

GLOBAL ANTI-SCAM SUMMIT AMERICA 2026

SAN FRANCISCO, USA | 2-3 SEPT



Welcome

GLOBAL ANTI-SCAM
SUMMIT AMERICA
2026



Jorij Abraham

Global Anti-Scam Alliance
Managing Director



Nils Mueller

Global Anti-Scam Alliance
Chapter Director North America

Anybody can get scammed...

Remember noreply@gasaconference.org?



GASA SUMMIT 2026
Uniting Experts to Fight Fraud & Scams
Join speakers, security experts, and peers worldwide.

Dear Summit Participant,

GASA considers security of the upmost importance. We therefor are offering participants a free VPN so they can enjoy the free Wi-Fi at our summit safely.

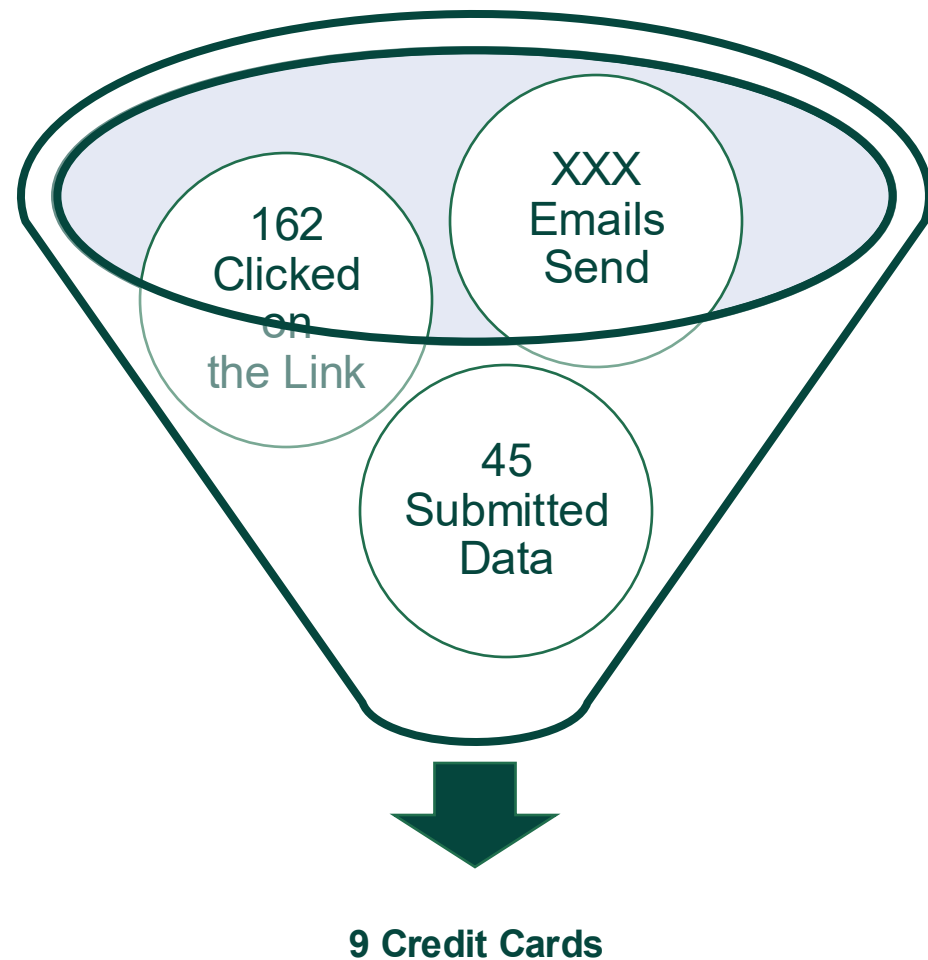
If you like to receive the free VPN software (you can use it for one year).

