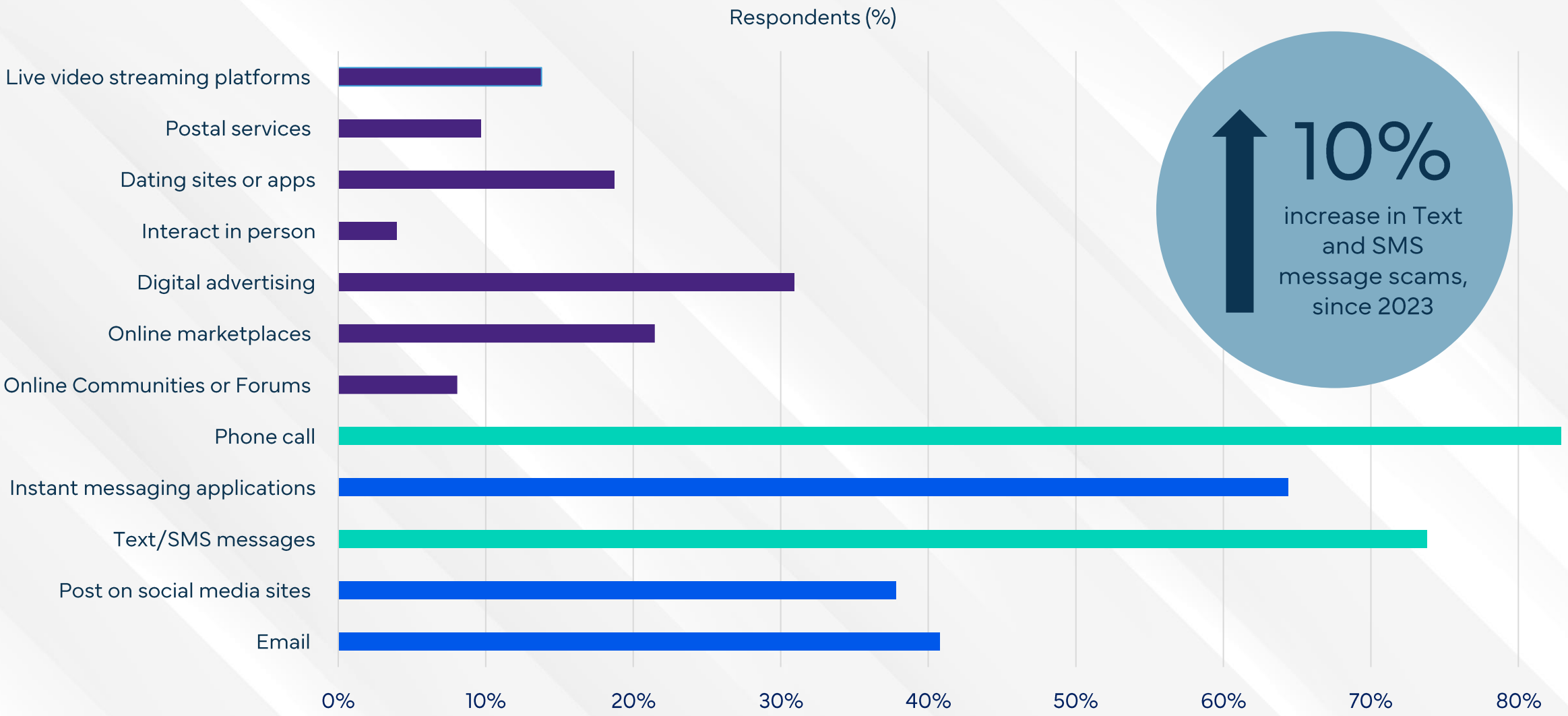
Most Hongkongers are aware scammers can use AI against them



Awareness of AI generated chat & text is high, while complex images & videos are less widely known.

Q5 - For which of the following can Artificial Intelligence (AI) be used?

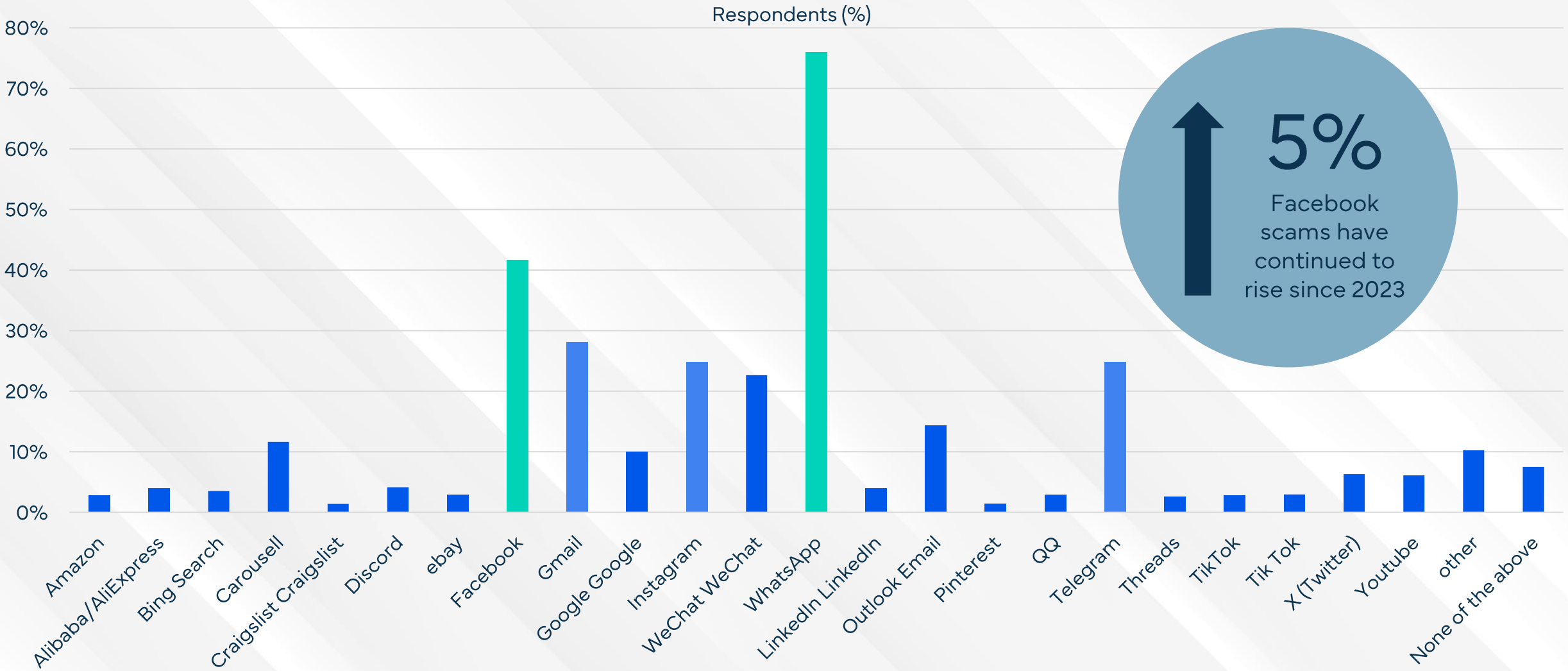
Majority of scams are delivered via phone calls or text/SMS messages



Instant messaging apps, emails, and social media platforms are also common scam media.

Q6 - Through which communication channel(s) did scammers approach you in the last 12 months?

