

STATE OF SCAMS REPORT 2026



BRAZIL



One in four Brazilian adults that interacted with a scam lost money



Jorij Abraham

MANAGING DIRECTOR



Renata Salvini

CHAPTER DIRECTOR BRAZIL

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.

Summary

Normalization of scam exposure

Scam exposure is widespread and persistent, with 81% of Brazilian adults encountering scams—often on a daily basis, averaging over 200 attempts per person annually. Despite this intensity, concern remained stable year-on-year (67% in both 2025 and 2026), pointing to a normalization of risk rather than improved resilience.

Confidence varies — and engagement is high as detection lags behind

Only around two in five adults feel confident recognizing scams. More than half of those encountering scams go on to interact, and one in four of these interactions leads to financial loss—indicating persistent gaps between perceived and actual ability to detect threats. Consumers say they rely on simple cues such as spotting suspicious messages or “too good to be true” offers to avoid scams. At the same time, fewer victims are identifying scams independently, suggesting detection strategies are struggling to keep pace with increasingly convincing fraud.

Financial losses are widespread and repeat victimization persists

10% report losing money, total losses are significant—estimated at over R\$21 billion annually, with average losses exceeding R\$1,200 per victim. Repeat victimization remains a concern, with one in three victims losing money more than once within a year, highlighting ongoing susceptibility to re-targeting. Scammers continue to exploit everyday channels as payments are frequently made through standard methods (including instant payments, bank transfers, and cards) underscoring vulnerabilities in widely used financial systems.

Emotional impact remains high

Beyond financial loss, 76% of victims report an impact on mental wellbeing. Effects include reduced confidence, increased anxiety, and greater distrust of digital platforms.

Reporting shows limited outcomes

Reporting is dispersed across banks, platforms, authorities, and personal networks. When reported, only one in five victims recover funds and one in three victims say the organization they reported to did not take any action. The responsibility to protect the public against scams is in first place assigned to online platforms and government, who rank comparatively lower on perceived performance. Police performance is viewed as most closely aligned with expectations, suggesting more consistent delivery. Banks, meanwhile, stand out for providing practical support—particularly in reporting processes, payment blocking, and consumer education.

Building a National Response to Online Scams

In recent months, there has been a rise in digital scams that misuse government and corporate logos, as well as doctored images of both public officials and celebrities, including through the use of artificial intelligence. By misleading the public, these scams involve data theft and result in financial and emotional harm.

At federal level, the Attorney General's Office (AGU), together with the Secretariat for Social Communication (SECOM/PR) and partners, has adopted a strategy to tackle the issue across its technological, infrastructural, legal and financial dimensions.

These bodies have been working with internet service providers to curb misleading advertising relating to public policy, illegal posts and the hosting of fraudulent websites. This includes agreements with the private sector to improve ad verification mechanisms. The AGU has also been working collaboratively to prevent scams linked to high-profile events – such as income tax returns, public sector recruitment exams and debt refinancing.

The Central Bank (BC) has improved the Special Refund Mechanism, expanding the scope for refunds to victims and the precautionary blocking of suspicious PIX keys. Another important initiative was the partnership between the Ministry of Justice (MJSP) and the Brazilian Federation of Banks (FEBRABAN) to prevent and combat cybercrime. The Federal Police (PF) has also stepped up operations against electronic fraud and associated money laundering.

Following the Federal Supreme Court's (STF) update to the liability regime under the Civil Rights Framework for the Internet, advancing digital literacy – particularly amongst vulnerable groups – and stepping up cooperation and transparency efforts remain challenges on the horizon.



Raphael Ramos Monteiro De Souza
**NATIONAL ATTORNEY OF THE UNION
FOR THE DEFENSE OF DEMOCRACY - A
UNIT WITHIN THE BRAZILIAN
ATTORNEY GENERAL'S OFFICE**



About AGU

The Federal Attorney-General's Office (AGU) is the institution responsible for the judicial and extrajudicial representation of the Brazilian State, operating primarily in the civil and administrative spheres. Among its missions is the protection of the integrity of information relating to federal public policies, which are directly affected by the growing wave of fraud and scams in the digital environment.



Priscila Couto
PROGRAM LEAD, TRUST & SAFETY
GOOGLE LATIN AMERICA



About Google Trust & Safety

Google's Trust & Safety division is dedicated to making the digital advertising ecosystem secure. By combining advanced artificial intelligence, global policy enforcement, and multi-sector strategic alliances, we protect users, advertisers, and publishers from emerging threats around the clock.

Stopping Harmful Ads at the Gate

THE SHIFT TO PROACTIVE PROTECTION. In the fight against sophisticated online fraud, speed is paramount. Traditionally, ads safety systems operated reactively—removing malicious creatives post-exposure. Google is shifting the paradigm. By embedding our most advanced AI model, Gemini, we now intercept highly elusive threats during the ad-submission pipeline, neutralising scams before they reach user devices.

UNLOCKING THE POWER OF GENERATIVE AI. Bad actors continually refine their evasive tactics, leveraging automation and AI to spin up realistic brand impersonations and deep fakes. Gemini counters this by analyzing complex context and semantic nuance. Unlike traditional rule-based models, Gemini interprets the subtle relationships between ad copy, visual assets, metadata, and landing pages to detect patterns that suggest deceptive intent.

STOPPING BAD ADS BEFORE THEY ARE SERVED. Gemini operates directly within Google's pre-review pipeline. When an ad is submitted, the model completes real-time audits instantly. If violations are flagged, the ad is terminated immediately. This proactive intervention ensures that malicious creatives are never served to users, dramatically reducing regional exposure to financial fraud and preserving public trust in the digital ecosystem.

CONTINUOUS POLICY INNOVATION & VERIFICATION. No technology works in isolation. Google pairs Gemini enforcement with continuous policy updates and robust operational barriers. We require global advertisers to pass rigorous identity and location verification checks. Increasing the administrative and operational cost for bad actors actively disrupts the financial viability of massive, automated scam networks.

A SHARED MISSION: COLLABORATION AT SCALE. Because online fraud crosses regulatory and industry borders, systemic security requires deep, cross-sector partnership. Google's work with the Global Anti-Scam Alliance (GASA) and our founding role in the Global Signal Exchange (GSE) are central to this. Sharing real-time threat intelligence ensures that as defense models scale, they create a stronger, unified shield for users everywhere.



Raphael Mielle
DIRECTOR OF SERVICES AND
SECURITY



About Febraban

Founded in 1967, Febraban is a non-profit association that engages with all segments of society with the purpose of contributing to the country's economic, social, and sustainable development. Febraban believes that a truly strong financial system is built by financially strong companies and individuals. The Federation's mission is to represent its members before all branches of government — the Executive, Legislative, and Judiciary branches — as well as representative organizations of society, working to improve the regulatory framework, continuously enhance services, and reduce risk levels. It also seeks to promote initiatives that expand the population's access to financial products and services. Febraban brings together 114 members, including 108 financial institutions and six representative associations at the national or regional level, representing financial institutions or companies engaged in activities related or complementary to the banking sector.

The Brazilian Banking System at the Forefront

At the Forefront of Brazil's Banking System

Brazil is a global benchmark in banking technology and has developed solutions that have expanded access to the financial system for millions of Brazilians. This progress is supported by annual investments of R\$50 billion in technology, with 10% allocated to cybersecurity. The banking sector also provides a robust protection framework, enabling customers to carry out their everyday banking transactions with convenience and confidence.

New Scams, Old Strategies

In this scenario, criminals target end customers and use social engineering techniques to trick users into revealing passwords and personal information. They also continuously recycle old fraud schemes, such as fake call centers, phishing attacks, and fraudulent sales.

Awareness campaigns

Information is one of the most effective forms of protection. That is why Febraban and financial institutions continuously invest in awareness and education campaigns, with initiatives across television, radio, and social media.

Partnerships

Banks also work in partnership with law enforcement agencies to identify and hold cybercriminals accountable, including through initiatives such as Project *Tentáculos*. Launched in 2007, the project consolidates fraud-related criminal reports into a single repository. Today, 71 financial institutions participate in the initiative, and between 2018 and 2025, approximately 678 operations were carried out, resulting in 1,741 search and seizure warrants executed and 311 arrests.

Febraban is also a partner in *Celular Seguro*, launched in 2023 by the Ministry of Justice and Public Security, and participates in the National Anti-Fraud Alliance Plan, which brings together more than 20 initiatives aimed at a broad and coordinated approach to prevention, consumer education, detection, rapid response, enforcement, and asset recovery.

**SUZANA RODRIGUES**

SUPERINTENDENT OF REGULATORY COMPLIANCE AT THE BRAZILIAN NATIONAL TELECOMMUNICATIONS AGENCY (ANATEL). COORDINATOR OF ANATEL'S TECHNICAL WORKING GROUP ON CYBERSECURITY AND CRITICAL INFRASTRUCTURE RISK MANAGEMENT (GT-CIBER).

About Company

Established in 1997, the Brazilian National Telecommunications Agency (Anatel) is the federal regulatory authority affiliated with the Ministry of Communications. Its mission is to regulate Brazil's telecommunications sector by ensuring the quality of telecommunications services, protecting consumers' rights, and promoting fair competition among service providers. Anatel is responsible for regulating, overseeing, and setting standards for telecommunications services throughout Brazil. Its regulatory scope includes landline and mobile services, internet access, and pay television, ensuring that these services are provided with quality, efficiency, and in full compliance with applicable laws and regulations.

The Role of Telecommunications in Preventing Digital Scams

The expansion of mobile broadband, increased connectivity and the accelerating digitalisation of the Brazilian population – particularly in the wake of the pandemic – have brought significant benefits to society and the economy. At the same time, this progress has also provided greater scope for scammers, who have begun to exploit social engineering techniques, the misuse of data and the creation of fake profiles on messaging apps to deceive users and gain illicit advantages.

Although digital fraud occurs in various contexts, the telecommunications sector plays an important role in preventing and mitigating such scams, as communication services can be used to lend credibility to criminal schemes. One example is spoofing, a practice whereby the caller ID of a telephone call is falsified to make the victim believe they are speaking to a legitimate organization.

Anatel has been implementing regulatory and operational measures to tackle this problem. Of particular note are the directives aimed at combating spoofing and the provisions of the General Regulations on Telecommunications Services (Resolution No. 777/2025), which make the authentication of telephone calls mandatory.

However, this challenge requires coordinated action between telecoms providers, financial institutions, digital platforms, public security agencies and other stakeholders. It is also vital to raise public awareness of the main types of scams and how to prevent them. A combination of regulation, institutional cooperation, technological innovation and digital education is essential to strengthen communications security and boost citizens' confidence in the digital environment.

Brazil's Fraud Inflection Point: Why the Financial System Must Move at the Speed of Pix

Brazil's instant payment rail, Pix, has reshaped how money moves, delivering significant benefits to the Brazilian economy. However, bad actors have also found ways to exploit its role as a powerful connective tissue across the financial ecosystem. According to the 2026 Global Anti-Scam Alliance (GASA) State of Scams report, an estimated 16.5 million Brazilians lost money to scams in the past year, with total losses approaching R\$21.2 billion. One in four victims lost that money within minutes. The speed that makes Pix valuable to consumers makes it equally valuable to fraudsters.

Consumer trust is on the line.

One in two Brazilian scam victims reported becoming more distrustful of digital platforms afterward, highlighting a systemic risk for a country whose financial inclusion strategy depends on digital adoption. The public mandate is unambiguous: 80% of Brazilians support giving banks authority to block suspicious transactions proactively.

Speed demands intelligence at the point of transaction.

Any detection model operating on a batch or end-of-day cycle is structurally irrelevant when settlement is instant. We need to address this with sub-second, real-time risk scoring and the ability to identify counterparty risks across the entire network. This allows for a risk signal to be delivered before a payment clears, at the moment intervention is still possible.

The solution is inherently collaborative.

Fraudsters operate across institutional boundaries; defenses must too. This is where the collaborative solutions, such as a consortium data model, allow for the aggregation of anonymized risk intelligence across financial institutions. This surfaces mule account data and adverse incident signals that no single bank could detect alone. That type of shared intelligence transforms fraud defense from isolated institutional reaction into a coordinated early warning system. Brazil is not an outlier. Every market deploying instant payments faces this same inflection point. The infrastructure to respond exists. The urgency is now.



Mauriceo Castanheiro
**VP AND HEAD OF INTERNATIONAL
PAYMENTS FRAUD**



About Nasdaq Verafin

Nasdaq Verafin provides Financial Crime Management Technology solutions for Fraud Detection and Management, AML/CFT Compliance and Management, High Risk Customer Management, Sanctions Screening and Management, and Information Sharing. More than 2,800 financial institutions, representing \$12 trillion in collective assets, use Nasdaq Verafin to prevent fraud and strengthen AML/CFT efforts.



Guilherme Favaro
**SENIOR HEAD OF FRAUD
PREVENTION**



About Santander

Santander is a commercial bank founded in 1857 and headquartered in Spain. It is one of the world's largest banks by market capitalization. The Group's operations are organized into five global business divisions: Retail & Commercial Banking, Digital Consumer Bank, Corporate & Investment Banking, Wealth Management & Insurance, and Payments (including cards, payment solutions, and the PagoNxt holding company). This operating model enables the Group to maximize the benefits of its unique combination of global scale and local leadership. Santander's ambition is to be the best open financial services platform for individuals, small, medium-sized and large businesses, institutions, and governments. As of the end of 2025, the Santander Group had total assets of €1.4 trillion, served 180 million customers, operated approximately 7,100 branches, and employed 198,000 people worldwide. Present in the Brazilian market since 1982, Santander is the country's largest financial group with a retail banking presence, serving more than 75 million customers.

Technology, Intelligence, and Collaboration in the Fight Against Digital Scams

Over the past year, we have observed a significant evolution in Brazil's scam landscape, particularly with the growing use of artificial intelligence to create more convincing messages, voices, and social engineering tactics. There has also been an increase in scams that exploit consumers' trust in digital channels, including fake customer support schemes, social engineering linked to instant payment transactions, and fraud that leverages publicly available data to personalize fraudulent communications.

Brazil's response has become increasingly coordinated. In the context of Pix (National Instant Payment System), financial institutions and technology companies have increased information sharing on emerging threats, enabling faster identification of fraud patterns and more effective blocking of suspicious activities. At the same time, public awareness campaigns have reinforced the importance of identity verification, exercising caution when faced with urgent requests, and protecting digital credentials.

On the technology front, we have seen greater adoption of artificial intelligence-based solutions to detect anomalous behavior, account takeover attempts, and potentially fraudulent transactions in real time. Regulatory initiatives and institutional cooperation mechanisms have also continued to evolve, strengthening both fraud prevention and incident response.

One of the key lessons is that effective scam prevention increasingly depends on the combination of technology, consumer education, and cross-sector collaboration. The greatest challenge remains the speed at which fraudsters adapt, making continuous monitoring, intelligence sharing, and ongoing innovation essential.



