CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

PROTECTING CONSUMERS FROM ONLINE SCAMS

A Global Action Agenda

CALL TO ACTION

Online scams are increasing rapidly in scale, sophistication and impact, putting millions of people at risk every day. In 2019, we warned that coordinated action was needed to prevent an online scams crisis.[1] While progress has been made, efforts remain fragmented, with many regions struggling to modernise rules and strengthen enforcement.

Without urgent and collaborative action, the consequences for consumers and markets will be severe. That's why we are calling on the international community to unite behind our **Global Action Agenda** - a set of core principles and a checklist of policy actions that together will strengthen consumer protection, safeguard economies, and enhance trust in digital systems.

Global solutions are vital, but they can only succeed if every nation plays its part. Building strong national foundations - strategies, rules and infrastructure - is the essential first step. Consumers International members urge governments - policymakers, ministries, regulators and law enforcement agencies - to take the lead.

1 Consumers International, 'Social Media Scams: understanding the consumer experience to create a safer digital world' 2019 - https://www.consumersinternational.org/media/604472/social-media-scams-final-245.pdf

WHY ACTION IS URGENT

THE GROWING THREAT OF ONLINE SCAMS

Online scammers don't break into systems; they manipulate people into authorising payments themselves. Digital technology has made that easier than ever:

- **Reach:** From lone individuals to global crime networks, scammers exploit digital channels - such as social media, marketplaces, email and messaging apps - to reach billions of potential victims.

- **Realism:** Scam tactics are increasingly sophisticated. AI tools such as deepfakes, voice clones, and synthetic IDs allow criminals to impersonate organisations - such as government agencies, banks or retailers - or even loved ones, applying psychological pressure to push people into acting fast.

The result is that online scams now spread faster and look more convincing, making it much harder for consumers to know who to trust.

THE HUMAN IMPACT

Anyone can be a potential victim, although some groups - such as children or others in vulnerable circumstances - may be at greater risk of harm. In 2023, 78% of consumers worldwide encountered at least one scam attempt, and one in four lost money.[2]

The consequences can be devastating, with people losing their homes or life savings. In 2024, global consumer losses reached $1.03 trillion - and the real figure is believed to be far higher, since 93% of scams go unreported. Even when victims do speak up, only 4% get their money back.[3]

The damage is not just financial. Victims often experience stress, shame, guilt and serious mental health impacts. Many lose confidence in digital life or withdraw altogether, risking digital exclusion. When consumers lose trust in online platforms or payment systems, businesses face financial losses and reputational damage - costs that can cascade across national and global economies.

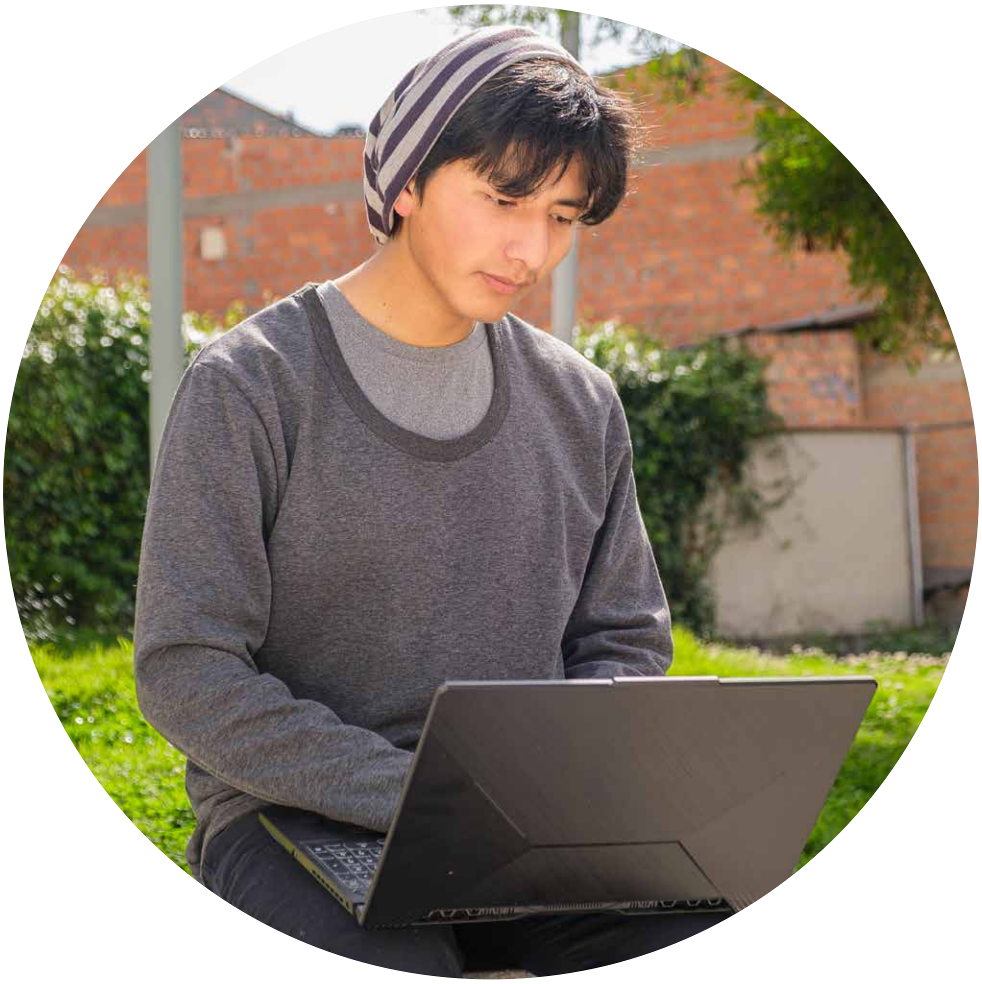
2 Global Anti-Scam Alliance (GASA), 'Global State of Scams 2023'
3 Global Anti-Scam Alliance (GASA), 'Global State of Scams 2024', (countries show some variation)