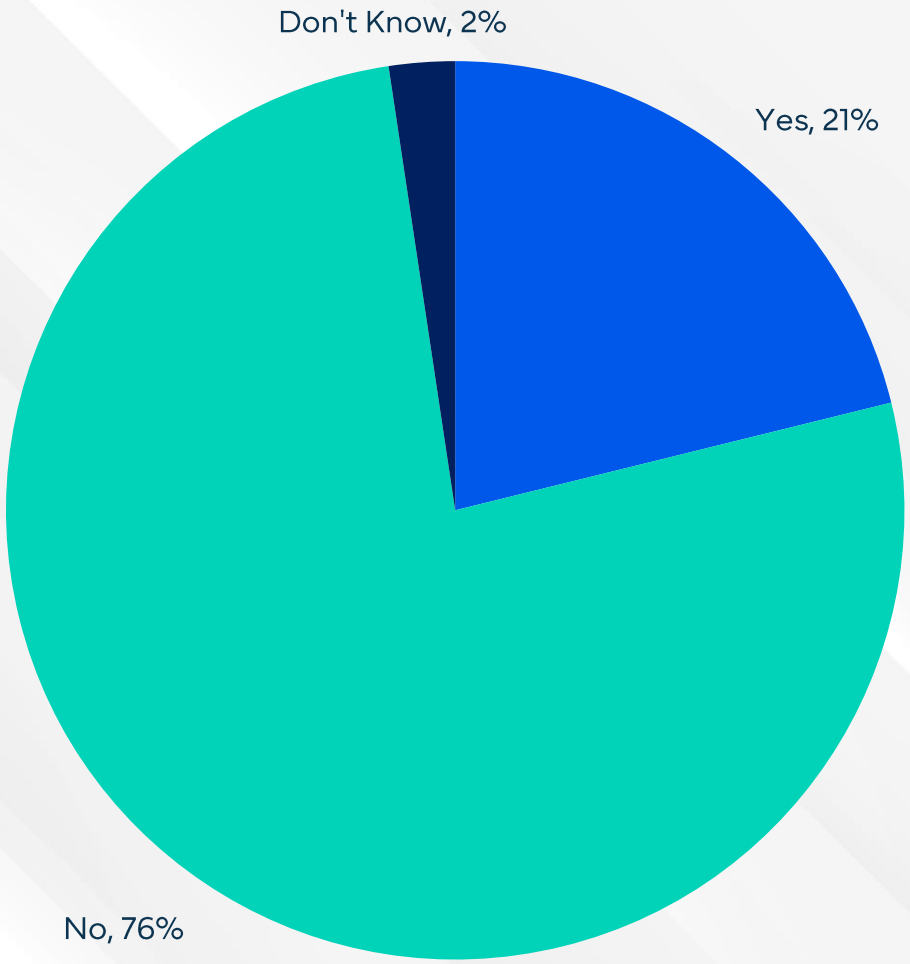
WhatsApp & Facebook are the most exploited platforms by scammers



Gmail, Instagram & Telegram round out the top five platforms where people encounter scams.

Q7 - Though which platform(s) did scammers contact you in the last 12 months?

76% of Hongkongers did not report the scam to law enforcement



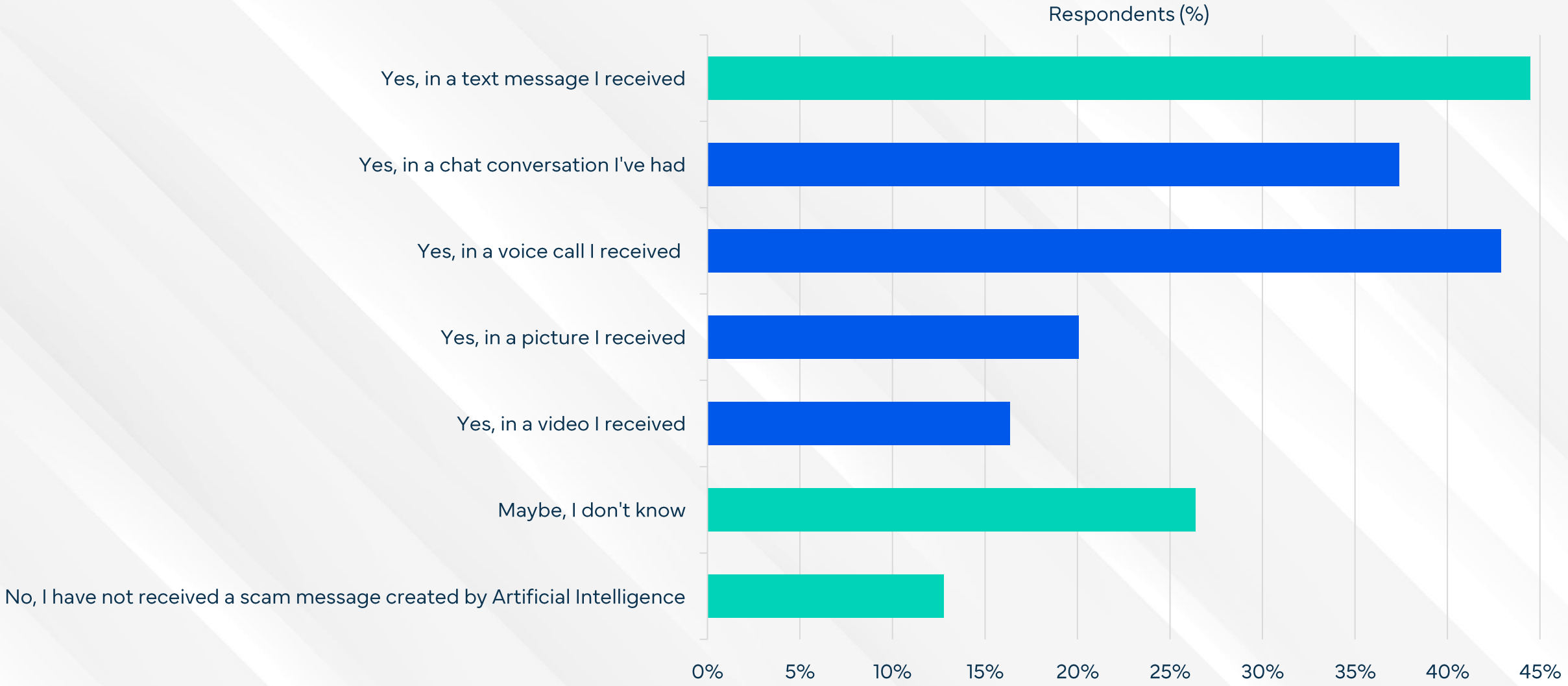
5%

Hongkongers not reporting scams to law enforcement

21% stated having reported the scam to law enforcement or another government authority.

Q8 - Did you report a scam or scam attempt to the police or authorities in the last 12 months?

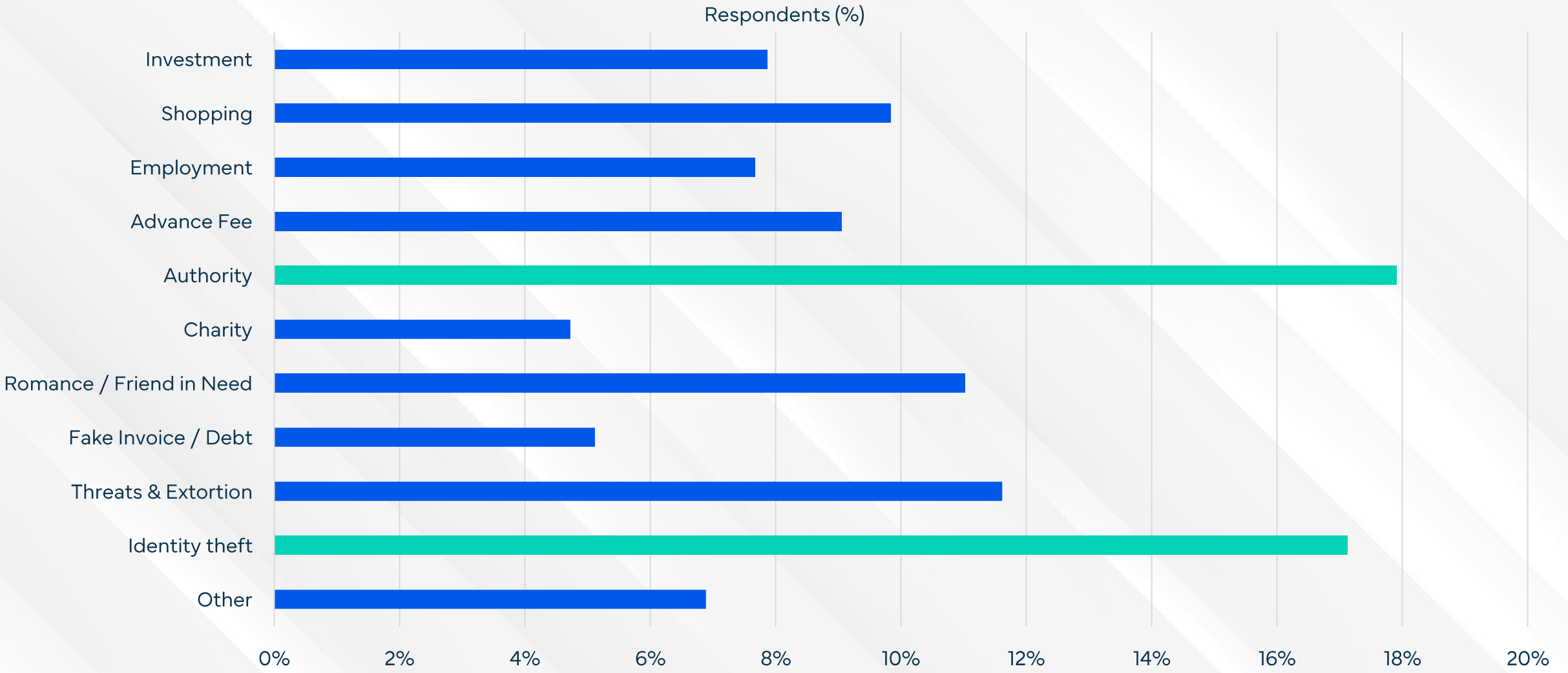
26% of Hongkongers were uncertain whether AI was used to scam them



13% of Hongkongers stated they did not believe they were subjected to scams utilizing AI.