Rodrigo Henriquez
CHIEF INNOVATION AND
STRATEGY OFFICER

FENASBAC
I N O V A Ç Ã O

About Fenاسبac

The National Federation of Central Bank Employees' Associations (Fenasbac) has a legacy spanning more than five decades. Originally established to provide financial services to employees of Brazil's Central Bank, the organization has expanded its role and is now recognized as the country's leading catalyst, connector, and driving force for financial innovation. As an ecosystem accelerator, Fenاسبac plays a strategic role in fostering ongoing dialogue among emerging technologies, new business models, and the evolution of the regulatory framework, helping to build a financial system that is more dynamic, modern, competitive, inclusive, and fair. We drive the transformation of the financial and capital markets by delivering Open Innovation Programs, industry events, and consulting solutions. We work in close and continuous collaboration with the leading regulatory authorities of Brazil's National Financial System to identify and promote initiatives that generate value for society. This is the purpose that unites and drives us.

Innovation, Regulation, and Collaboration for a More Resilient Financial Ecosystem

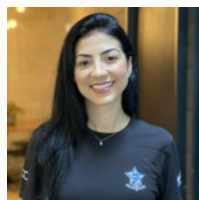
The rise and negative impact of financial scams and fraud across all countries of the world – and Brazil is no exception – will only be addressed if we are able to establish close coordination between regulators, financial institutions, telecommunications companies, big tech firms and social media platforms. Either the ecosystem operates in an integrated, multi-sectoral manner on a global scale, or we are doomed to lose a significant portion of the global economy to fraudsters and scammers.

The good news is that this path is being forged by a range of stakeholders. Thanks to its history of hyperinflation and significant investment in technology, Brazil has developed one of the most sophisticated financial systems in the world. With proactive regulators willing to operate at the cutting edge of innovation, the model has become an international benchmark, demonstrating how technology removes barriers to financial inclusion whilst at the same time building defenses against fraud and scams.

We operate within this ecosystem as a catalyst and facilitator, bridging the gap between the market, academia and regulators. By bringing these sectors together, we translate the real-world challenges facing the financial system into viable proposals, fostering testing and prototyping environments to trial technologies that mitigate the harmful effects of fraud, particularly amongst the most vulnerable sections of society.

If crime operates as a network, our only real defense is to fight fire with fire. What sets the Brazilian model apart is how it operates and with whom. Over the last decade, the creation of innovation hubs such as LIFT Lab (Central Bank) and LEAP (CMV), where Fenاسبac, regulators and innovators work side by side to develop innovative solutions that take into account and tackle the issue of fraud and scams, has been fundamental to the responses provided to society.

The survival and long-term success of this new digital society depend on moving beyond isolated initiatives and fostering global ecosystems of collaboration, where experimentation and the sharing of practical intelligence form the foundation of a truly resilient system capable of addressing this urgent challenge.



Luana Tavares
CEO & Founder



About INCC

The National Institute for Combating Cybercrime (INCC) is a civil society organization dedicated to strengthening cybersecurity, preventing cybercrime, and enhancing digital resilience. It brings together government, the private sector, academia, and civil society to foster a safer, more resilient, and more trustworthy digital ecosystem.

Sources: Brazilian Federal Senate (Bill No. 4,752/2025, approved by the Constitution and Justice Committee (CJI) in December 2025; pending final review by the Science and Technology Committee (CCT)); draft General Cybersecurity Law prepared by CNCiber/GSI (released publicly in April 2026); media coverage by TELETIME, Convergência Digital, Mobile Time, and Telesintese. The approval assessment is an estimate and is subject to change. Status as of June 2026.

Brazil's Cybersecurity Regulatory Framework

10

State of Scams Brazil - 2026

Two Legislative Initiatives Beginning to Converge. For the first time, Brazil is developing its cybersecurity policy through two complementary legislative initiatives. In Congress, the Cybersecurity Legal Framework (Bill No. 4,752/2025) is advancing through the Senate, establishing principles, guidelines, and funding mechanisms that provide the institutional foundation for digital protection. In parallel, the draft General Cybersecurity Law, prepared by the National Cybersecurity Committee (CNCiber) and currently non-binding in nature, further develops the “how”: risk management obligations, incident reporting requirements, and the protection of critical infrastructures. The most significant development in recent months has not been a dispute between the two proposals, but rather their growing convergence: the government has begun coordinating efforts to merge the initiatives so that they can move forward together.

Approval in 2026: A Favorable Window, but a Narrow One. The likelihood of approval still in 2026 should be viewed as an assessment rather than a certainty. The Cybersecurity Legal Framework is the more mature proposal: it has already been approved by the Senate’s Constitution and Justice Committee and is now proceeding under a final review process at the Science and Technology Committee, which shortens its internal legislative path. It also has the explicit support of the federal government, which has advocated for its urgent approval. In its favor is the unusual consensus among the Executive Branch, Congress, and the private sector. On the other hand, the 2026 electoral calendar may constrain the legislative agenda in the second half of the year, and the proposal still faces review by the Chamber of Deputies. Because the General Cybersecurity Law is still a non-binding draft proposal, it is unlikely to become law independently in the short term. The most likely outcome is its incorporation into the Cybersecurity Legal Framework.

For Citizens: Fewer Disruptions, Greater Transparency. For the public, the effects are primarily indirect, but tangible. By establishing minimum standards and resilience plans for essential services — from healthcare and education to public security — the new framework is expected to reduce the frequency and severity of disruptions caused by cyberattacks. This is complemented by the obligation to notify users affected by significant incidents, a transparency measure that provides citizens with greater predictability and helps rebuild the digital trust that underpins the economy.

For Companies: From Voluntary to Mandatory. It is in the private sector that this shift in standards will be felt most strongly. The core change is the transition from voluntary best practices to clear obligations, particularly the mandatory reporting of significant incidents to the competent authority. Based on a risk- and size-proportionate approach, organizations are expected to appoint a cybersecurity officer within senior management, maintain incident response plans and Computer Security Incident Response Teams (CSIRTs), and assess the maturity of their suppliers. More than a compliance cost, this represents greater regulatory predictability and a reduction of systemic risk across the entire supply chain.

For Government: A National Coordination Framework. For the government, the key benefit is greater organization and coordination. The proposals establish an integrated national architecture, including a National Cybersecurity System coordinated by the Institutional Security Office of the Presidency of the Republic, as well as a dedicated center for incident monitoring and response (CENCiber). They also make incident reporting mandatory for federal government agencies. Financial sustainability would be supported by existing sources, such as allocations from the National Public Security Fund and lottery revenues, providing the framework with a more stable and predictable resource base than the current model.

Our global research surveyed 58,900 respondents across 42 countries

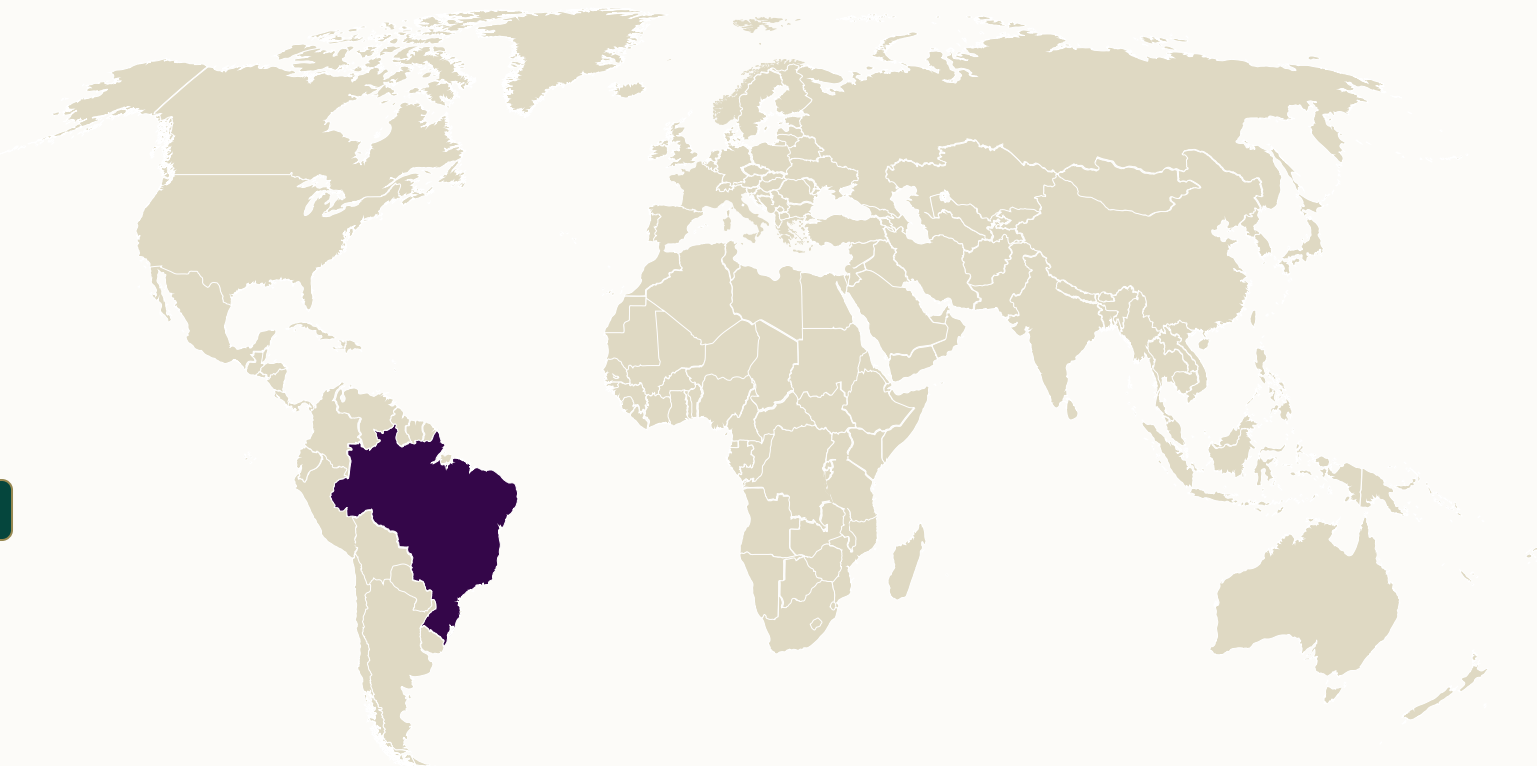
GLOBAL COUNTRIES

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

LATAM COUNTRIES

Argentina
Brazil
Mexico

The data in this report will focus on findings within the **Brazil**



Who we spoke to in the **Brazil**

Sample size | 1,170 people

Audience | Adults aged 18+ living in the Brazil

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

Methodology | 15-minute online survey

Sample source | Online research panel

Fieldwork | 16th March – 13th April 2026

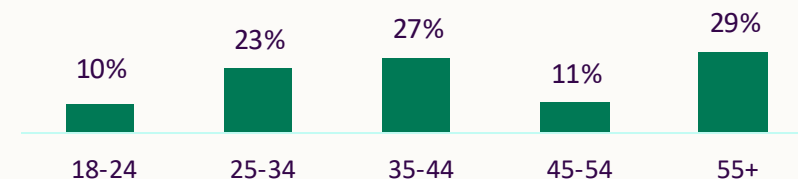
Base: All respondents (n=1170)

GENDER

Male
47%

Female
53%

GENERATION / AGE



WORKING STATUS

NET: Working



NET: Not working

PARENTAL STATUS

NET: Parents

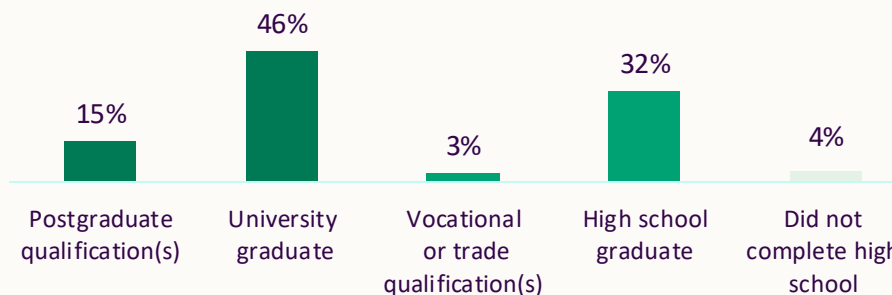


NET: Not parents

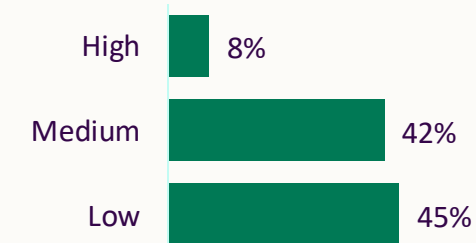
EDUCATIONAL STATUS

NET: High Education 64%

NET: Mid Education 36%



HOUSEHOLD INCOME



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 Brazil, 113 of 1,170 respondents reported losing money to scams, equating to an estimated 16,504,738.28 affected adults nationally.

Multiplying this by the average loss (R\$ 1,287.20) produces an estimated total loss of R\$ 21,244,899,110.06

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 5.21 Brazilian Reais

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

42% are confident they recognize a scam

Total participants (1,170)

81% encountered a scam in the last year

Top reasons for not interacting with scams

43% message or request did not seem legitimate

42% I do not respond to unsolicited messages or calls

38% contact came from an unknown source

14% of parents say their child has been scammed too

39% interacted with the scammer
(56% amongst those that encountered a scam)

Top reasons for not giving money

31% offer or request felt too good to be true

31% request was suspicious

25% request did not match how legitimate organizations normally operate

The Scam Funnel in Brazil

10% lost money or data that led to money lost (scammed)
(25% amongst those that interacted with a scam)

Most common scams interacted with

22% Shopping scam

17% Unexpected money scam

17% Employment scam

76% of those scammed say it impacted their mental wellbeing

34% of those scammed say it happened more than once

4% reported the scam to authorities
(38% amongst those that lost money to a scam)

20% of those who reported their losses say their money was reimbursed by the organization they reported to

The research covers **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 Latin American average are made either in brackets (X%) or alongside the market 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:



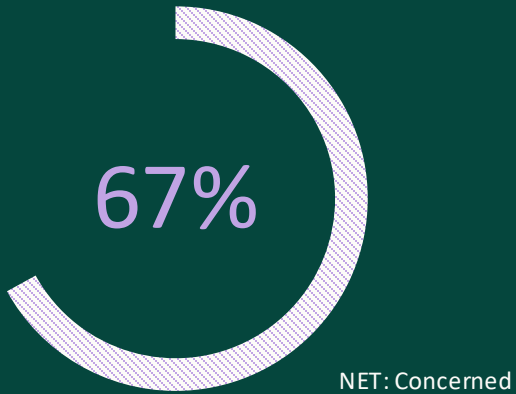
To find out more about the report and its authors:

[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.