PROTECTING CONSUMER RIGHTS ONLINE

The United Nations Guidelines for Consumer Protection[4] state that consumers have a right to safety, information, inclusivity and redress when interacting with organisations – whether offline or online. However, in digital environments, weak rules, remote services, and powerful companies can put people at a disadvantage.[5]

To deliver positive impact, measures to tackle online scams must recognise real consumer experiences and enhance protection throughout the scam lifecycle. For example, consumers have a right to expect:

- Effective protection from scams
- Clear information and practical safeguarding tools
- Swift action to reduce harm when scams occur
- Fast and fair redress when they experience harm



4 United Nations Guidelines for Consumer Protection (UNGCP) - https://unctad.org/topic/competition-and-consumer-protection/un-guidelines-for-consumer-protection

5 https://www.oecd.org/en/publications/consumer-vulnerability-in-the-digital-age_4d013cc5-en.html

A GLOBAL ACTION AGENDA

CORE PRINCIPLES

Protecting consumers in this fast-changing landscape requires harmonised global efforts, underpinned by strong national action. Governments must build strategies, infrastructure, and partnerships that support effective cross-border solutions. The following three core principles provide the foundation for a robust and consistent national approach:

1. **Build and strengthen national anti-scam frameworks**
2. **Unite stakeholders for coordinated protection**
3. **Drive global cooperation to protect consumers**

---

1. BUILD AND STRENGTHEN NATIONAL ANTI-SCAM FRAMEWORKS

WHY?

Government leadership is essential to set direction, coordinate action and drive improvements. Every country needs a clear anti-scam strategy that reflects its own circumstances but aligns with global best practice and standards.

HOW?

- ✓ Create a National Strategy that defines goals and sets out a roadmap for tackling online scams. Include annual targets, public dashboards and transparent progress reporting.
- ✓ Allocate sufficient resources to relevant agencies to enable operation.
- ✓ Establish a national Anti-Scam Authority to oversee the response, with powers to coordinate relevant government departments, law enforcement, regulators and consumer agencies.
- ✓ Ensure national legislation includes clear rules and accountabilities for key stakeholders *(See 'Glossary' on page 10)*.

---

2. UNITE STAKEHOLDERS FOR COORDINATED PROTECTION

WHY?

Consumers have complex lives - interacting with multiple organisations across sectors every day. All relevant stakeholders in the digital ecosystem must play their part, working together to tackle scams, improve practices and deliver effective protection.

HOW?

- ✓ Create a National Task Force to convene stakeholders, share insight and shape strategy.
- ✓ Maintain targeted and valuable communication, offering regular opportunities to engage.

3. DRIVE GLOBAL COOPERATION TO PROTECT CONSUMERS

WHY?

Online scams spread quickly across borders,[6] so it is vital that national strategies connect with wider global systems to protect people wherever they live. Building international partnerships is key to a strong and coordinated global response.