Q9 - Do you think Artificial Intelligence (AI) was used in an attempt to scam you?

Authority scams is the most common type of scam in Hong Kong



58% did not fall victim to the most common scams in the last year. 1.09 scams were reported per victim.

Q10 - Which of the following negative experiences happened to you in the last 12 months?

Hong Kong scam victims share their stories

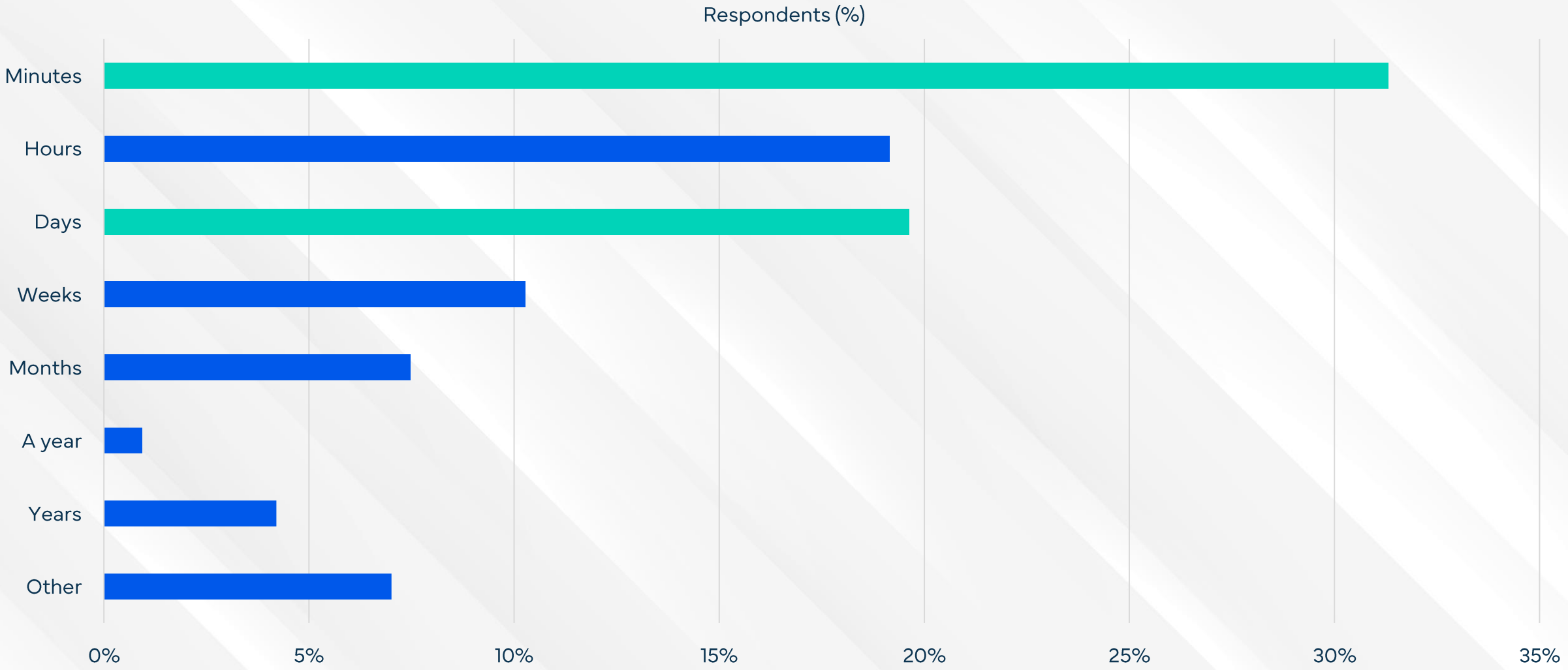
"I often receive phone calls and he (scammer) is a government official in mainland China. WhatsApp or text messages falsely claim that I have a fine to pay."

"The scammer called and told me that my husband was hospitalized due to illness and needed 20,000 life-saving help."

"Received a message from The Club saying the points earned were about to expire, and went inside the link to redeem gifts, only after entering credit card number did we realize it was a scam."

"I saw the product I was interested in on the Facebook advertising page and paid for it. However, I received the product with extremely poor quality and the wrong version. The seller also disappeared."

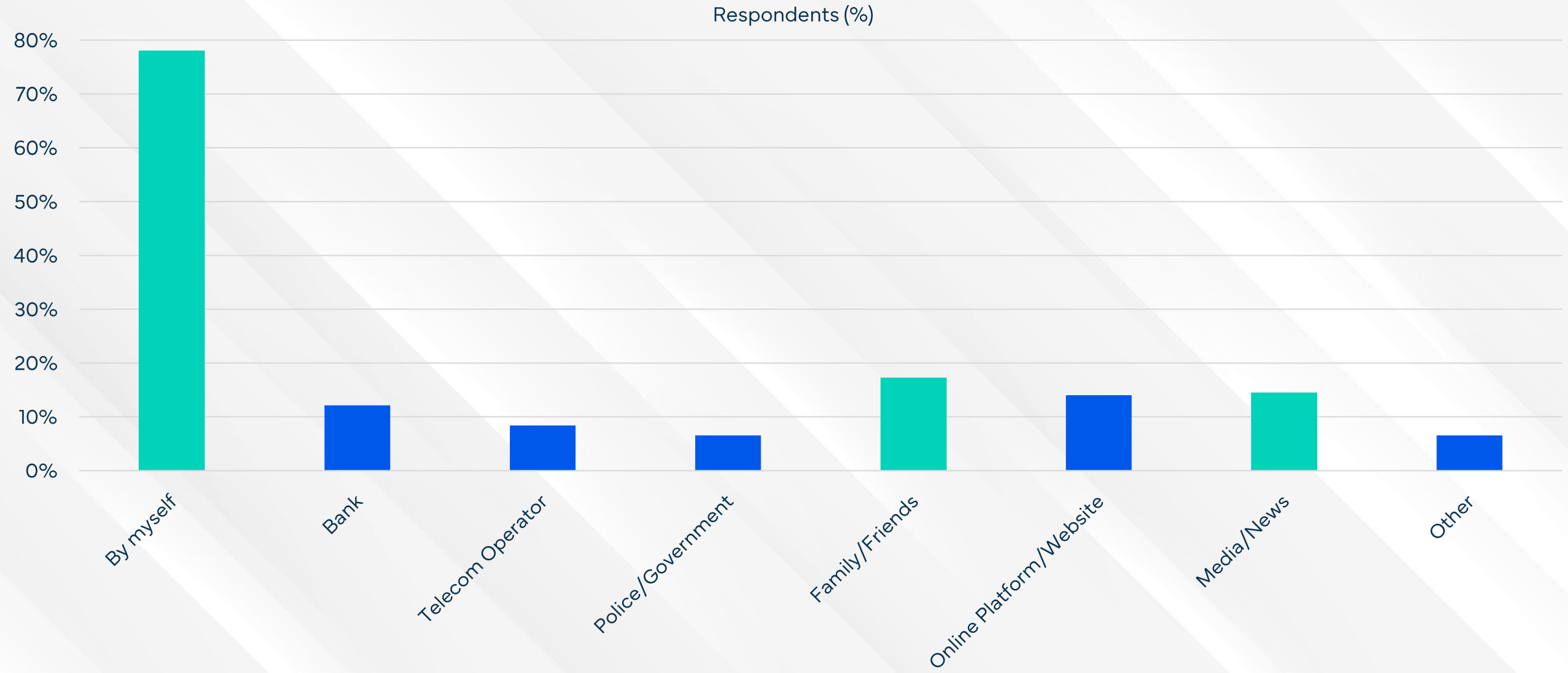
1-in-2 scams in Hong Kong are completed within 24 hours of first contact



31% reported scams that were over in minutes, while 5% were scammed over a year or more.

Q12 How long did the scam last, from the first time you heard from the scammer until the last payment you made or the last time you contacted them?

78% came to their own conclusion that they had been scammed



Others were informed by family/friends, while media/news are also popular in pointing out scams.

Q13 How did you discover you were scammed?