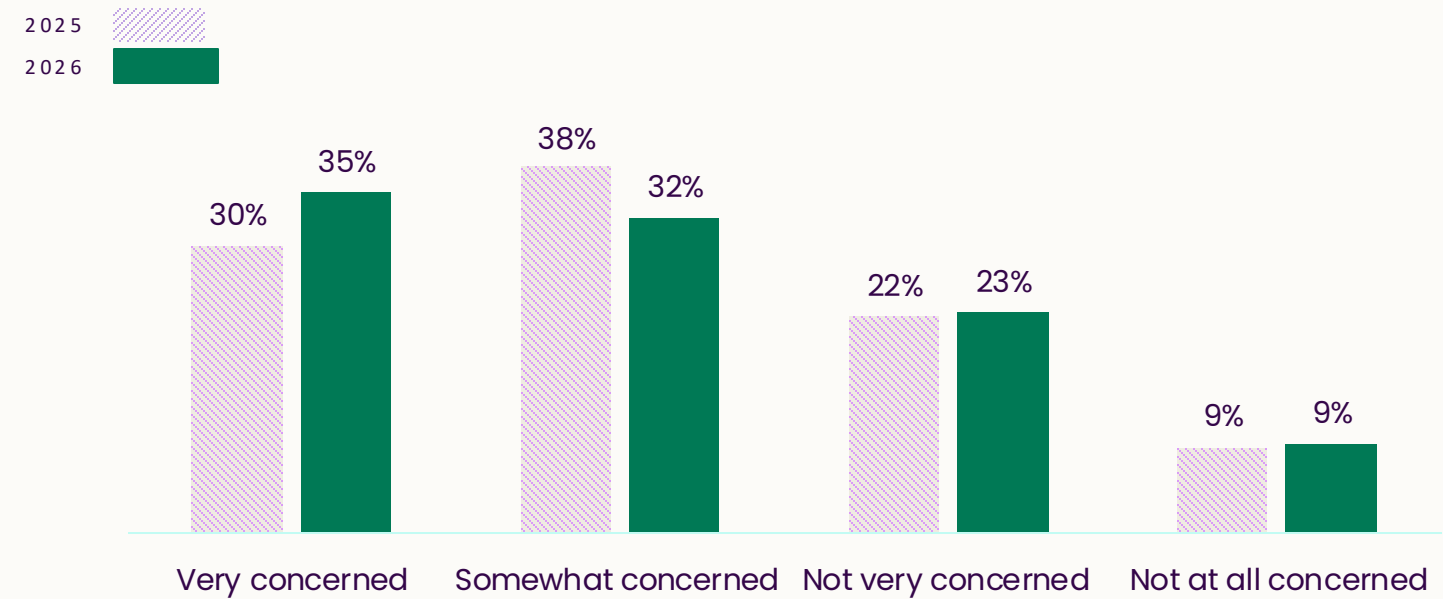


are concerned about
being scammed in 2025
vs



Concerns about scams in Brazil remain the same

Proportion concerned about being scammed in 2025 vs 2026



Q1B. How concerned have 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 (n=1170)

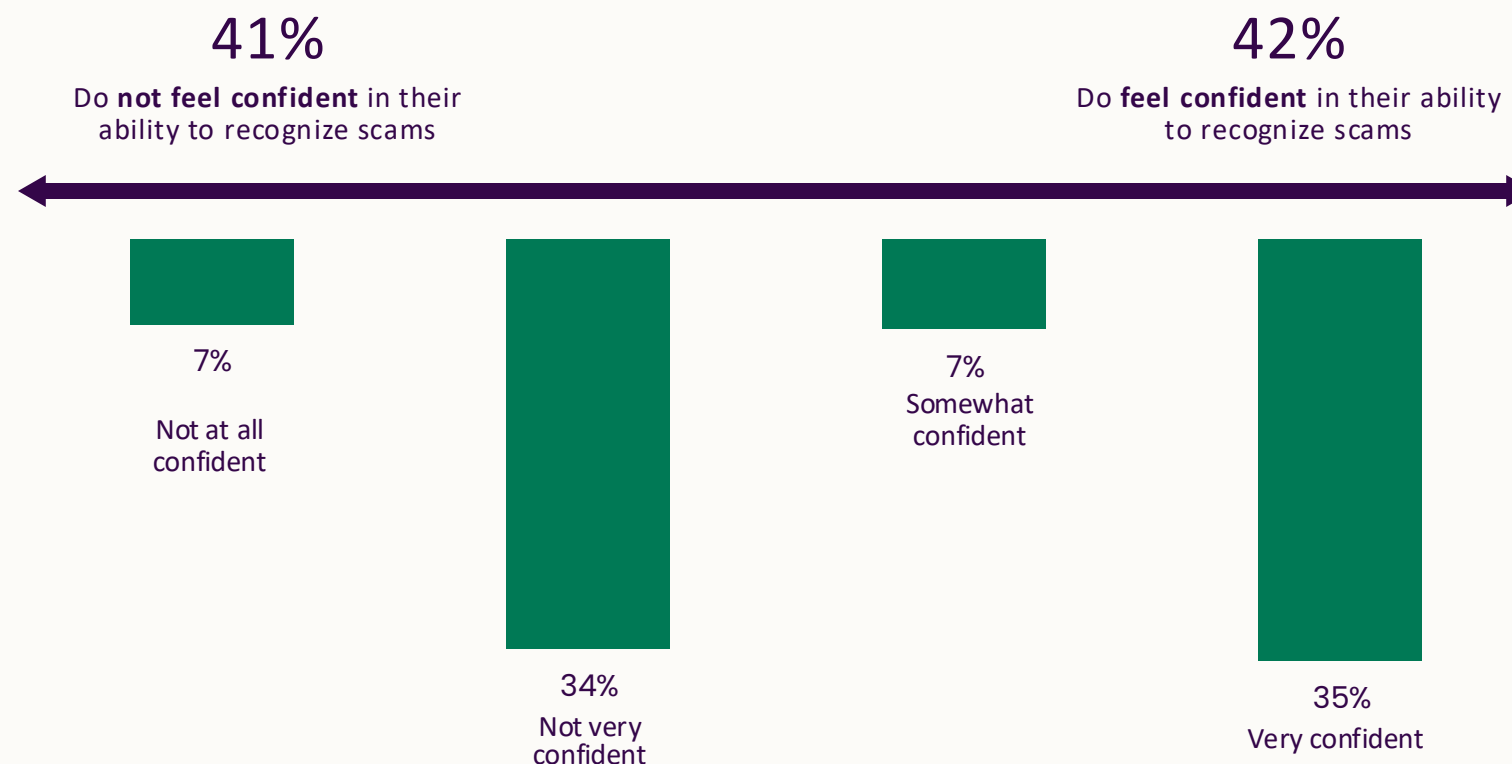




Scam-recognition confidence in Brazil skews strongly towards **Gen Z (51%)**, those with **higher education (45%)**. By comparison, lack of confidence is much higher older generations of **Gen X (53%)** and **women (48%)**.

Two in five Brazilian adults are **confident in their ability to spot scams** – but equally two in five are not confident

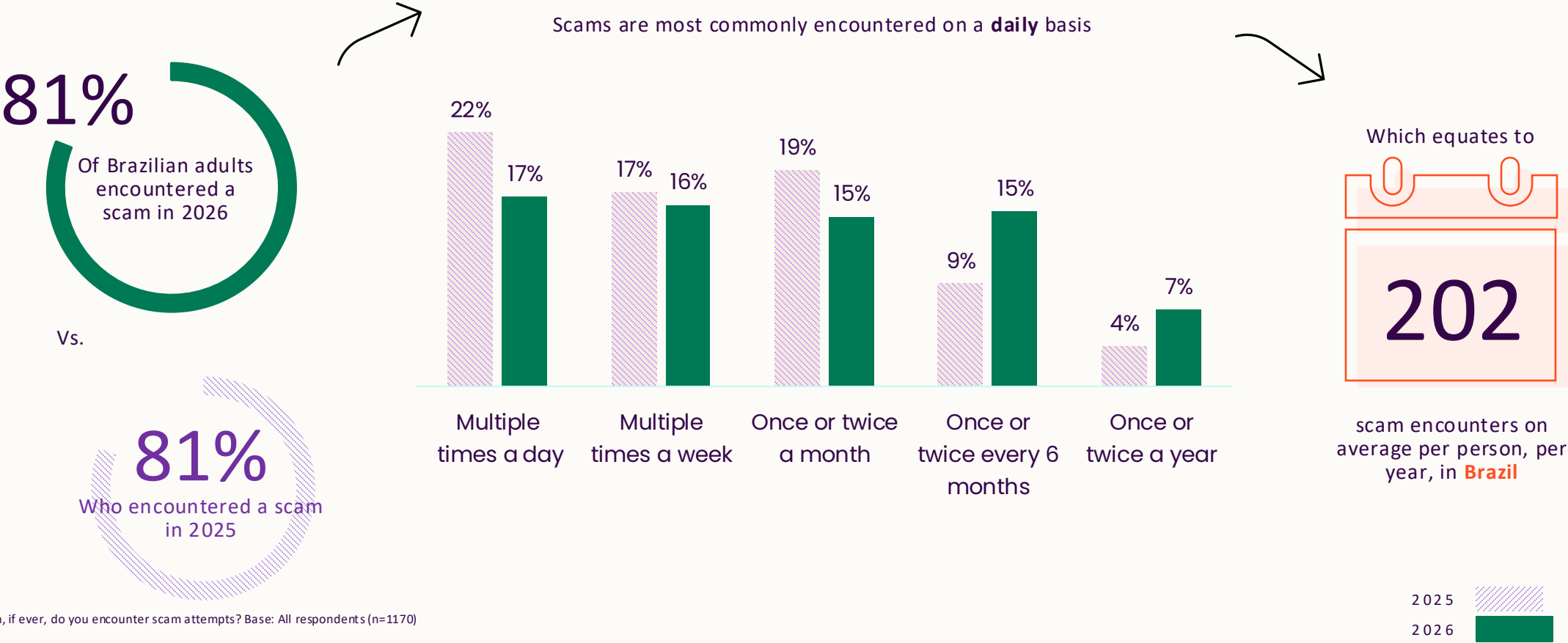
Confidence in recognizing scams



Q1A. How confident are you, if at all, that you can recognize scams? Base: All respondents (n=1170)

Three in four Brazilian adults encounter a scam in 2026, same as 2025

Prevalence & frequency of encountering a scam

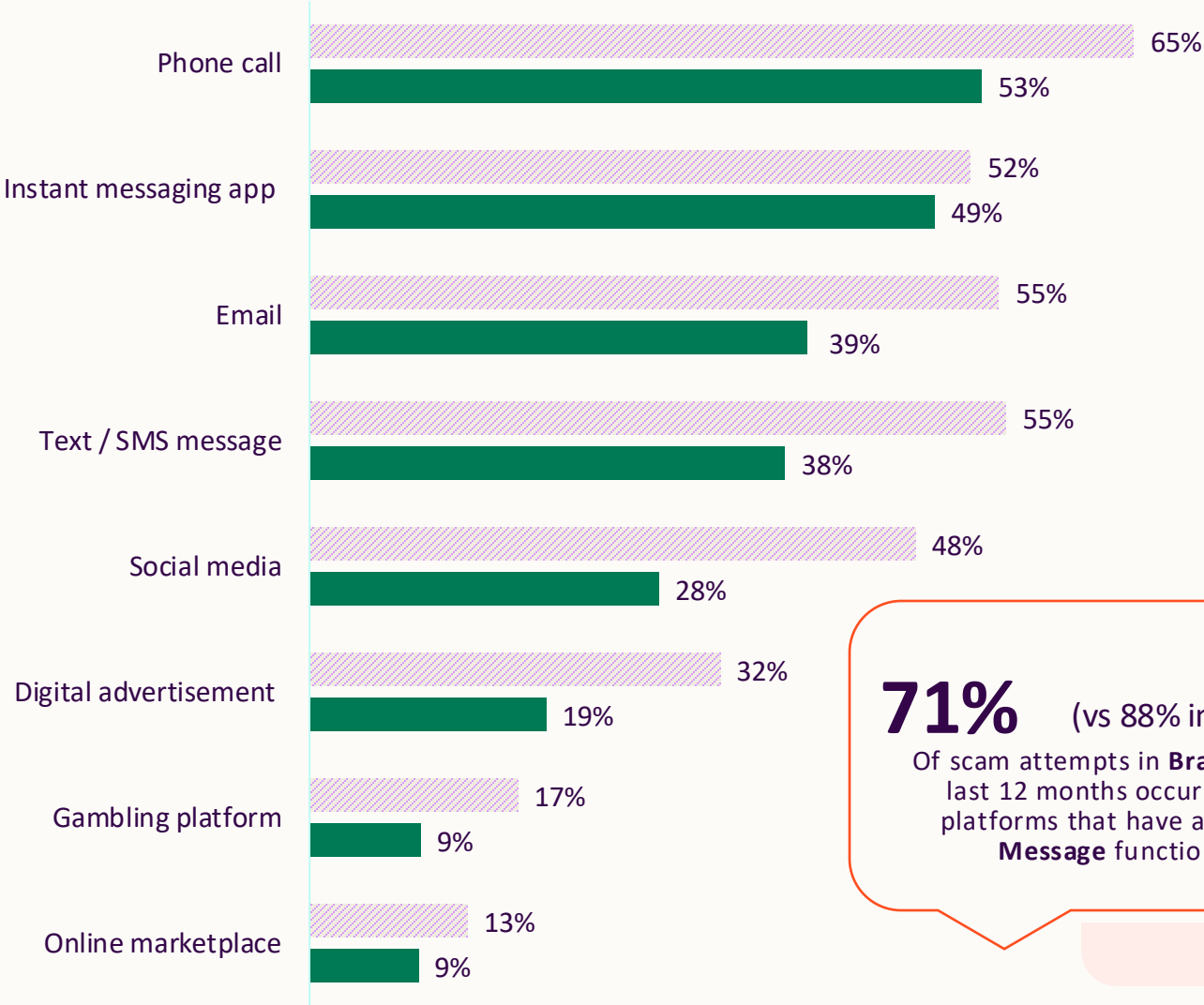


Q2. How often, if ever, do you encounter scam attempts? Base: All respondents (n=1170)

Note: Using the average number of scam attempts reported by all respondents (201.6 per person per year) and applying this figure to Brazil's adult population (170,889,768 people) results in an estimated 34,451,377,229 scam attempts, equivalent to approximately 34.5 billion scam attempts per year.