Claim Your Free VPN

Best regards,
The GASA Team

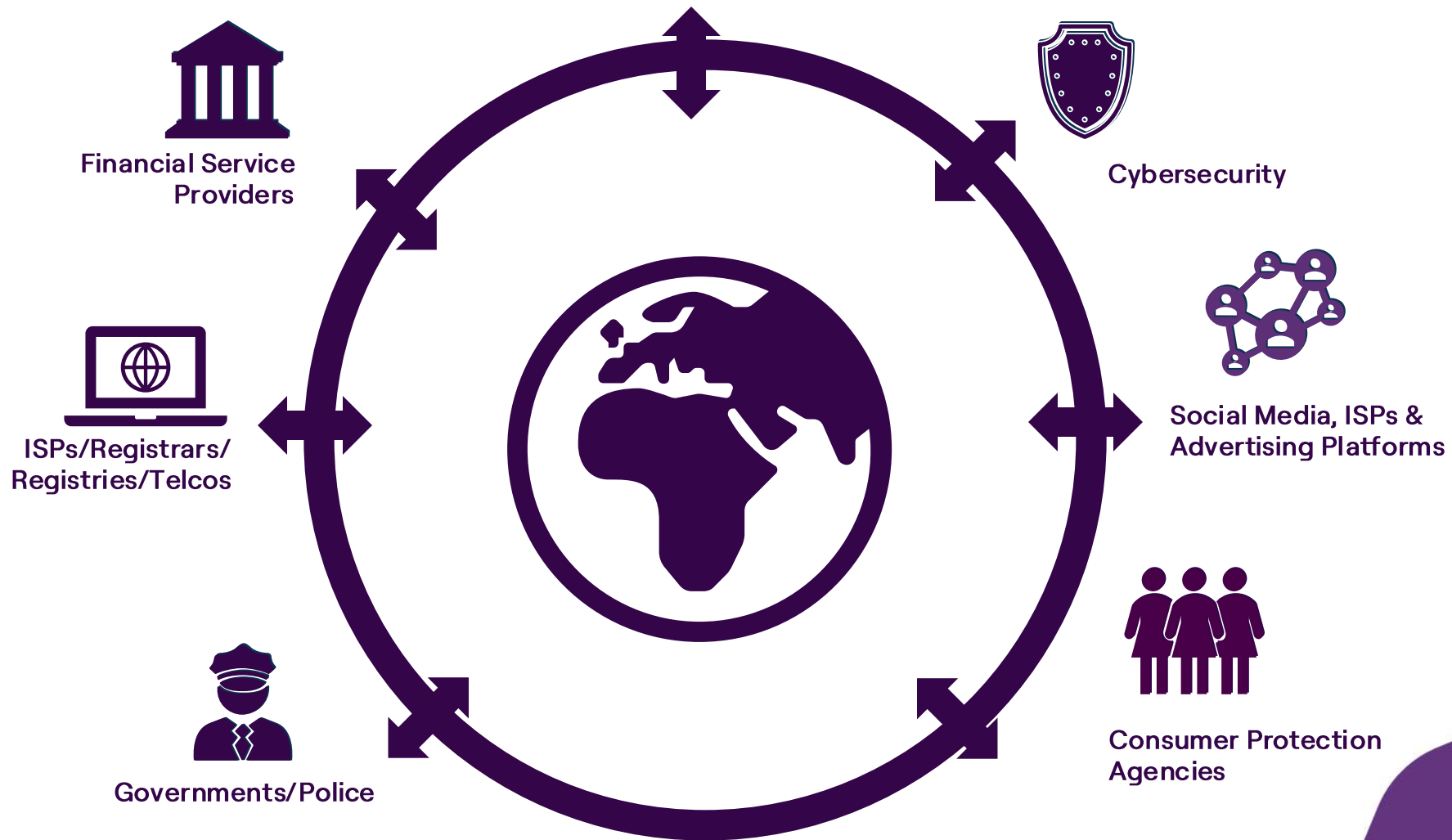
If you wish to unsubscribe [click here](#)

 **Malwarebytes™**



At the Malwarebytes booth 50 people can receive a lifetime license including a free VPN

Scams are a worldwide problem



That needs to be solved globally

GASA

GASA is the Network to Beat a Network



Intelligence Sharing

- Virtual Meet-ups
- Best Practice Blogs
- Working Groups



Networking

- 3 Summits
- Member Directory
- GASA Chapters



Research

- 30+ State of Scam Reports
- Global, Cross-Sector Policy Papers
- Scam Fighter Awards