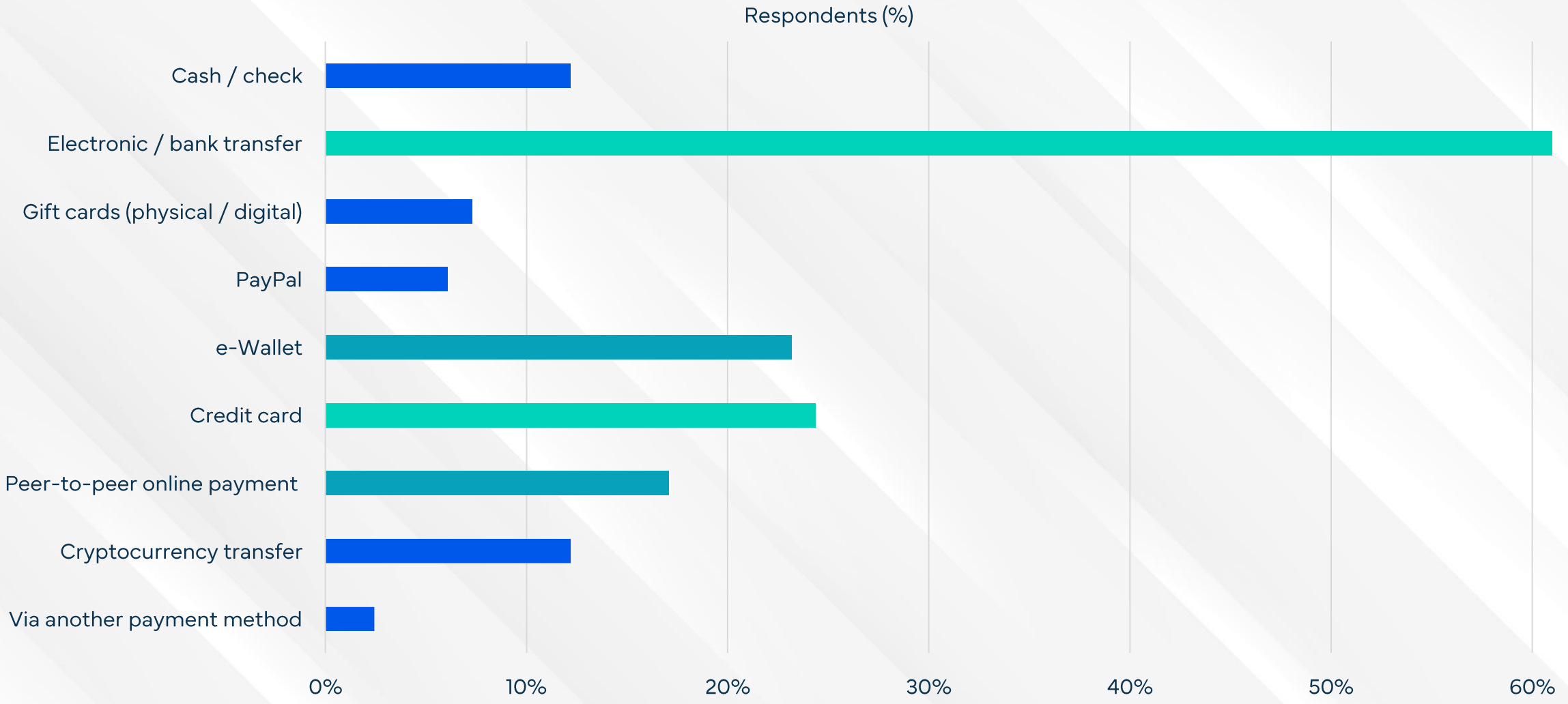
In total, 16% of Hong Kong's participants lost money in a scam

Survey Key Statistics	
Persons approached	511
Participants losing money	82
% losing money / survey participants	16%
Average amount lost in US Dollars	1,581
Total country population	7,297,821
Population over 18 years	6,174,196
# of people scammed > 18 years	990,771
Estimated total scam losses (USD)	1,566,409,233
Estimated total losses (HKD)	12,202,684,844
Gross Domestic Product (USD, millions)	385,546
% of GDP lost in scams	0.4%

In total, Hong Kong lost $1.5 billion to scams, which is equal to 0.4% of Hong Kong's GDP.

Q14 In the last 12 months, in total, how much money did you lose to scams before trying to recover the funds?

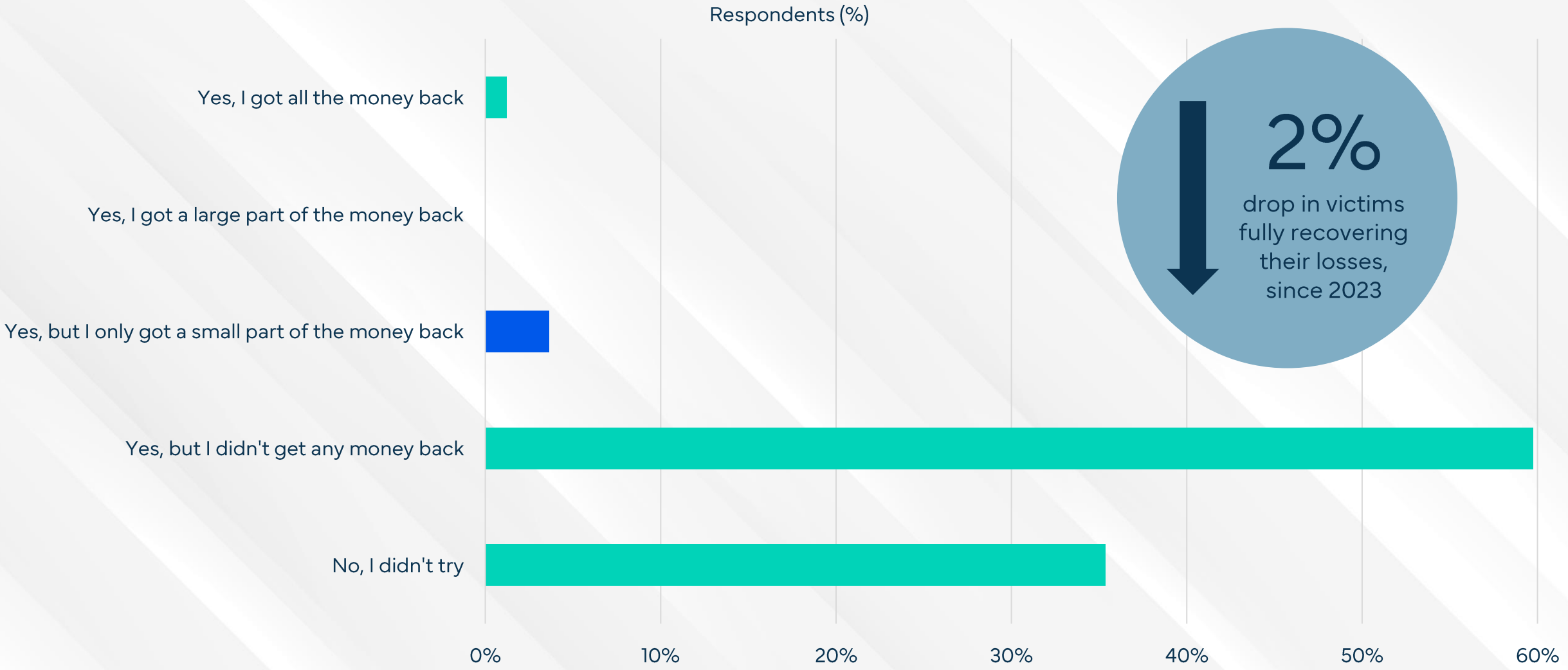
Bank Transfers & credit cards are the dominant payment methods



e-Wallet & peer-to-peer apps are also key tools which scammers use to receive their stolen gains.

Q15 - How did you pay the scammer?