Scam messages over phone calls and instant messaging apps remain most common in Brazil – while scam encounters are reported across fewer channels

Communication platforms where scams are encountered – top 8

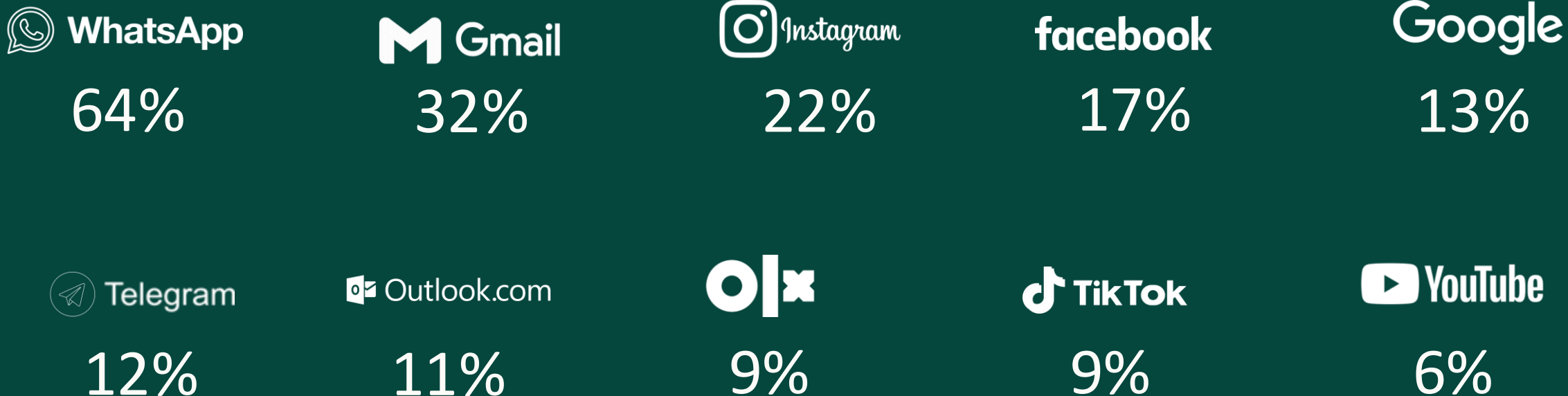


71% (vs 88% in 2025)
Of scam attempts in **Brazil** in the last 12 months occurred on platforms that have a **Direct Message** function*

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 (n=820).
*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).

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

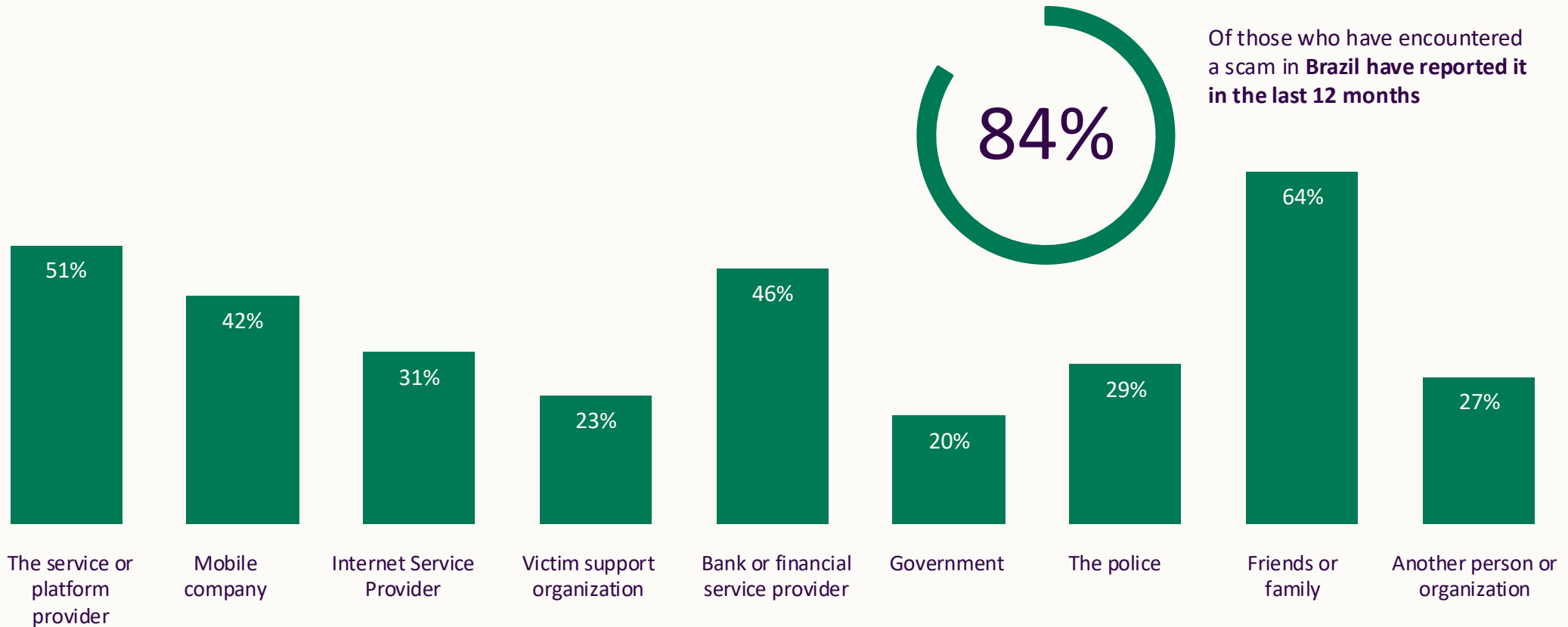
Top 10 online platforms that victims report are used by scammers to contact them in the last 12 months in Brazil



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=820)

Scam encounters are reported most frequently to **close relations** as well as **platform providers** and **banks**.

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** (n=820)

While multiple sources help, **past scam experiences** and close relationship of **friends/family** are considered most effective in helping Brazilian adults 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 (n=1170)

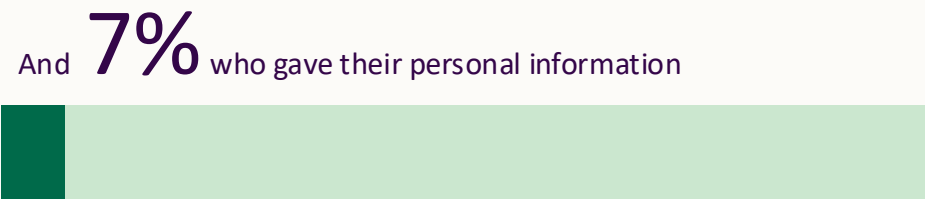
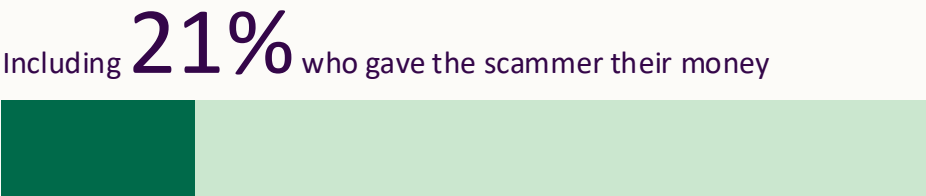
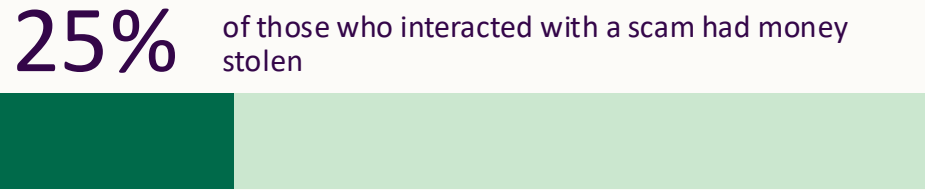
SCAM INTERACTIONS

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.

More than half
Brazilian adults that
encounter a scam
attempt go on to
interact with it

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.

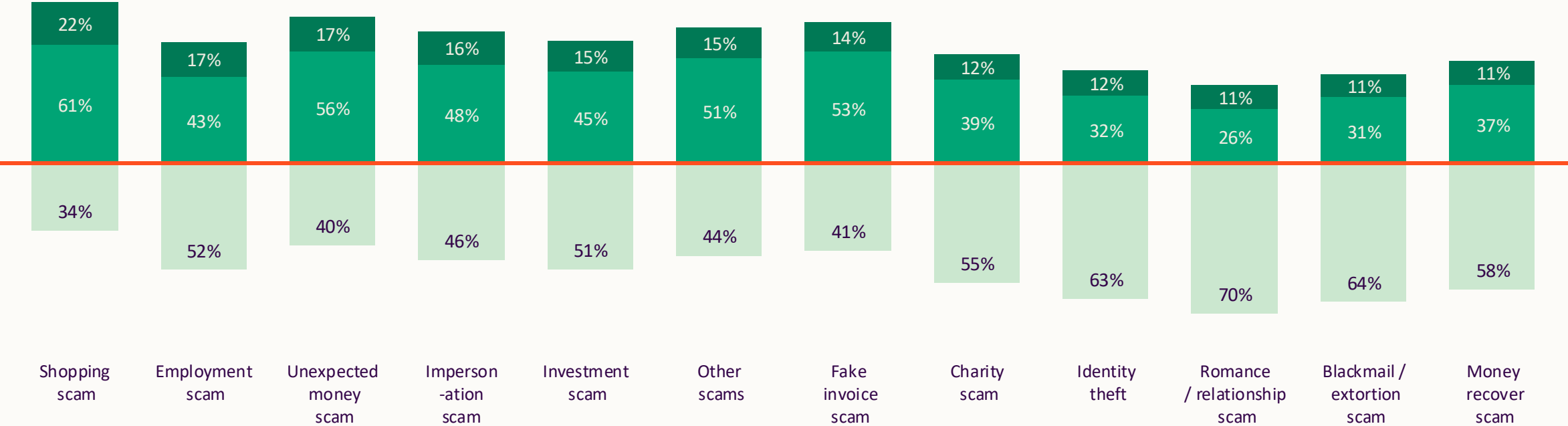
Brazilian adults most commonly interact with shopping, unexpected money and employment scams

Level of interaction with scams in the last 12 months

Interacted

Encountered but did not interact

Did not encounter



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 realised 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 (n=820)

The main reason Brazilian adults give for not interacting with scams are intuitive – **sensing messages are not legitimate** or **not replying to unsolicited message as a rule**

Top 10 reasons for not interacting with scam encounters



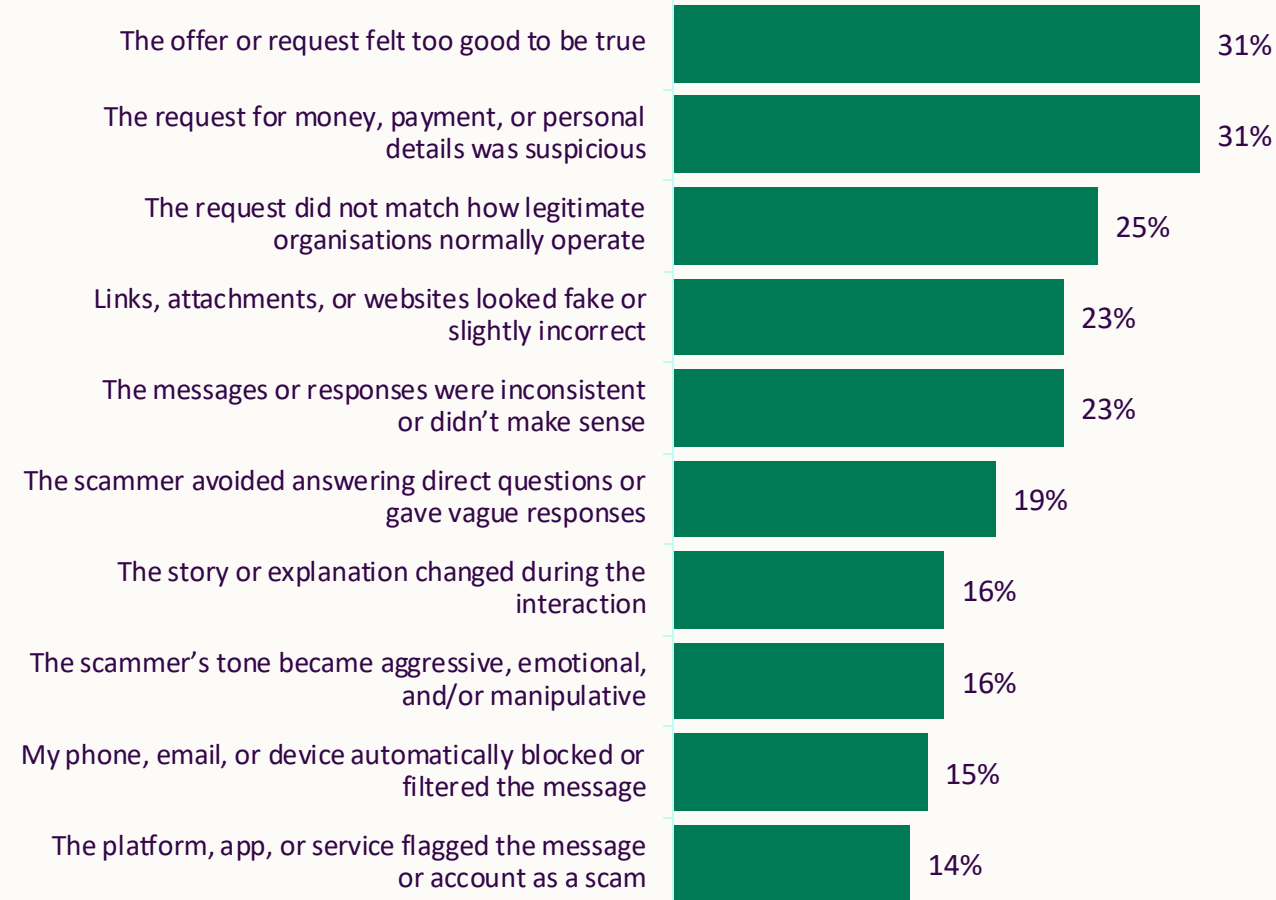
37% of Brazilian adults say they recognized common scam warning signs



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: (n=747)

Requests for money, payment, or personal details being suspicious and unrealistically good offers are the main reasons Brazilian adults do not go on to hand money over to scammers after interaction

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 (n= 276)

A woman with blonde hair and glasses is shown in profile, looking out a window. The scene is dimly lit, with light coming from the window, creating a contemplative mood.

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.