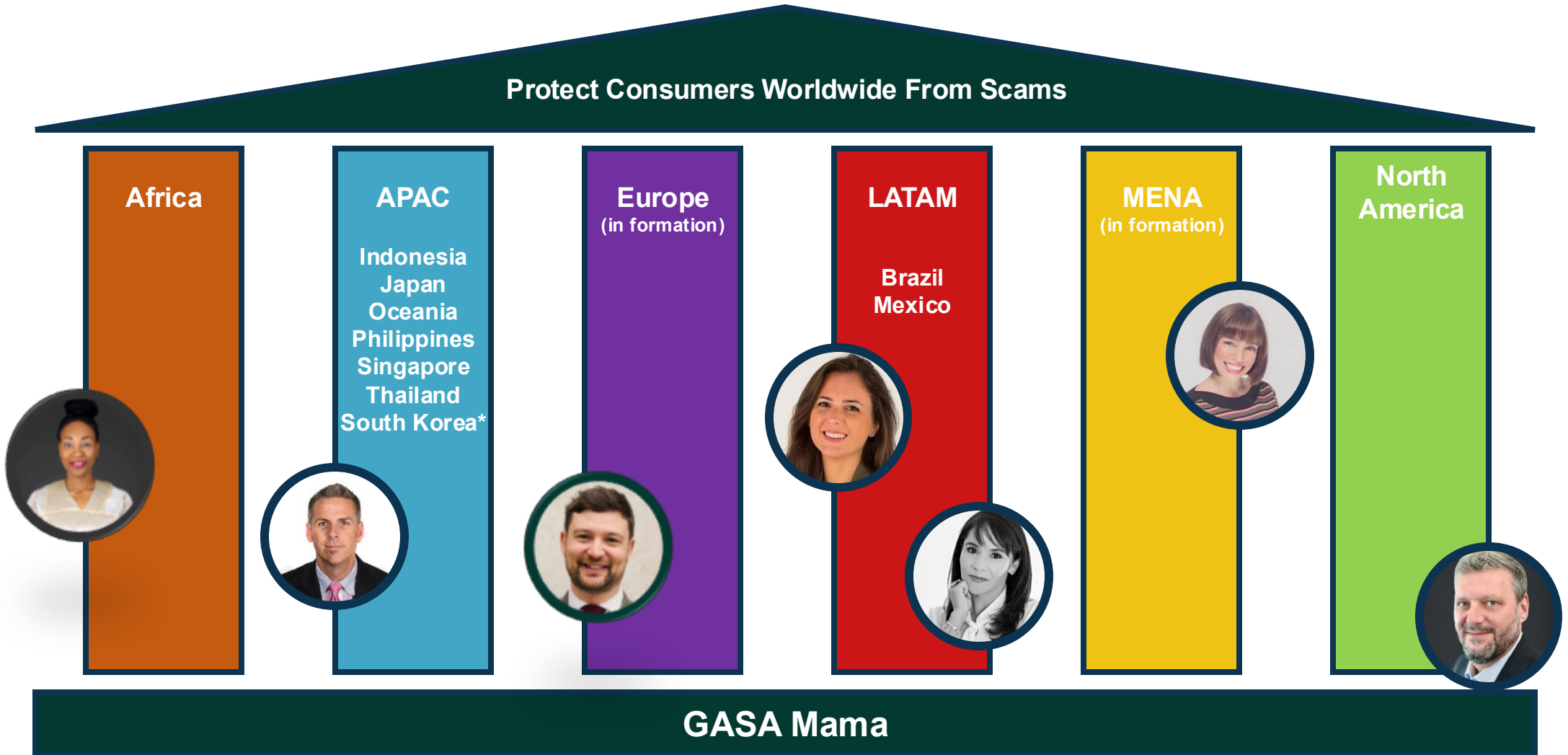
Solutions

- Scam.org
- SpotScam.org
- Global Signal Exchange

We focus on 4 pillars...