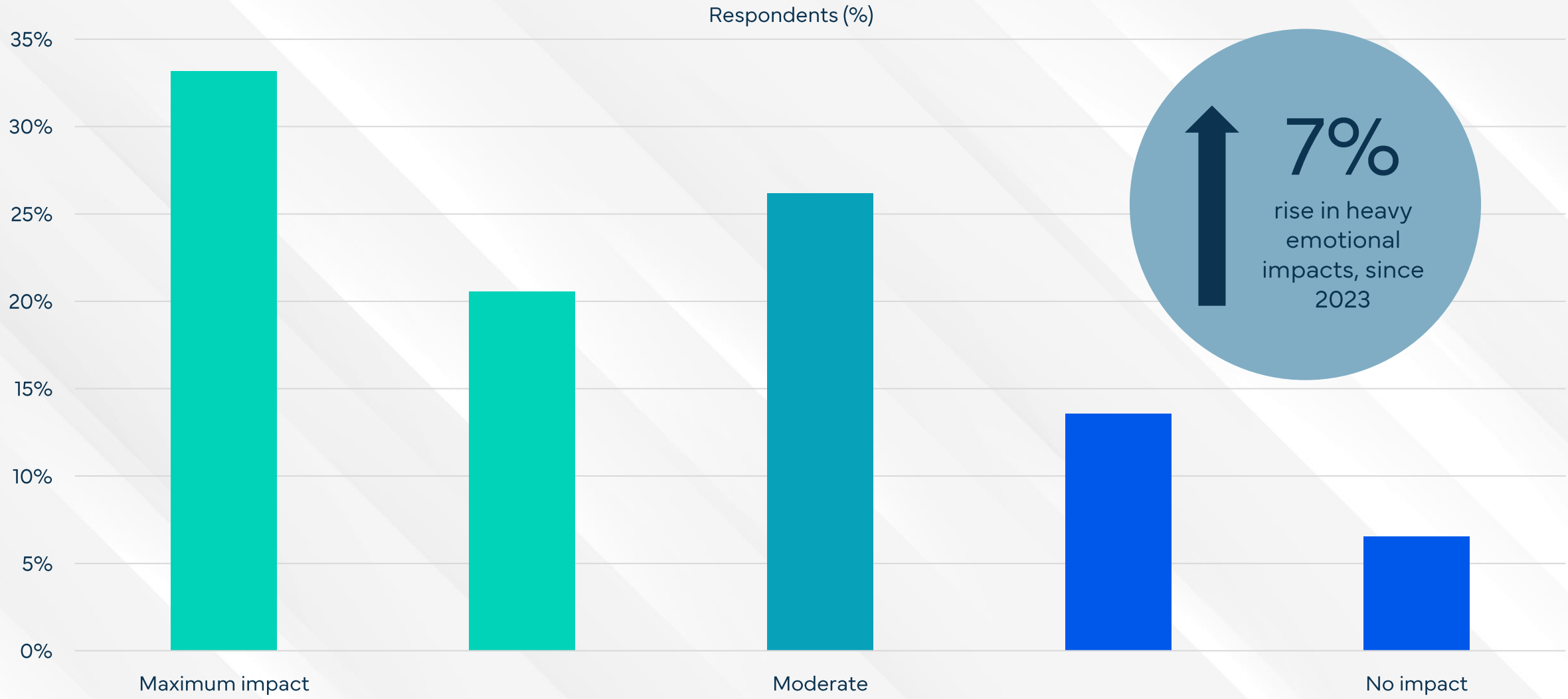
Only 1% of victims were able to fully recover their losses



35% did not try to recover their funds. 60% tried but were not able to recover any money.

Q16 - Did you try to recover the money lost?

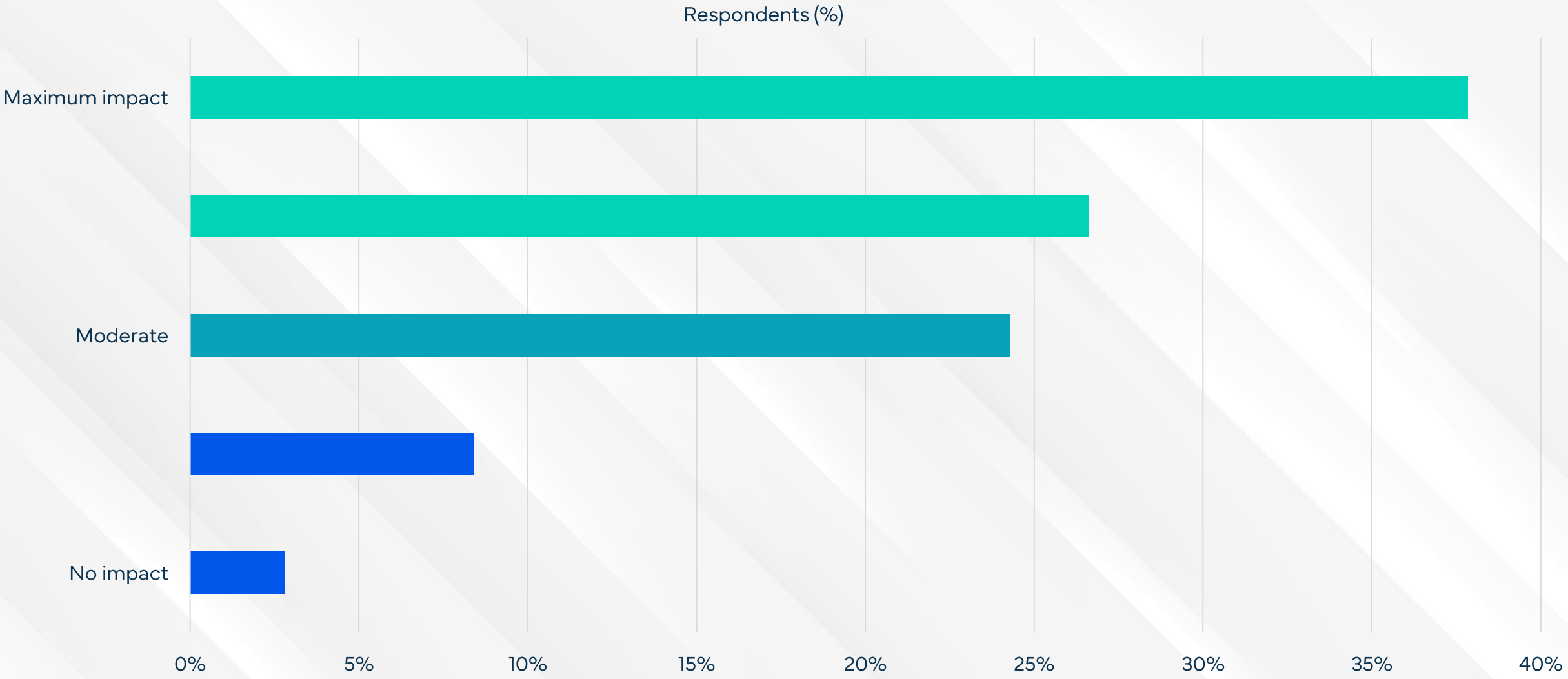
54% of the scam victims perceived a (very) strong emotional impact



20% of the survey respondents reported little to no emotional impact due to scams.

Q17 - To what extent did the scam(s) impact you emotionally?

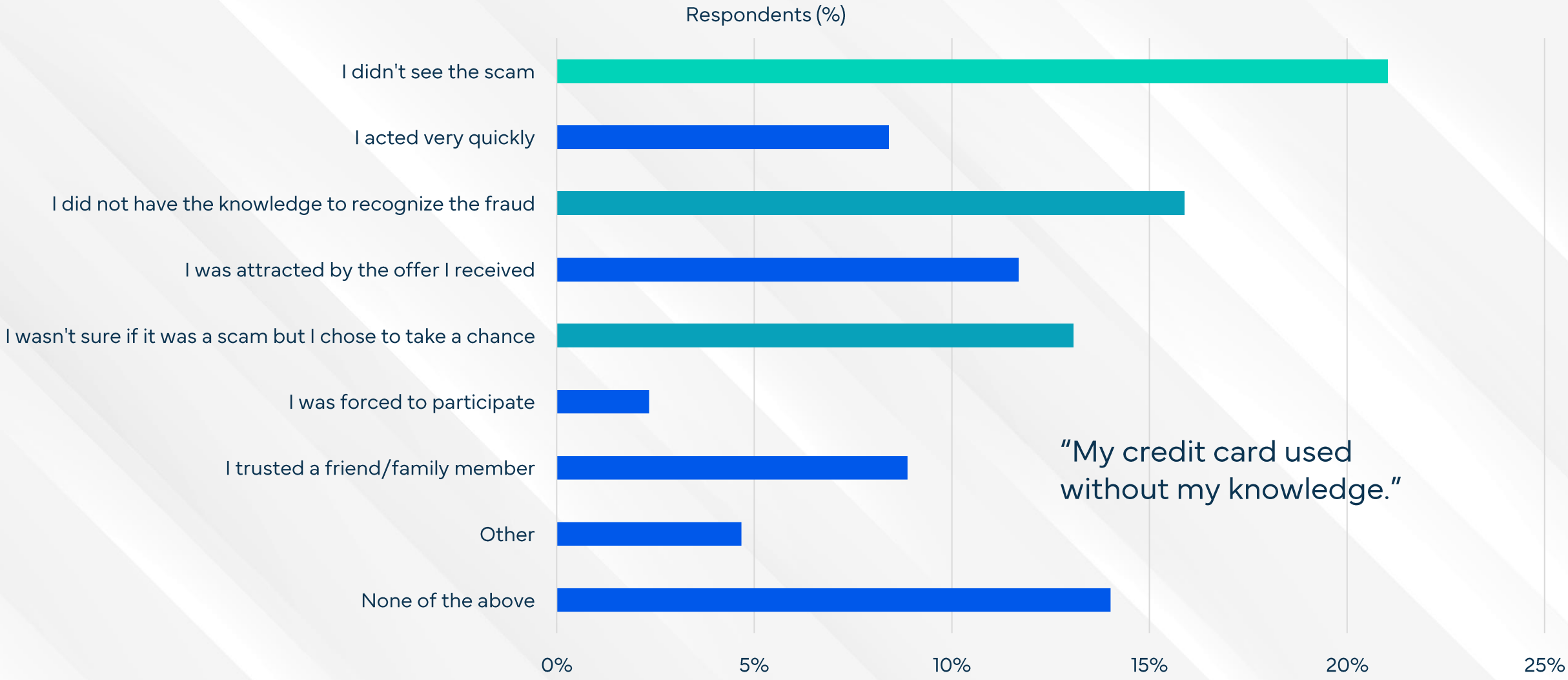
65% of Hongkongers have less trust in the Internet as a result of scams



Only 11% of Hongkonger reported little to no loss of trust in the Internet due to scams.