One in three scam victims who lost money in the last year say it happened more than once

Prevalence of revictimization

The average scam victim lost money 1.7 times

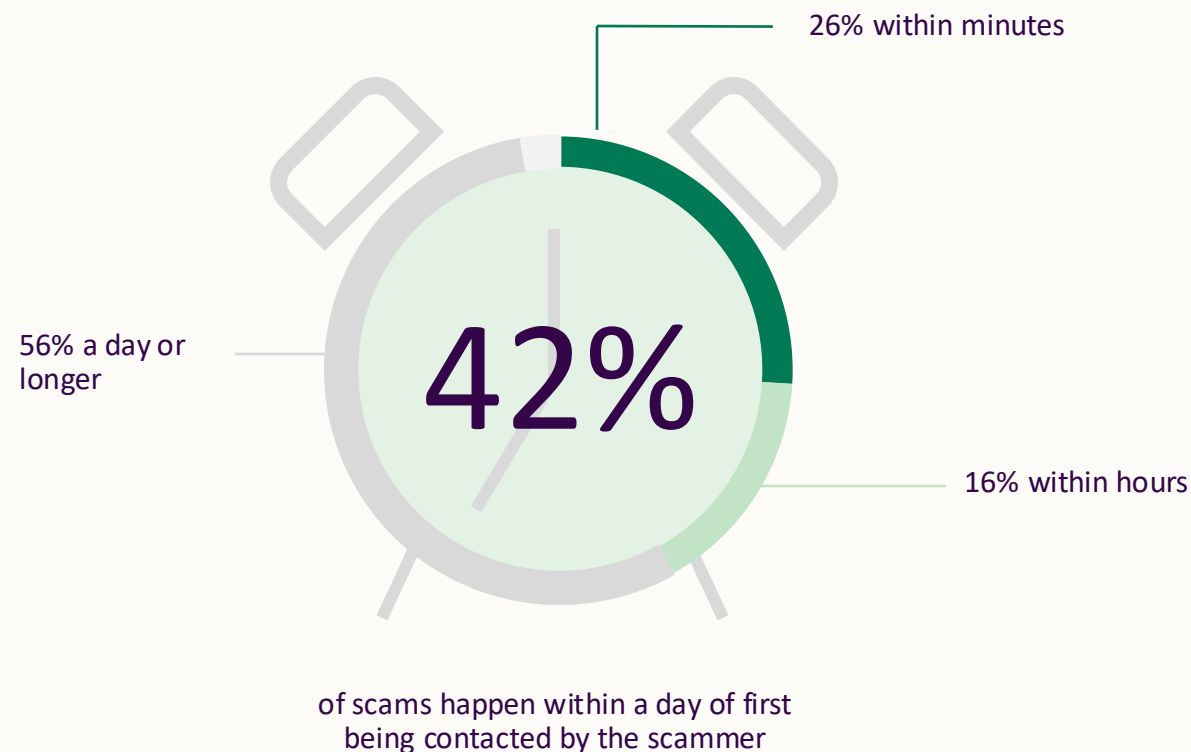


34%

Of Brazilian adults lost money to scams more than once

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 (n=113)

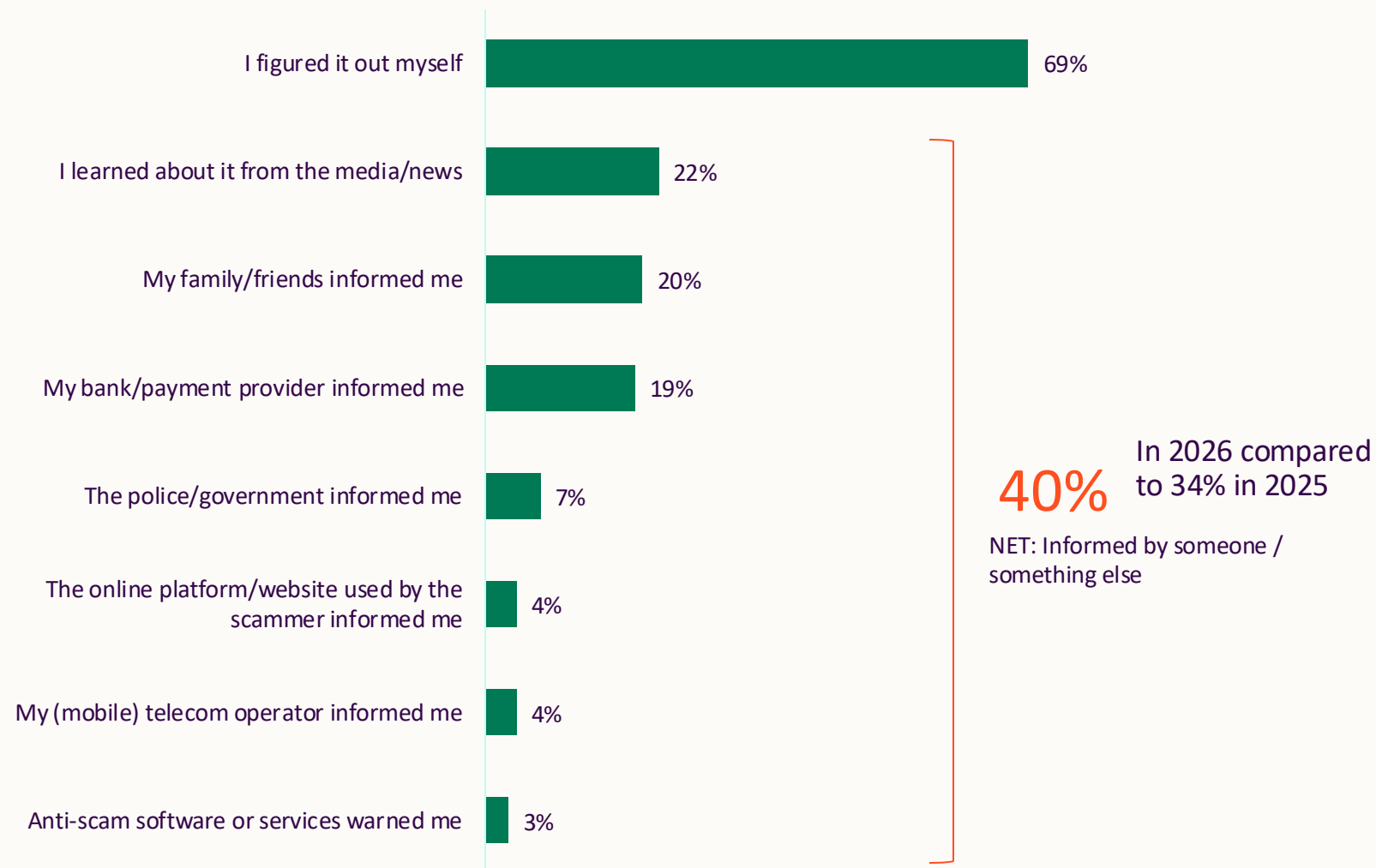
One in four scams
where victims lost
money lasted only
a few minutes



Q10B. Thinking about the most recent time you have 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 (n=113)

There's a rise in Brazilian scam victims discovering they've been scammed after being informed

How victims discovered they are scammed



Q11. How did you discover you have 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 (n=113).

(US\$4.08 billion)

Brazilian adults lost **R\$21.24 billion** in the last year with an average loss of **R\$ 1,287**

(US\$ 247)

Mean: R\$ 1287.2 US \$ 247.1

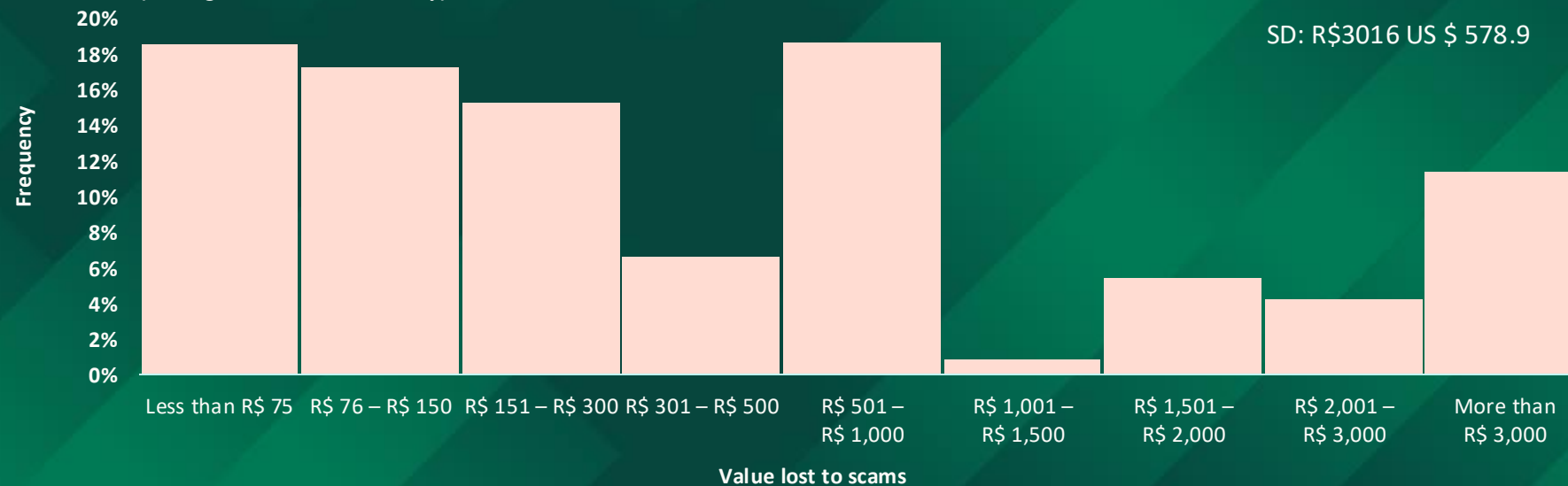
Median: R\$ 295.9 US \$ 56.8

Mode: R\$ 266.7;322.4 US \$ 51.2;61.9

SD: R\$3016 US \$ 578.9

Distribution of value lost to scams

(Among those who lost money)



See appendix . Base: All respondents that lost money to a scam (n=113).

[Click here](#) to see full methodology for average loss calculations



The fake website was indistinguishable from the real one

On TikTok, I saw a perfect video that took me to a website that looked identical to a famous company's. I was careful not to use the link from TikTok and searched for the official website myself, but it looked exactly the same. I fell for it because I thought I could buy without fear.



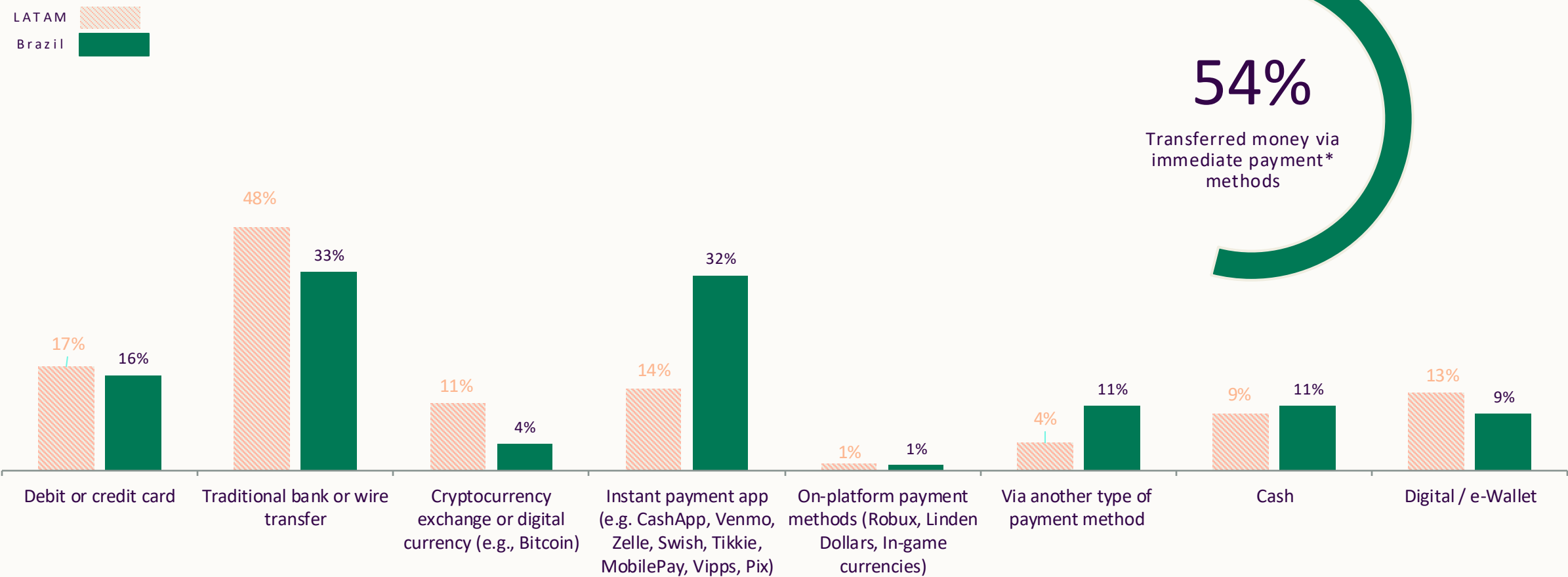
The request came from a cause I trusted

I received a call from a charity I had supported before. They asked for help, so I made a transfer. Later, I mentioned it to someone I knew who worked there, and they told me it was a scam and that many other people had fallen victim as well. I then saw that the charity had already posted warnings on social media, but I hadn't seen them

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=113)

Victim most often send money through **traditional wire transfers**, and with above-average use of **instant payment methods**.