GASA

In March GASA Africa was formally launched



* Associated Organizations

GASA Europe will be launched on the 24th of September

Our Working Groups are global and cross-sectorial in nature



Consumer

(awareness, education, support)



Prevention & Intervention

(Raising the Bar to Scam)



Enforcement

(Catching The Scammers)



Research

(State of Scam Survey, Scam Typology)



Finance

(Monitoring, Money Mules)



Intelligence Sharing

(GSE, Privacy vs Crime)

A Working Group can have multiple knowledge sharing, policy or research projects which can turn into permanent solutions like the GSE and Scam.org

GASA

The State of Scams in America: New Data, Global Context



Jorij Abraham

Managing Director
Global Anti-Scam Alliance



Chris Willis

Chief Marketing Officer
Outseer



Paige Schaffer

Chief Executive Officer - Global
Identity & Cyber Protection
Iris® OnWatch

Who we spoke to across the globe

Sample size | 58,900 people

Audience | Adults aged 18+ living in 42 countries across the globe

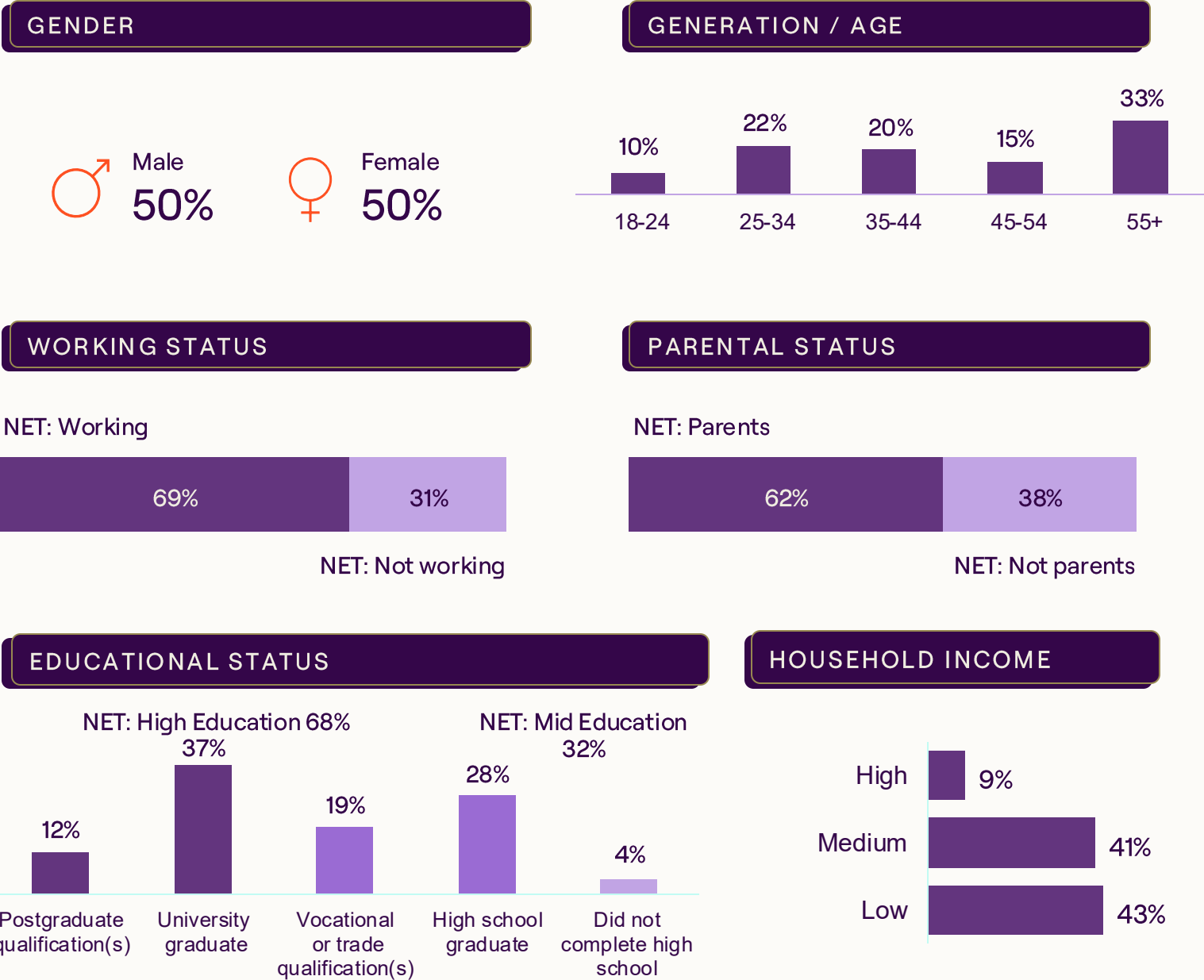
Weighting | Nationally representative of each country in study for adult population on age, gender and region

Methodology | 15-minute online survey

Sample source | Online research panel

Fieldwork | 16th March – 13th April 2026

Base: All respondents – Global (n=58,900)





58,900
42 countries
Among global adults



3,110
Among US adults



1,160
Among CN adults

75%
(125 encounters p.p.)