Q18 - To what extend do scams impact your trust in the Internet, in general?

Hongkonger fall for scams by failing to recognize the scam

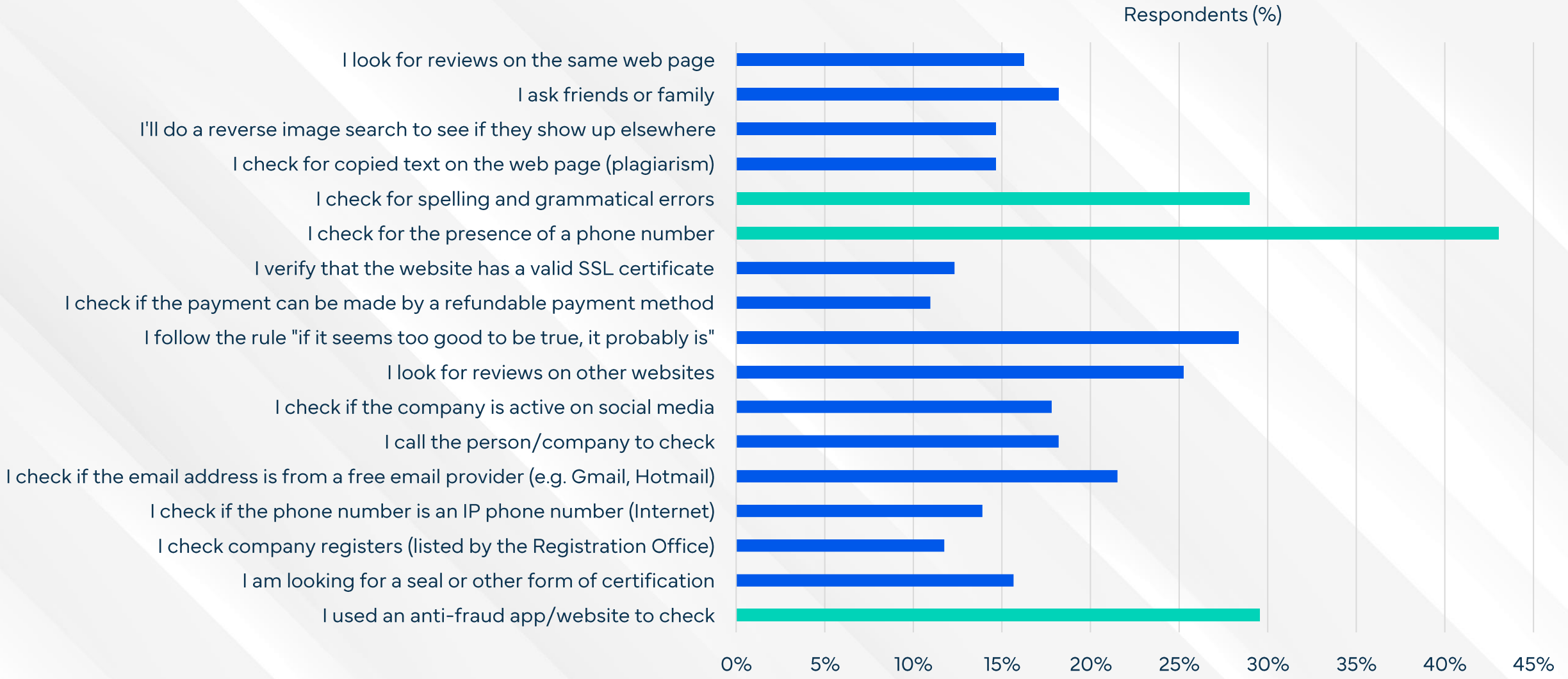


"My credit card used without my knowledge."

Several victims reported they did not grasp the scam while others weren't sure but choose to risk it.

Q19 - What was the main reason you were deceived?

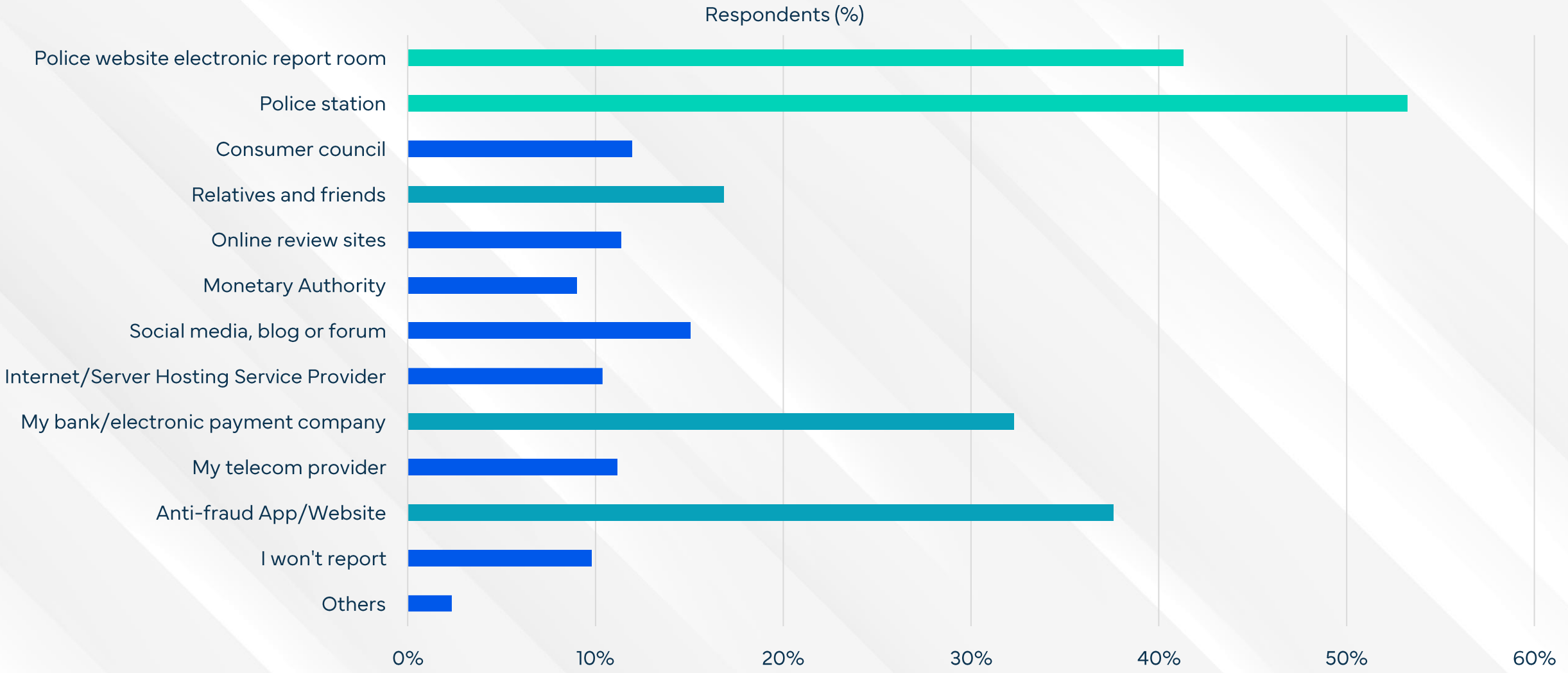
43% check for the presence of a phone number when checking for scams



Many reported using an anti-fraud app/site while others check spelling and grammatical errors.

Q20 - What steps do you take to check if an offer is real or a scam?