Top 8 payment channels scammers received the payment

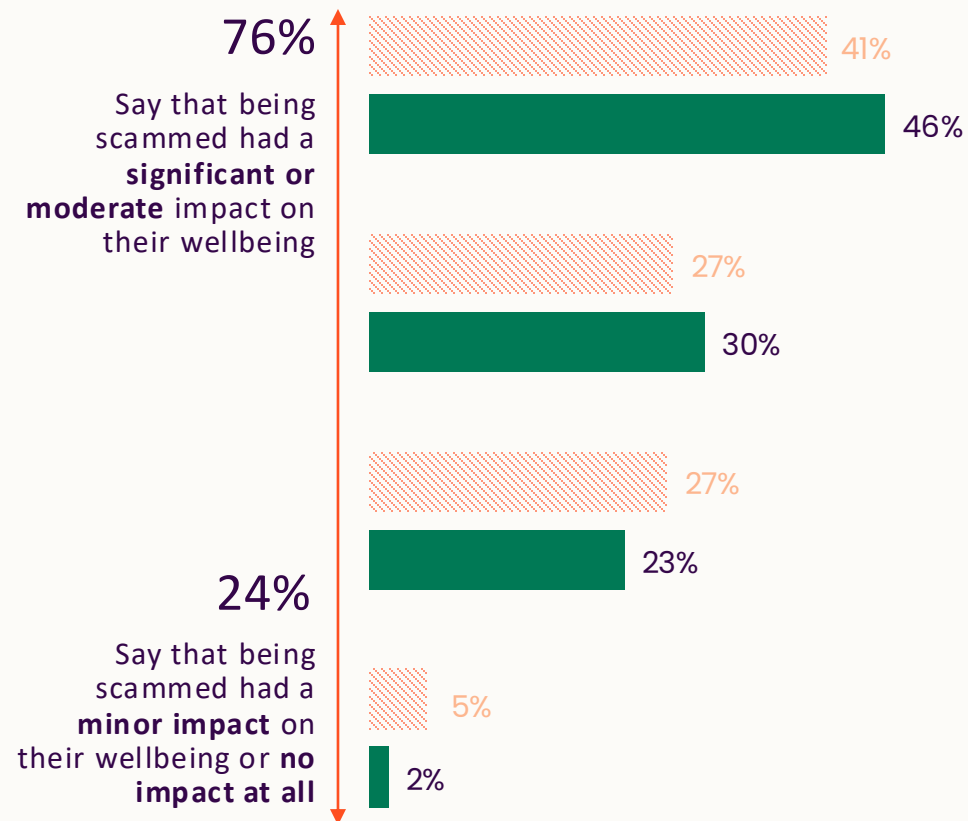


Q13. How did the scammer receive your money? Continue to think about the times you've been scammed and lost money in the last 12 months. Base: All respondents that lost money to a scam (LATAM n=398 | Brazil n=113) | *Immediate payment include Instant payment app, gift cards, digital / e-wallet, cryptocurrency exchange and on-platform payment methods



Three in four victims say being scammed impacted their wellbeing

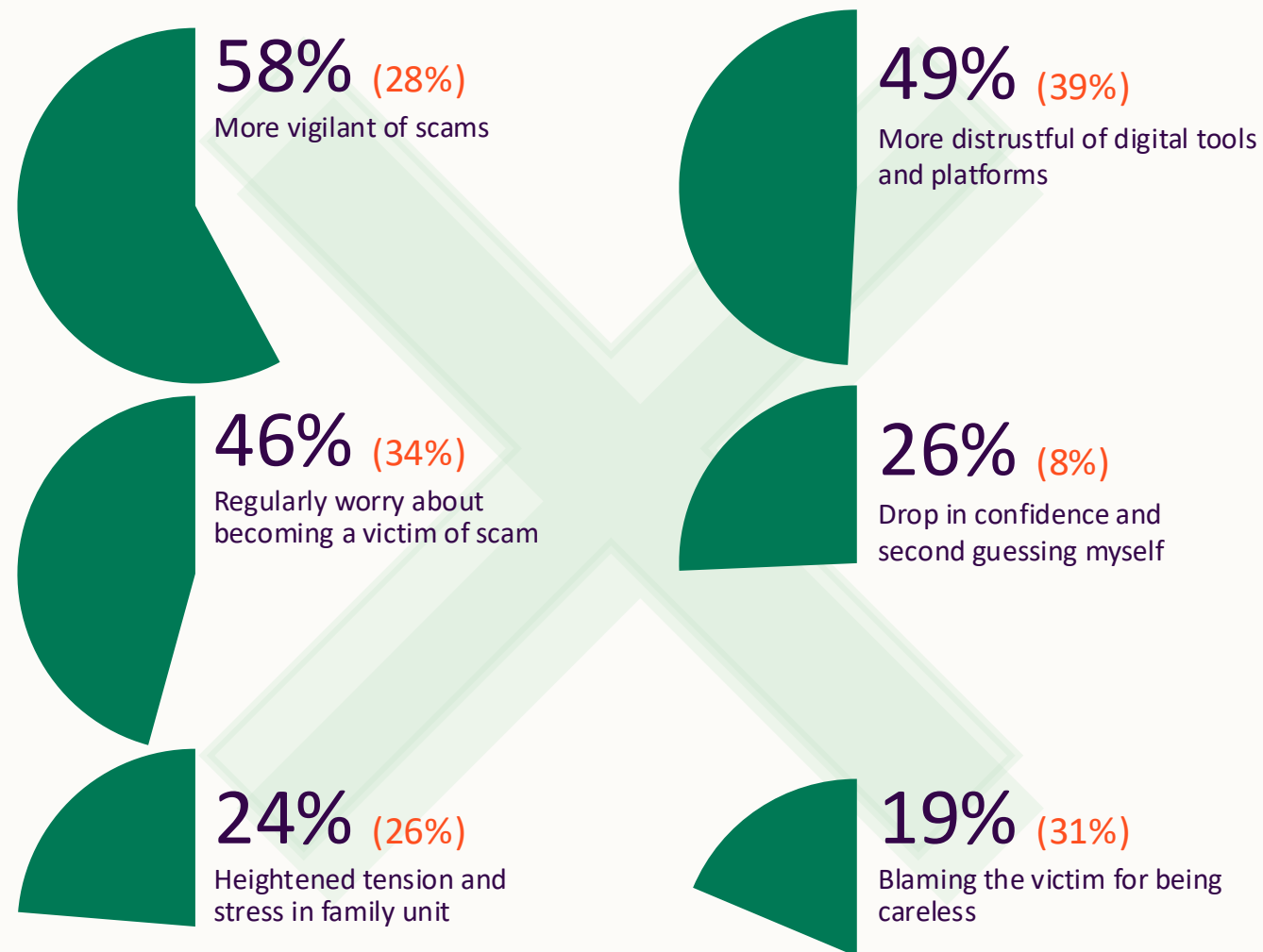
Impact of being scammed on wellbeing



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 (LATAM n=398 | Brazil n=113)

One in two victims who lost money to a scam become more vigilant of scams and distrustful of digital tools and platforms

Impact of scams on victims and their family
– top 6



(X%): LATAM

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 (LATAM n=398 | Brazil n=113)

Brazilian victims say scammers are successful because...

Reasons why scams are successful – top 6

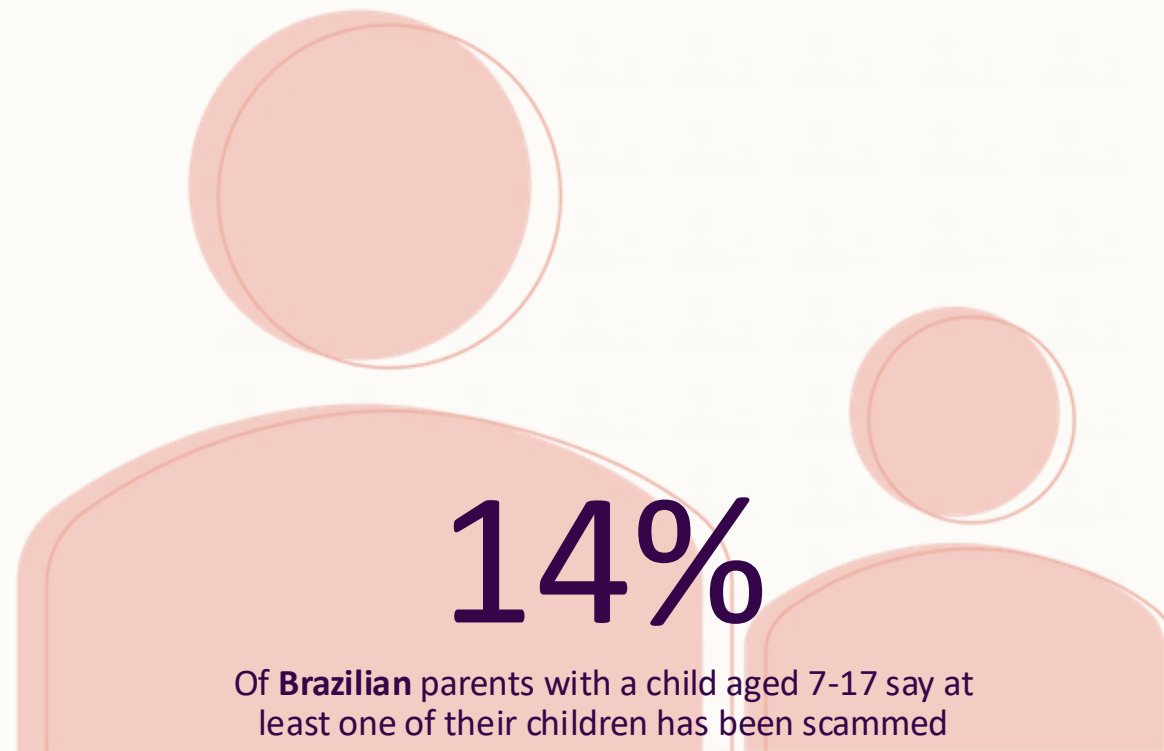


(X%): LATAM

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 (LATAM n=398 | Brazil n=113)

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

Proportion of parents reporting scam experiences amongst their children



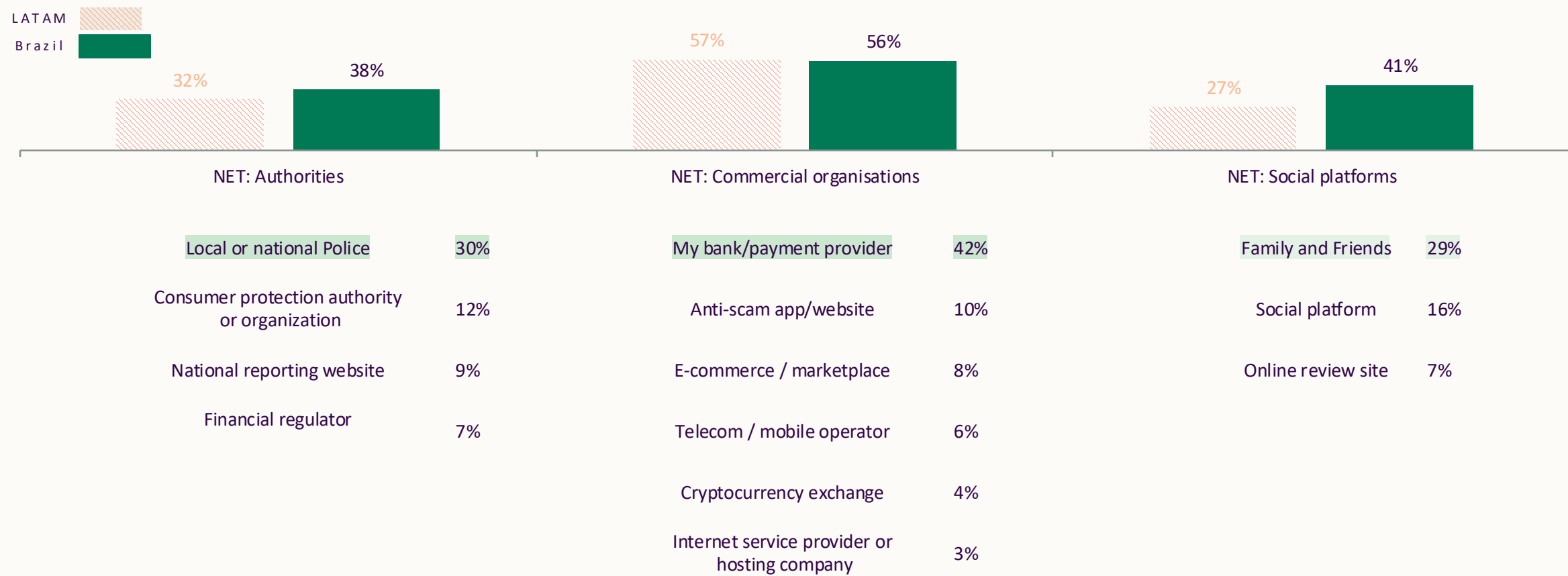
Q19. Have any of your children between the age of 7-17 been scammed? As a reminder, scams are fraudulent or deceptive acts to obtain money and/or personal information. Base: All respondents with children aged 7-17 (n=487)

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.

Reporting is highest to **commercial organisations of banks**, followed by reporting to formal channels of **police** and informally with **friends** - indicating reporting behavior is spread across channels

Channels / organizations scams reported to – top 10



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 ((LATAM n=398 | Brazil n=113)

One in five of those who report their money loss to an organization have money reimbursed or recovered at least partially

20% of those who reported their losses had money recovered or reimbursed



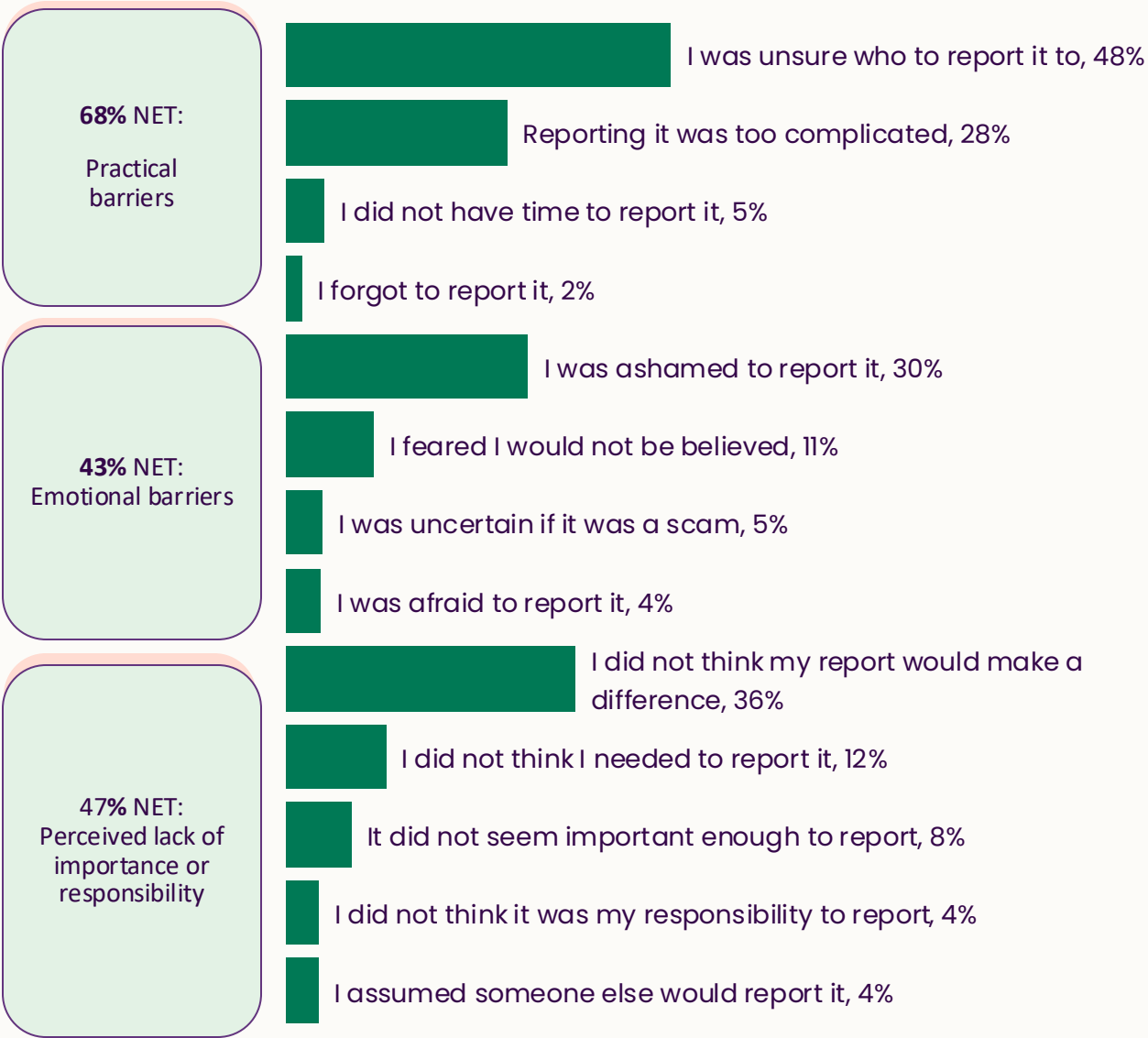
NET: Action taken across: National reporting website, Financial regulator, Local or National Police, Consumer protection authority or organization, E-commerce / marketplace, Online review site, Social platform, Internet service provider or hosting company, bank / payment provider, Cryptocurrency exchange, 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 n=85)

Across LATAM, scams go unreported due to doubts where or why to report, as well as emotional cost



LATAM barriers to reporting scams
Latin American data charted due to low base size in Brazil



Q17. Who did you report the scam to? Base: All respondents that lost money to a scam (Brazil n=113) | Q20. What reasons might you have to not report a scam?. Base: All Latin American respondents that did not report the scam to an organization (LATAM n=289 incl. n=36 from Brazil sample).