**encountered a scam
in the last year**

82%
(347 p.p.)

84%
(201 p.p.)

35%

**Interacted with the
scammer**

43%

35%

9%

Had money stolen

9%

6%

Among those who lost money

21% Police
27% Bank/PSP
29% Friends & Family

**Reported to
authorities**

Among those who lost money

Police	12%	19%
Bank/PSP	33%	30%
Friends	25%	17%



OnWatch

OUTSEER

North Americans are notably more confident in their ability to recognise scams



69%



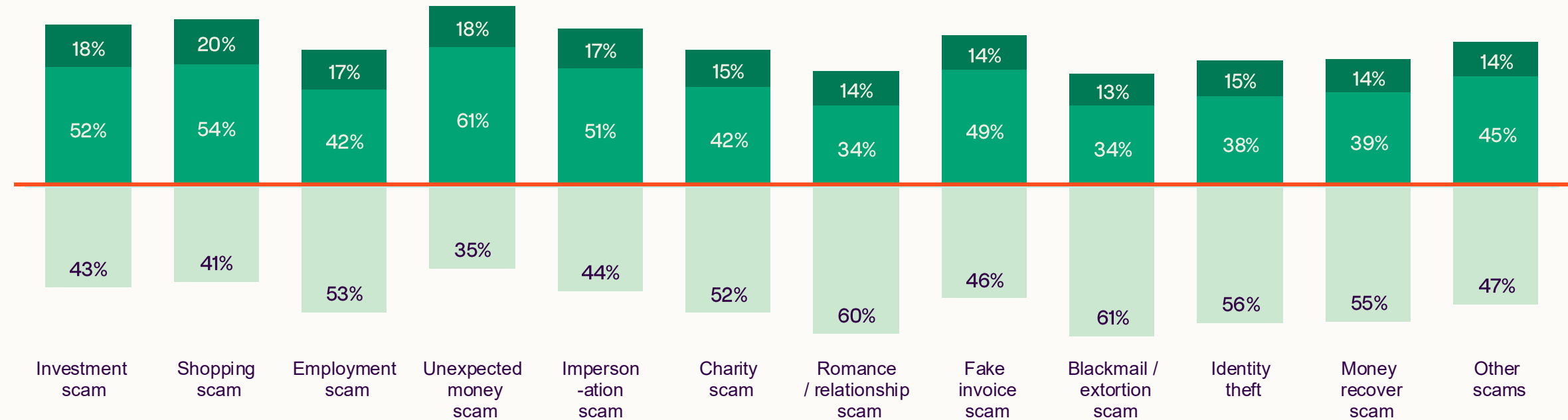
86% ↑



88% ↑

Globally, adults most commonly interact with shopping scams, followed by investment and unexpected money scams