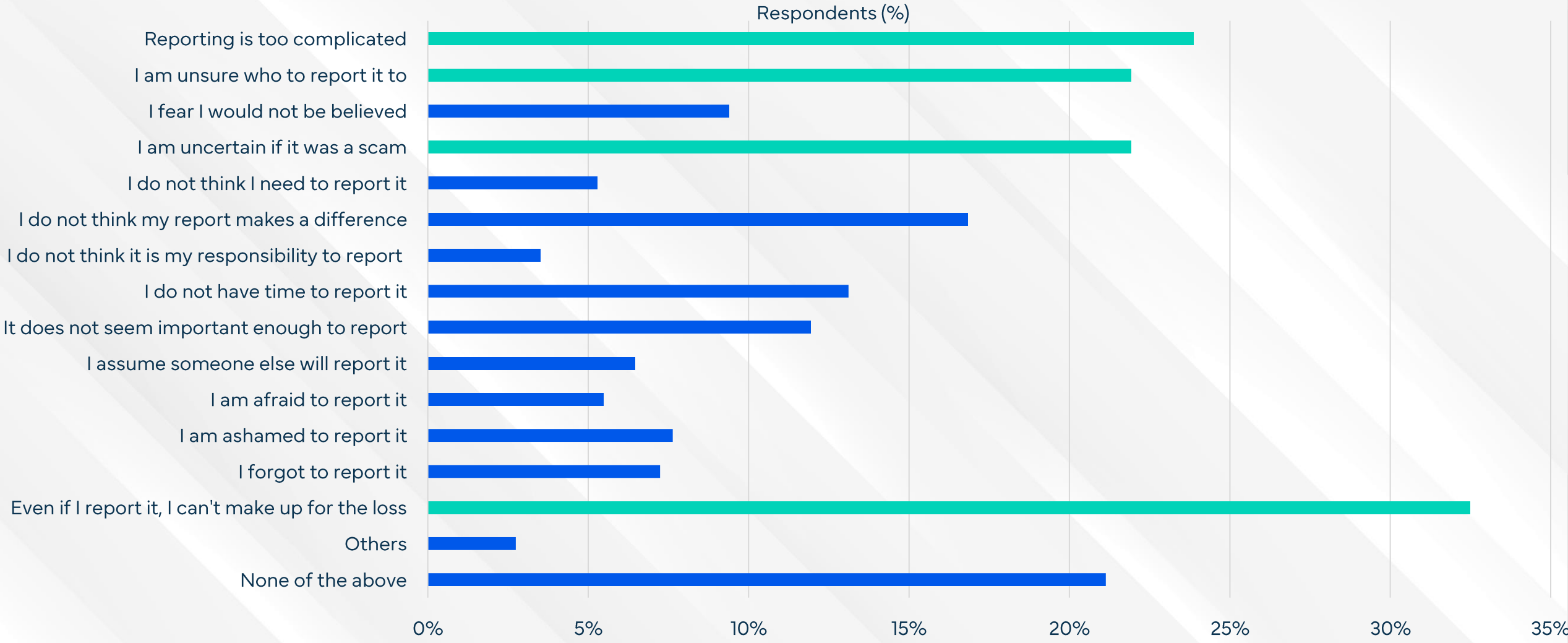
Scams are mostly shared with local police stations & police website



Anti-fraud app/site, banks, and friends/family are popular places to report scams.

Q21 - If you were to be deceived by a scam, who would you report this to?

Many Hongkongers think reporting scams won't get their money back



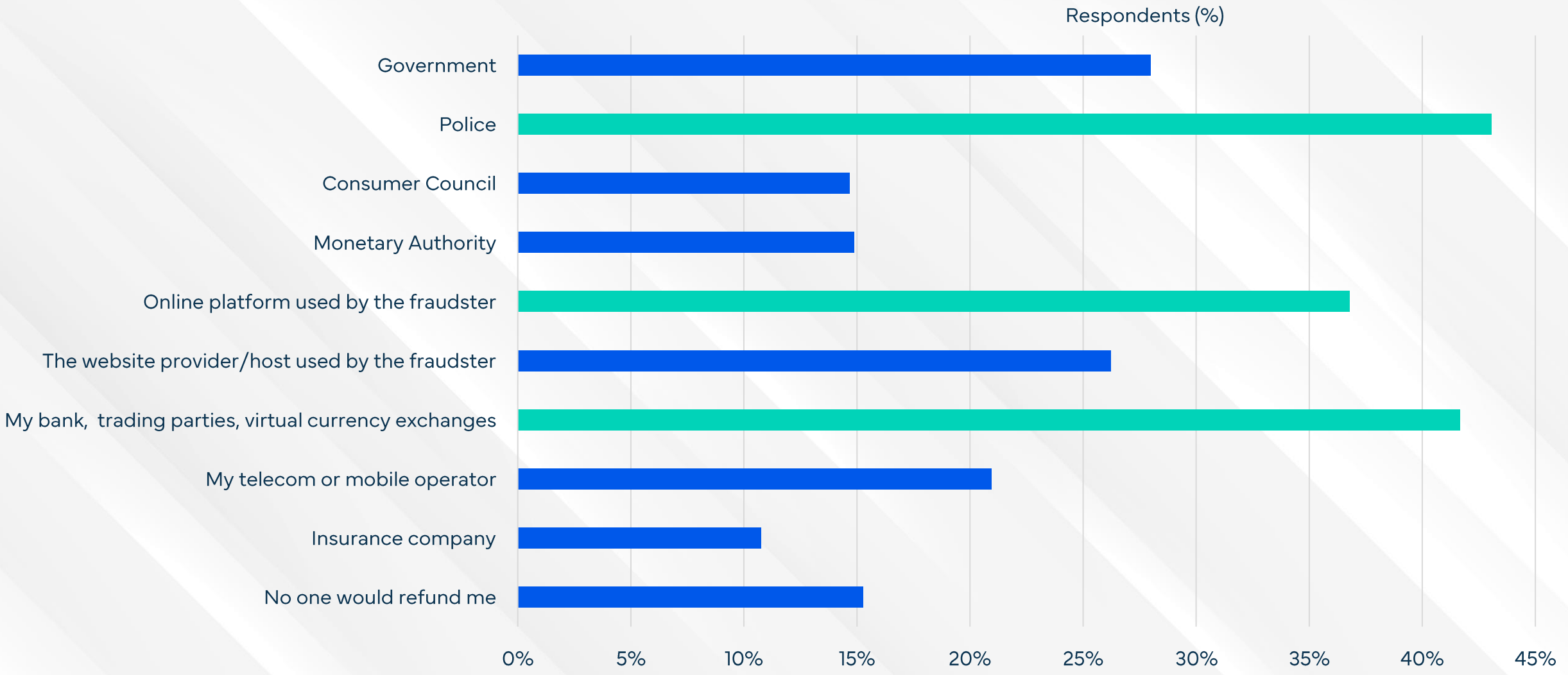
Other reasons for not reporting are complex reporting process & fearing no one will believe them.

Q22 - What reasons might you have to not report a scam?