HOW?

- ✓ Work with other nations to share learning and build effective systems for data sharing, enforcement and cross-border cooperation.
- ✓ Support the development and adoption of international standards that help prevent scams, through engagement with the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).[7]
- ✓ Engage with intergovernmental policy and enforcement bodies such as the UN, OECD, INTERPOL and ICPEN to strengthen global efforts to prevent, detect and respond to online scams.[8]

6 For example, the OneCoin crypto scam 2014-2019 where investors across Europe, Asia, Africa and the Americas lost billions.

7 International standards related to managing risks across digital systems include: information security (ISO/IEC 27001, 27002), privacy and data protection (ISO/IEC 27701), and digital identity and verification (ISO/IEC 24760, 29115, 18013-5). Further information: www.iso.org and www.iec.ch.

8 OECD's Consumer Protection Enforcement in a Global Digital Marketplace (2018) report: https://www.oecd.org/en/publications/consumer-protection-enforcement-in-a-global-digital-marketplace_f041eead-en.html

ACTION CHECKLIST

Each country experiences scams differently and faces its own challenges. While there is no single solution, all governments can take practical steps to protect their citizens and contribute to a stronger, more coordinated global response. Our checklist sets out priority actions under four pillars to help governments:

- Benchmark existing measures and identify gaps
- Target the channels and systems exploited by online scammers
- Strengthen cross-sector partnerships
- Contribute meaningfully to global cooperation

PREVENT & DISRUPT

What consumers say:	***"Scams are everywhere - ads, emails, message – it feels impossible to deal with this by myself"***
Goal:	**Stop scams before they reach consumers**

✓ **Secure communications and data:** Ensure strong regulation for safe communication channels (email, SMS and other digital notifications) and robust data handling (cybersecurity) to protect consumers' privacy and personal information.

✓ **Platform accountability:** Ensure laws require online platforms to prevent scam content within their environments - by verifying users and advertisers, and pre-approving listings - and swiftly remove scam content if it appears. Platforms should be transparent about the measures they are taking and collaborate to disrupt cross-platform scams.

✓ **Secure payment systems:** Work with payment service providers and online businesses to embed safeguards such as multi-factor authentication, passkeys, and require regular system reviews.

✓ **Global disruption:** Share intelligence across borders to dismantle scam networks, license and audit bulk-messaging hubs, and establish joint takedown pipelines for removal of transnational scam infrastructure.

EMPOWER & DEFEND

What consumers say:	*"I don't know how to protect myself from scams or where to get reliable information"*
Goal:	**Equip consumers with the knowledge and tools to identify and resist scams**

- **Education campaigns:** Run timely, accessible campaigns, backed by interactive resources, that raise awareness of how to identify and protect against current scams. Target outreach to high-risk groups (such as older people and young adults) while reducing stigma and encouraging reporting.
- **One-stop guidance:** Provide a national consumer portal with clear, consistent scams advice, linked across sectors, online platforms and businesses.
- **Certification:** Develop schemes by sector (e.g. financial services, retail, telecoms) that verify authenticity of businesses and providers. These should be easy to use, helping consumers to make informed decisions and improving trust.
- **Payment friction:** Work with payment service providers to build safeguards that give people time, information and choice before completing a transaction. For example, confirmation-of-payee checks and real-time warnings on suspicious activity.
- **Global messaging:** Share scam intelligence internationally so that new threats detected in one region - such as a fake celebrity crypto endorsement - trigger rapid global alerts.

REPORT & ACT

What consumers say:	*"I don't know where to report a scam, or if it will make any difference"*
Goal:	**Act quickly when scams are reported to limit consumer harm**

- **One-stop reporting:** Provide a single national portal for consumers to report scams - integrated into browsers, online platforms and digital communication providers - that links into a national scams database.
- **Real-time response:** Establish a 24/7 inter-agency scams intelligence hub that collates insight from all sectors and connects relevant stakeholders to take swift and appropriate action.
- **Data sharing:** Establish clear legal frameworks that enable businesses to share relevant data safely with governments, law enforcement and trusted partners to help protect consumers.
- **Rapid investigations:** Ensure consumer reports trigger instant checks, freezes or investigations, as appropriate.
- **Cross-border enforcement:** Secure international agreements for joint investigations, takedowns and enforcement actions.

CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

RECOVER & DETER

What consumers say:	***"I don't know who is responsible - and have little confidence in getting my money back"***
Goal:	**Support victims, recover losses and hold those responsible to account**

- ✓ **Consumer redress:** Clearly communicate rights and responsibilities and provide accessible complaint channels. Ensure prompt resolution through mandatory redress schemes that place responsibility on those best positioned to manage fraud risks within the digital ecosystem. For example, telecoms companies, online platforms and payment service providers.

- ✓ **Consumer support:** Provide access to specialist help, such as financial advice, mental health support or other recovery services.

- ✓ **Accountability:** Ensure transparent reporting on compliance, apply penalties where organisations fail to protect consumers, and develop mechanisms for coordinated enforcement across borders.

- ✓ **Global recovery:** Harmonise scam categories and establish reciprocal agreements to recall or freeze funds across borders.

LOOKING AHEAD

By embedding the core principles across all areas of policy and practice, and working through our checklist, governments can make a meaningful contribution to reducing the scale and impact of online scams worldwide.

Successful and coordinated implementation of these measures at national level will amplify global impact – strengthening consumer protection, safeguarding economies and enhancing trust in digital systems, enabling people to navigate their digital lives with confidence.

GLOSSARY

Online scams
Online scams are a type of fraud where criminals use digital channels (such as websites, apps, social media, email, messaging, phone/SMS) to manipulate or deceive individuals into authorising payments, in good faith, to a recipient reasonably believed to be a legitimate payee.

Key stakeholders
Relevant stakeholders in the digital ecosystem may include government agencies, regulators, law enforcement, consumer organisations and industry, such as telecom companies, online platforms and payment service providers.

Online platforms
Digital multi-sided intermediaries that enable interactions among user groups (producers/consumers). Different types of online platforms include social networks and content sharing, online marketplaces, communications and messaging.

Payment service provider (PSP)
A third-party company that acts as an intermediary between consumers and merchants, enabling electronic payments. For example, credit/debit cards, bank transfers, digital wallets.

CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

SIGNATORIES

The Consumer Coalition to Stop Scams was created at the Consumers International Global Congress 2023. Led by Consumers International, it comprises 40 consumer organisations, businesses and consumer protection authorities.

The Global Action Agenda is endorsed by the following organisations:

Acción del Consumidor (Argentina)

Alliance of Digital Finance and FinTech Associations

Benin Santé et Survie des Consommateurs (Benin Health and Consumers' Survival)

CHOICE (Australia)

Consumer Council of Fiji

Consumentenbond (Netherlands)

Consumer Council of Zimbabwe

Consumer Education and Research Centre (India)

Consumer NZ (New Zealand)

Consumer Reports (United States)

Consumer VOICE (India)

Consumers Council of Canada

Consumers Organisation of Macedonia

Federation of Malaysian Consumers Associations

Myanmar Consumers Union

Siphosethu Consumers for Development Cooperative Ltd (South Africa)

Sudanese Consumers Protection Society

Which? (United Kingdom)

Consumers Association of Singapore

Consumers Korea

ERA Consumer Malaysia (Education and Research Association for Consumers)

Instituto Brasileiro de Consumidores e Titulares de Dados (Brazil)

Fédération des Associations de Consommateurs de Côte d 'Ivoire (National Federation of Consumer Associations of Ivory Coast)

Tec-Check Digital Consumers Organization (Mexico)

Yemen Association for Consumer Protection

ACKNOWLEDGEMENTS

This document was developed by Consumers International with guidance and input from a multi-stakeholder Working Group, drawn from members of the Consumer Coalition to Stop Scams. Participating organisations are listed below.

We thank all contributors for their valuable insight and feedback, while noting that the recommendations presented here do not necessarily reflect the individual views of all organisations in the Working Group.

ORGANISATION	COUNTRY
Accion del Consumidor (ADELCO)	Argentina
Amazon.com, Inc.	Global
Brazilian Institute of Consumer Protection (IDEC – Instituto Brasileiro de Defesa do Consumidor)	Brazil
Consumer Council of Fiji	Fiji
Consumer VOICE	India
Consumers Council of Canada	Canada
Protection and Consumer Protection Foundation of the State of São Paulo (PROCON SP – Fundação de Proteção e Defesa do Consumidor do Estado de São Paulo)	Brazil
Myanmar Consumers Union	Myanmar
PayPal, Inc.	Global
Smart Consumer Institute	Slovakia
Tec-Check Mexico	Mexico
Visa, Inc.	Global