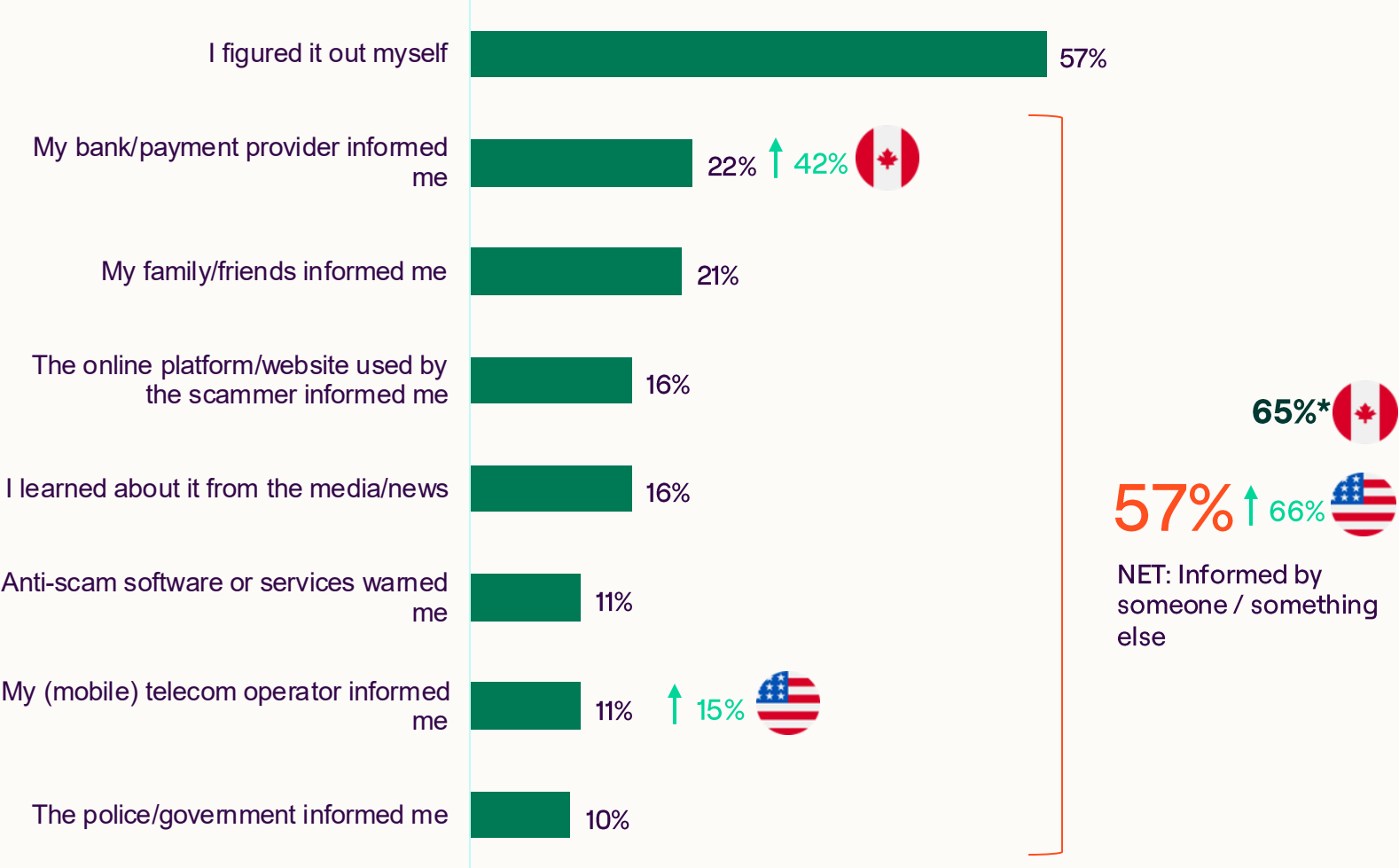
Global Level of interaction with scams in the last 12 months



Q6. Scams are becoming increasingly sophisticated, meaning anyone could be affected. Between 2024 and 2025 it is estimated that 202.3 billion people interacted with scam encounters. We'd like to understand how, if at all, you interacted with scams you encountered in the last 12 months. Interacting with a scam can range from simply opening or reading a message to replying, picking up a call, clicking links, visiting fake websites, or engaging in back-and-forth communication. You said you experienced scam encounters in the last 12 months. To what extent, if at all, did you interact with the following types of scams? Answer based on your interactions with the scammer before you 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 (global n=37473)

Canadian and American scam victims more frequently discover they've been scammed after being informed

How victims discovered they were scammed



 Significantly higher/lower

Q11. How did you discover you were scammed? Continue to think about the times you've been scammed and lost money in the last 12 months Base: All respondents that lost money to a scam (n=5390; Canada (n=70); USA (n=280) ~ * due to base size N70 in Canada, the value of 65% is not statistically significantly higher at 95% confidence interval.