Two in five Brazilian adults check for external reviews – considered a more effective way to spot scams.

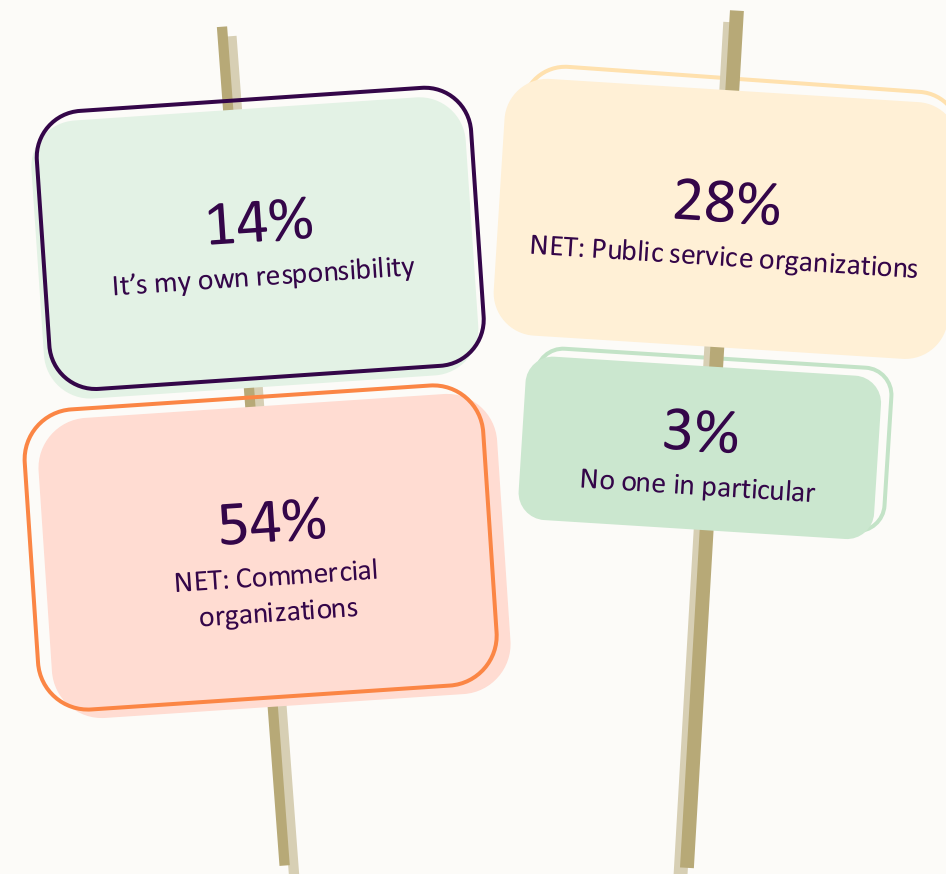
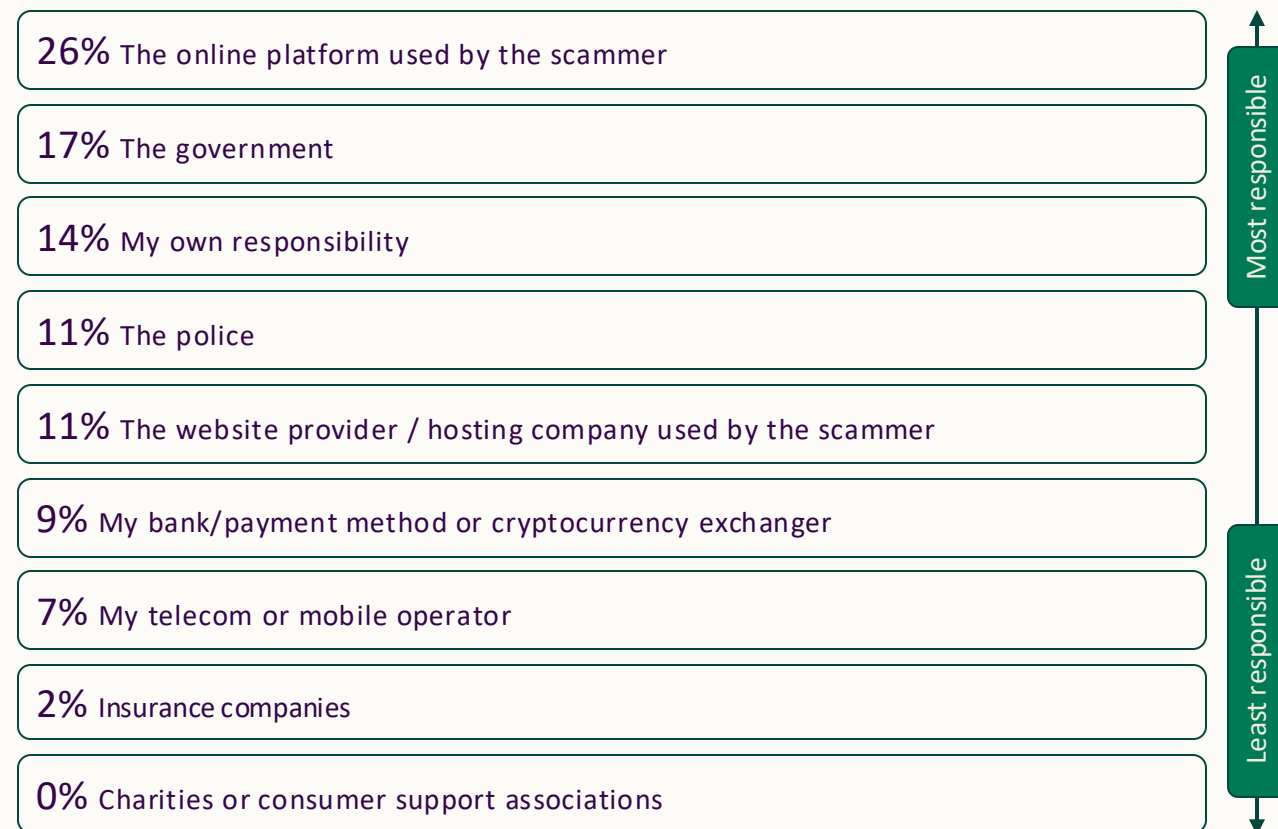
Steps taken to check legitimacy of offer



Q24. What steps do you take to check if an offer, messages, or requests are real or a scam? Base: All respondents (n=1170)

One in four Brazilian adults find the **online platform used by scammers** the most responsible for keeping people safe from scams

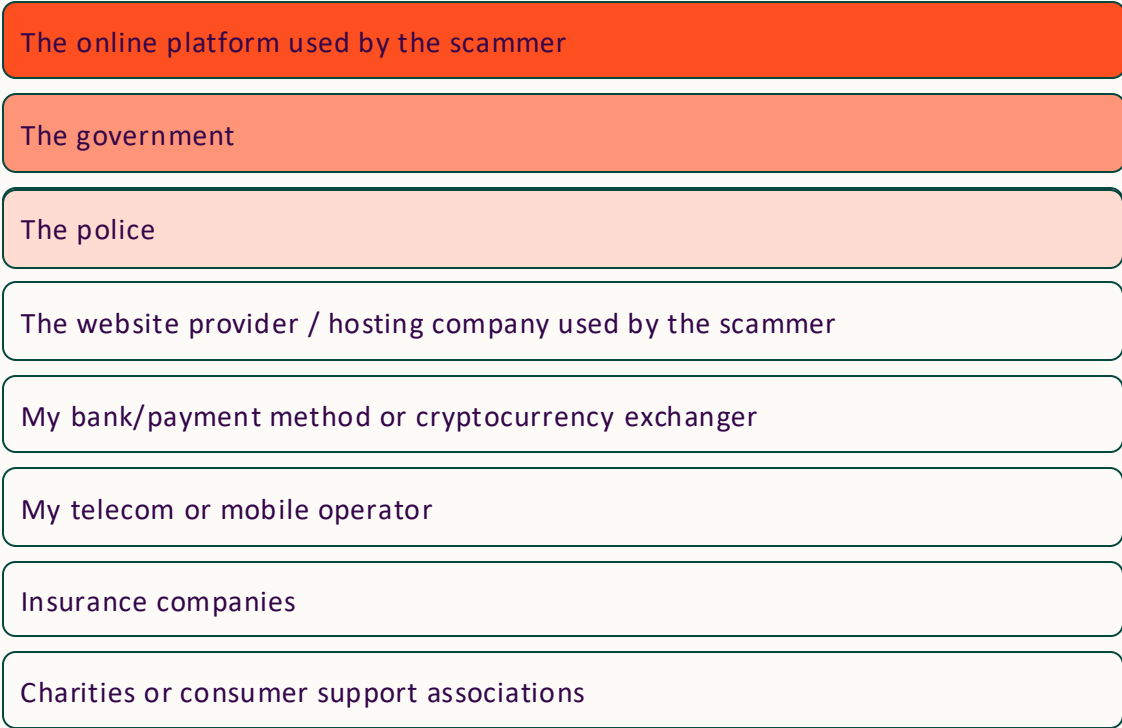
Responsibility for keeping people safe from scammers ranking:



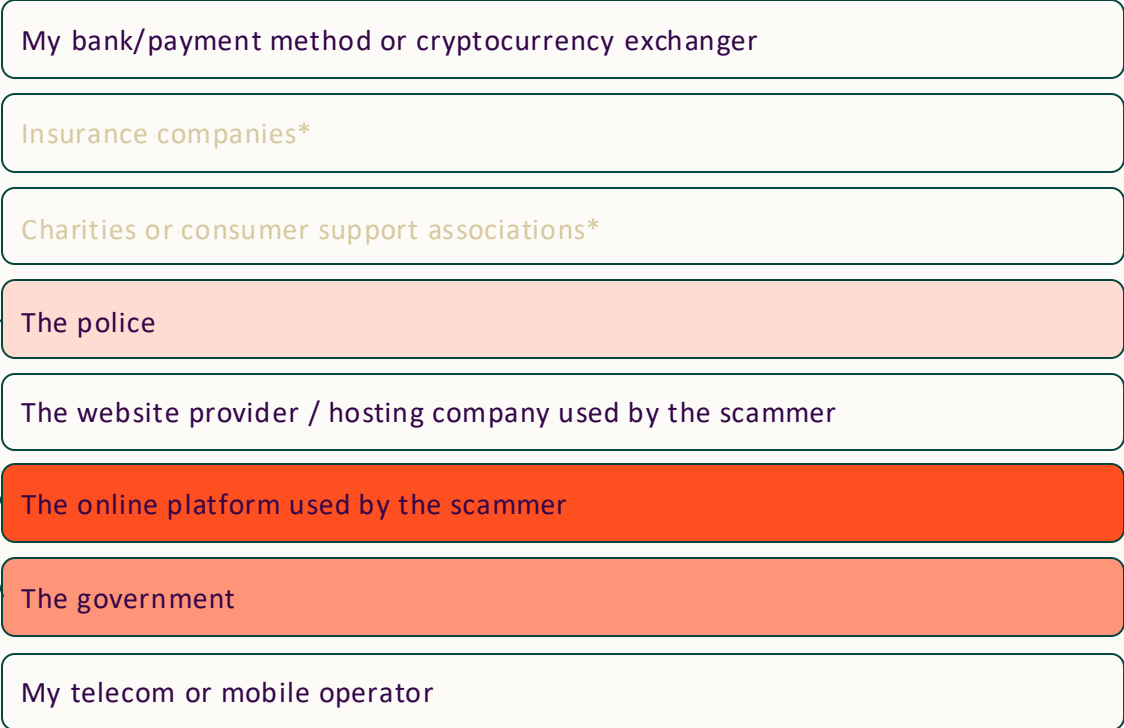
Q21. Who do you think should be most responsible for keeping people safe from scammers? Base: All respondents (n=1170)

The **police's** performance in preventing and resolving scams aligns closest to the expectations. **Government** and **online platforms** rank less effective comparatively

Responsibility for keeping people safe from scammers ranking:



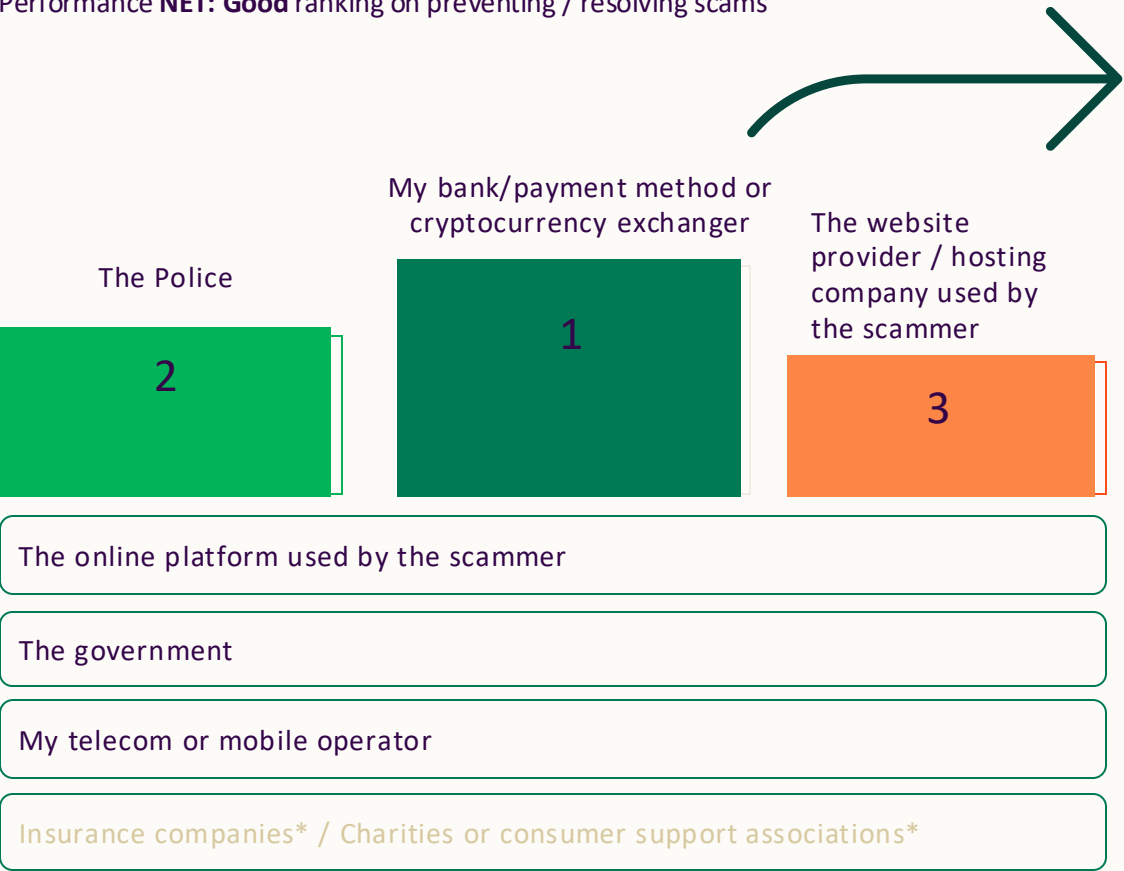
Performance NET: Good ranking on preventing / resolving scams:



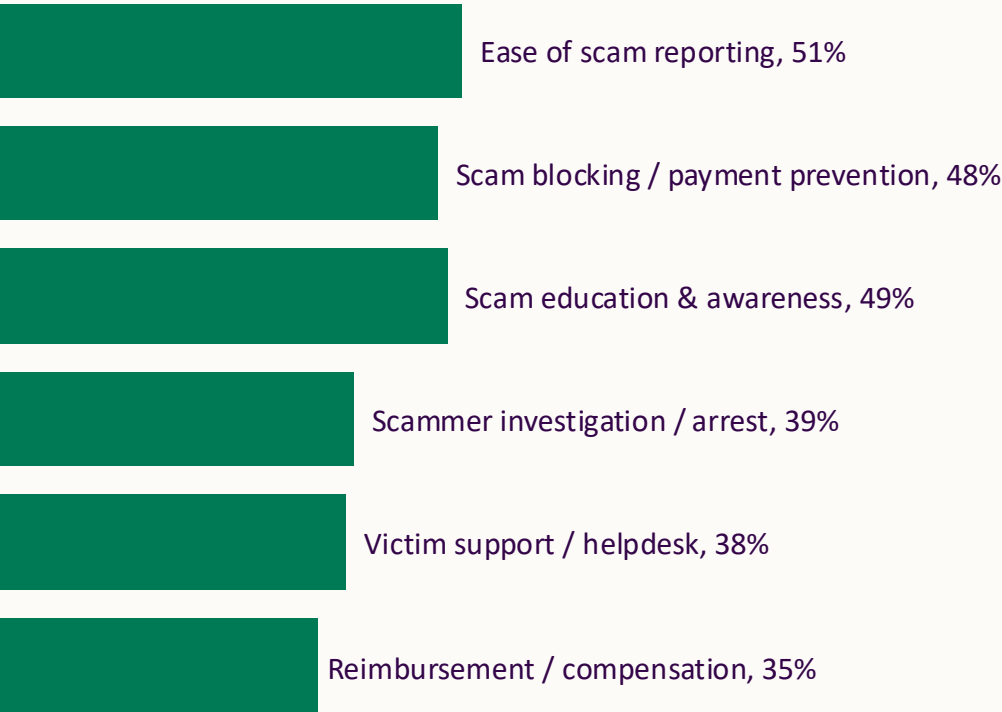
Q21. Who do you think should be most responsible for keeping people safe from scammers? Base: All respondents (n=1170) | Q22. You said should be most responsible for keeping people safe from scammers. How do you rate on the following aspects: Base: All respondents that think .. is responsible for keeping people safe from scammers (government n=199 | police n=124 | charities n=6* | online platform n=309 | website provider n=123 | bank n=105 | telecom operator n=76 | Insurance companies n=20*) *Low base size

Banks cover the scam funnel with education up front, blocking scam payments and having easy reporting - accessible to victims.

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



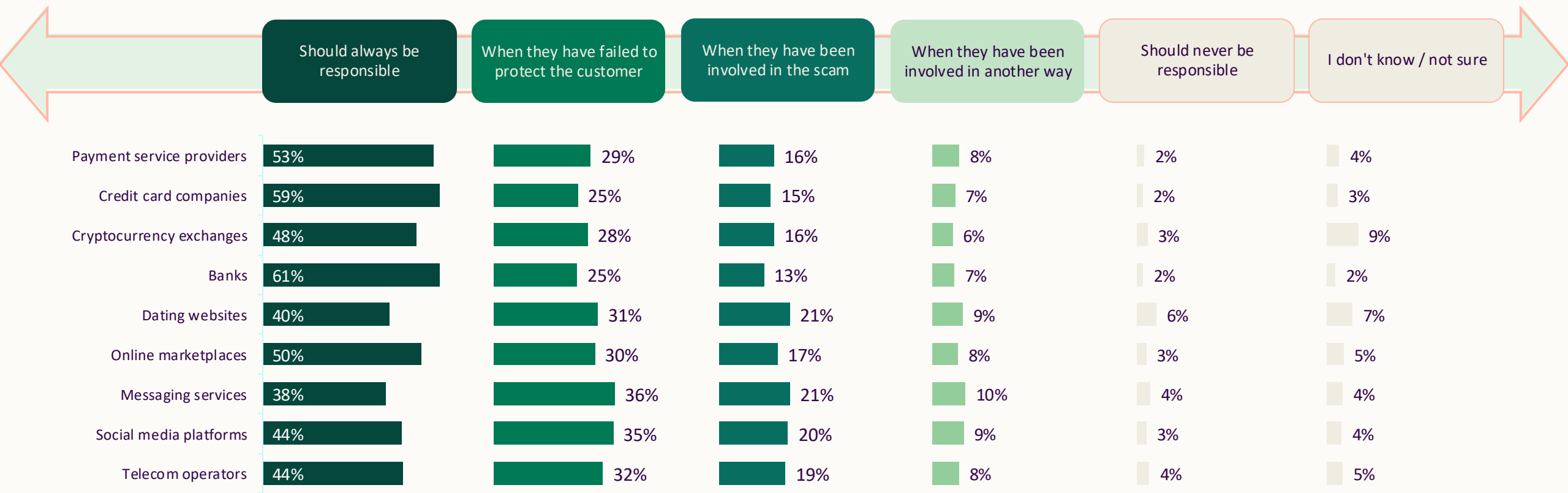
My bank/payment method or cryptocurrency exchanger -NET: Good:



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=199 | police n=124 | charities n=6* | online platform n=309 | website provider n=123 | bank n=105 | telecom operator n=76 | Insurance companies n=20*) *Low base size) | Due to low base size for performance Insurance companies and charities are not included in ranking here

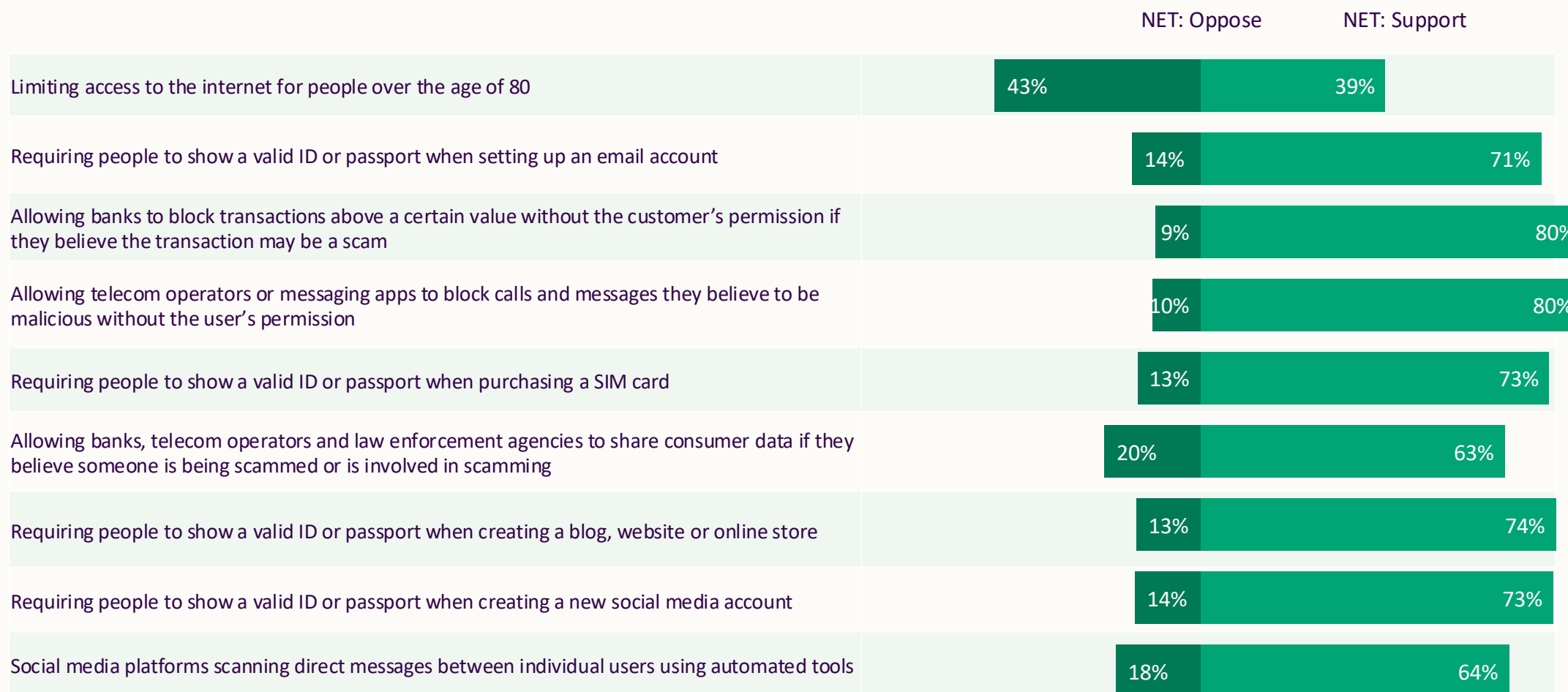
Three in five Brazilian adults believe Banks and Credit card companies should always be responsible for reimbursing those experiencing a scam

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 (n=1170)

Three in four **Brazilian adults** support banks and telecom operators blocking scams directly – but opposition is stronger towards restricting internet access for the elderly.



Q26. To what extent do you support or oppose the following measures designed to protect consumers from scams? Base: All respondents (n=1170)

A magnifying glass is positioned over a line graph on a clipboard. The graph shows a fluctuating line with a general upward trend, set against a grid. The clipboard is on a dark surface, and a beam of light illuminates the graph area.

ABOUT THIS REPORT

[SCAM ENCOUNTERS](#)[SCAM
INTERACTIONS](#)[COST OF
SCAMS](#)[SCAM PREVENTION](#)[ABOUT THE REPORT](#)[ABOUT THE
AUTHORS](#)

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



Opinium is an award-winning strategic insight agency that utilises 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 programme.

Contact europe@opinium.com for enquiries.

About the authors



Jorij Abraham

MANAGING DIRECTOR



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.



Renata Salvini

CHAPTER DIRECTOR BRAZIL



Renata Salvini is the Brazil Chapter Director for the Global Anti-Scam Alliance (GASA), leading efforts to strengthen cross-sector collaboration in the fight against online fraud and scams in the region.

With over two decades of experience managing complex initiatives, at GASA, Renata works to advance consumer protection in Brazil through partnerships with government, private sector, and civil society organizations. Her focus is on translating global best practices into local action—fostering collaboration, building awareness, and promoting coordinated responses to emerging online threats.



Molly Maclean

ASSOCIATE DIRECTOR



Molly Maclean is an Associate Director specialising 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.

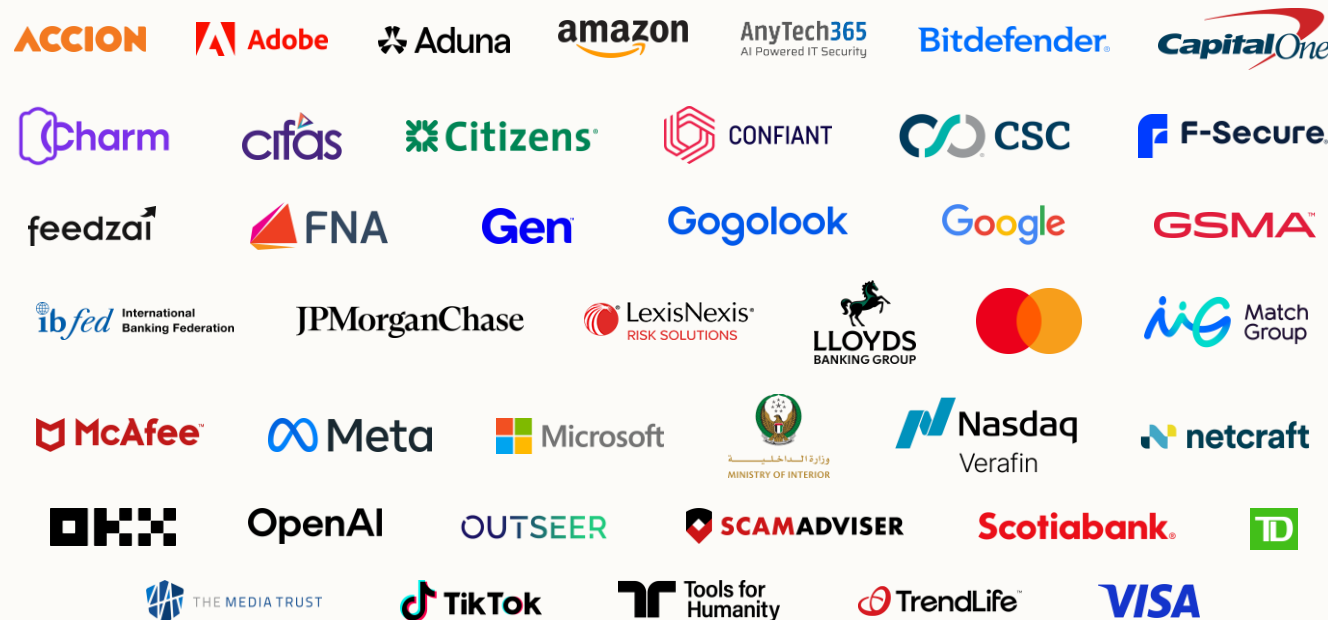
Global Solutions

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



Our Corporate Members



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 ENCO UNTERED 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 realised 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 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. Identity 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 have 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 have 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](https://twitter.com/ScamAlliance)



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