15% of Hongkongers assume no one will refund their scam losses

SCAMADVISER whoscall

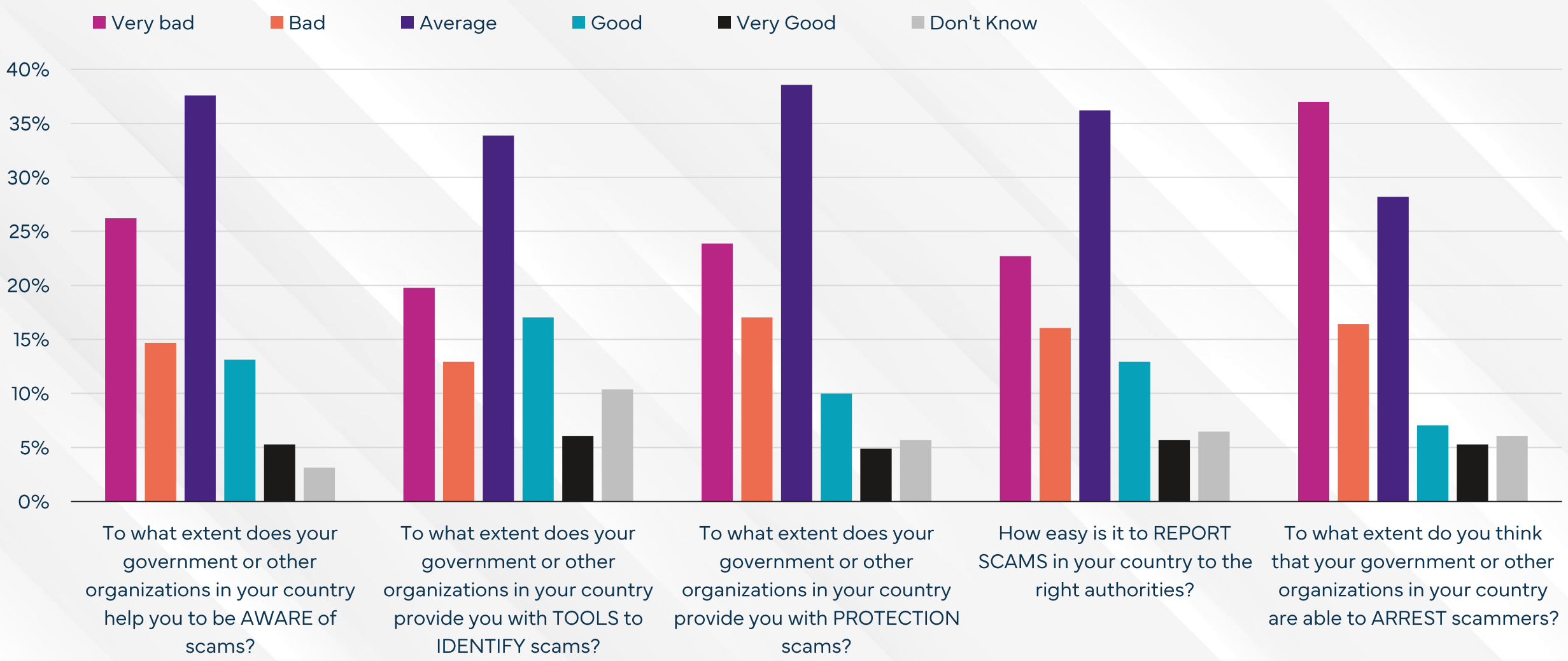
GASA Global Anti-Scam Alliance



Others deem their police, banks/virtual currency exchanges, and online platform used will refund them.

Q23 - If you were scammed, who do you think should be responsible for making sure you are paid back for your loss?

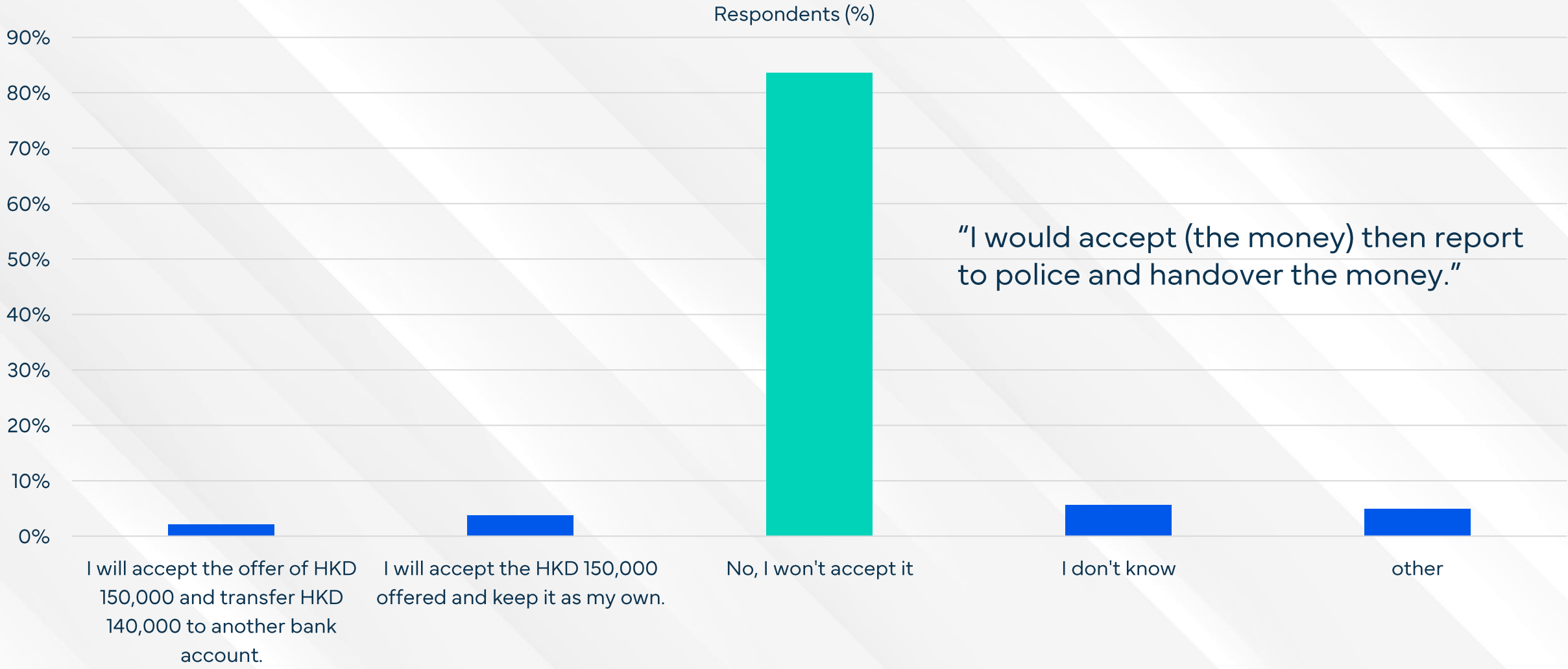
Citizens are unhappy with Hong Kong's attempts to arrest scammers



Overall, 41% of the participants rate the actions of the government as (very) bad, 17% as (very) good.

Q24 - Think about how well the government and other groups in your country are doing in the fight against online scams. How do you rate their efforts in the following categories?

2% of Hongkongers admit that they would consider being a money mule



"I would accept (the money) then report to police and handover the money."

However, 84% of those surveyed would refuse to be involved in a "money mule" scam.

Q25 - If someone offers you US$ 20,000 on the condition that you send US$ 19,000 to another bank account, leaving you with US$ 1,000 to keep, what would you do?

SCAMADVISER

whoscall

About This Report

GASA

Global Anti-Scam Alliance

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, and 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.

Whoscall, powered by **Gogolook**, is a cutting-edge digital anti-scam tool designed to protect users from scams across various channels, including phone calls, text messages, and links. With over 100 million downloads globally, it features the most comprehensive database in East and Southeast Asia, covering more than 2.6 billion phone numbers.

ScamAdviser is a global leader in scam prevention, committed to empowering businesses with its AI-powered Anti-Scam Intelligence (ASI). Our platform delivers real-time detection of suspicious activities, protecting websites, phone calls, messages, and online platforms from potential scams. With the world's largest scam database, we share insights with 400+ partners, collectively protecting more than 1 billion consumers worldwide.

About the authors

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

Nowadays, Jorij is a Professor at TIO University and Managing Director of the Global Anti-Scam Alliance (GASA) & ScamAdviser.

Clement Njoki is Editor and Researcher at GASA. His role involves creating engaging content about scams and fraud, simplifying complex financial information for various platforms. He also works on building GASA's online presence through blogs and news updates.

Clement possesses comprehensive expertise in identifying and combating deceptive practices and fraud, along with a strong background in cybersecurity.

Sam Rogers is GASA's Director of Marketing. Previously, he worked in Risk Advisory, before transitioning into a career as a researcher, copywriter, and content manager specialized in cutting-edge electrical engineering topics, such as photonics and the industrial applications of electromagnetic radiation.

Sam left the world of corporate industry seeking a role which would allow him to concentrate on networking and events management, while allowing him to contribute something worthwhile to society.

James Greening, operating under a pseudonym, brings a wealth of experience to his role as a scam investigator, content writer, and social media manager. Formerly the sole driving force behind Fake Website Buster, James leverages his expertise to raise awareness about online scams. He currently serves as a Content Writer and Social Media Manager for the Global Anti-Scam Alliance (GASA) and regularly contributes to ScamAdviser.com.

Join the Network to Beat a Network

SCAMADVISER whoscall GASA Global Anti-Scam Alliance

INTELLIGENCE SHARING
Regular Virtual Meet-ups
8 Topic-based Email Groups
10,000 Professionals Newsletter

RESEARCH
Global State of Scams
30+ Regional Reports
Policy Papers

NETWORKING
3 International Summits
Online Member Directory
National GASA Chapters

CYBERCRIME EXCHANGE
80+ Pooled Data Sources
Realtime Data Sharing
Access to Global Leaderboards

OUR FOUNDATION PARTNERS

amazon
Bitdefender
CapitalOne
feedzai
Gogolook
Google
SCAMADVISER
Meta
TREND MICRO
Match Group

Become a member, see all member benefits at: gasa.org/membership

SCAMADVISER

whoscall

Disclaimer

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

Copyright

Global Anti-Scam Alliance (GASA)
Oder 20 - UNIT A6311
2491 DC The Hague
The Netherlands

Email: partner@gasa.org
X (Twitter): @ScamAlliance
LinkedIn: linkedin.com/company/global-anti-scam-alliance

GASA
Global Anti-Scam Alliance