All our reports can be downloaded from **GASA.org**



Download all Reports

The global report will be released mid November



Changing the Game: What's Actually Working in Consumer Education for Scam Prevention

**GLOBAL ANTI-SCAM
SUMMIT** **AMERICA
2026**



Brian Cute

CEO
Global Cyber Alliance



Chris Apple

Principal Architect & Product
Manager - AI & Cyber Security
Solutions
Global Cyber Alliance



Adam Eads

Senior Program Manager
TechSoup



How to Keep 400 Million Micro & Small Business Safe

September 2026 - Global Anti-Scam Summit America

The Challenge for Under-Resourced MSMEs

- ▶ The speed and increasing effectiveness of genAI and deepfake enabled scams
- ▶ The vast majority of 400M MSMEs globally are unprepared and unprotected
- ▶ A response that delivers scam prevention at scale and speed is required
- ▶ **Collaboration and concerted effort** is the only way the scam defense community can effectively address the threat - *no one organization can solve this problem*

Scam Prevention for Under-Resourced MSMEs

The Current Approach

Train-the-trainer approach

- Time required: multiple year projects
- Process steps: extensive and iterative across a number of organizations
 - ▶ creating appropriate curriculum
 - ▶ localizing and contextualizing curriculum
 - ▶ train-the-trainer guides
 - ▶ training-the-trainers
- Current Reach – 10s of thousands to 100s of thousands
- The Model – one-off training sessions

Doesn't scale fast enough.

Lack of evidence that awareness raising alone is creating desired impact.

Awareness Raising is Not Enough. Now What?

-
- ▶ Teaching someone to spot one phishing email is skill building, and it has a short shelf life against genAI-enabled scams
 - ▶ But there is a prior question: does the user even know the risk is out there?
 - ▶ In the physical world we manage risk constantly and mostly unconsciously. Where we park, which route we walk, how we secure our home
 - ▶ In the digital world that instinct is missing for the vast majority. Most people are not under-trained, they are under-sensitized
 - ▶ When risk is invisible, the typical response is not caution, it is avoidance. Mild panic, then head in the sand
 - ▶ Risk rejection is not a strategy, but it is what most people are doing today

Awareness of Risk Creates the Demand

- ▶ Every intervention, tool, or training still depends on someone choosing to use it. That choice is a real bottleneck that needs to be addressed
- ▶ People act when they can see themselves in the consequences. Without that, security guidance lands as a chore and gets deferred
- ▶ "Inventory your systems" is a task nobody wants. "I could lose access to everything I need to operate" is a reason to build the inventory
- ▶ Distribution puts a tool in front of tens of millions. Felt risk is what gets them to open it, finish it, and come back three months later
- ▶ This is the demand side of the scale problem, and no tool can build it alone

The Change That is Needed

- ▶ Scale
- ▶ Automating process steps
- ▶ Delivering training and tools that provide operational protection with fit-for-purpose and secure agents

The Shift in Approach to Delivering Protection

Traditional Capacity Building	Continuous Scam Protection
Train-the-Trainer	AI-Powered Platform
Localized Curriculum	Personalized Guidance
Toolkits	Operational Scam Protection
Trusted Implementation Partners	Trusted Distribution Partners
Thousands Reached	Millions Reached

Collaboration and Collective Action

Phase 1

- ▶ Leveraging agentic AI - the need to test, pilot, learn, iterate, rinse, repeat (rapidly)
- ▶ The need for collaboration and human-in-the-loop in the early stages - feedback loops on end users' interaction with the agent, performance of the tool, and actions taken
- ▶ In parallel, collaborative work on expanding the distribution system - engagement with online service providers to align incentives
- ▶ Need for catalytic investment in the early stages

Collaboration and Collective Action

Phase 2

-
- ▶ Expand the distribution system:
 - ISPs, domain name registries and registrars, foundations have incentives to put prevention tools in the hands of their customers and grantees
 - Service providers who have a public interest mindset: country code Top Level Domain operator (ccTLDs)
 - Governments who work closely with their ccTLD operator and who prioritize scam prevention for small businesses in their countries
 - ▶ Learn, iterate, and improve to deliver fit-for-purpose and secure agents that deliver at global scale
 - ▶ Information sharing about AI learnings among tool developers, particularly those who develop “public interest” tools.



GCA's AI-guided scam-defense solution assesses, trains, and assists each person to safety: open-source and self-hostable, multilingual, and sector-tailored.

PROTECT YOURSELF FROM ONLINE SCAMS

 globalcyberalliance.org/scamsafe



The ScamSafe Method

Assess

An Assessment Agent runs a short, plain-language self-check that gives each person a clear maturity picture for their situation.

Train

Based on the assessment, the agent directs the user to specific relevant training, drawn from GCA's courses and free tools.

Support

The agent supports users through and beyond that training, answering questions in natural language.

Thank You!



GLOBAL
CYBER
ALLIANCE™