CONSUMERS INTERNATIONAL

COMING TOGETHER FOR CHANGE

STOPPING ONLINE SCAMS: BUILDING CONSISTENCY AND COORDINATION FOR CONSUMERS

March 2026

EXECUTIVE SUMMARY

"Scams are everywhere – ads, emails, message – it feels impossible to deal with this by myself"

"I don't know how to protect myself from scams or where to get reliable information"

"I don't know where to report a scam, or if it will make any difference"

"I don't know who is responsible – and have little confidence in getting my money back"

Versions of these sobering statements are made the world over by consumers who have been exposed to online scams. They are heard daily by the 200 members of Consumers International – the consumer advocacy organisations that fight on behalf of all of us to make sure that the scourge of online scams is eradicated for good. By stopping scams before they reach consumers. By equipping people with the knowledge and tools to identify and resist scams. By making sure that businesses and authorities act quickly once a scam is reported to limit more harm. And by supporting victims, recovering losses and holding those responsible to account.

Online scams are increasing at an alarming pace. Consumers bear the brunt, suffering financial and emotional damage. The effects cascade across national and global economies, as more money gets channelled to criminal purposes and trust in the digital and financial systems wanes. Despite broad agreement on the need for urgent action, efforts are often fragmented, necessitating a coordinated global response to address scams (INTERPOL, 2025).

Through its Consumer Coalition to Stop Scams ("the Coalition"), Consumers International convenes 40 consumer groups, businesses and consumer protection authorities in 30 countries to connect the lived consumer experience of scams with the systems and decision-makers shaping the global response. The Coalition is the only global initiative built with consumer representatives that is dedicated to tackling online scams.

What does a strong global response look like? In our view, it requires **consistency** and **coordination**. Consistency, because while a global response is clearly needed, it can only succeed if every nation plays its part. Building strong national foundations that meet a strong and equal minimum standard is the essential first step. And coordination, because it is vital that national strategies connect with wider global systems to protect people wherever they live. Building international partnerships that involve all relevant stakeholders in the digital ecosystem, and which ultimately target and dismantle the organised crime networks behind online scams, is therefore just as important.

In 2025, a Working Group of the Coalition helped Consumers International define the specific actions that will meaningfully change the scam environment for consumers – from detection and disruption through to accountability and recourse. Consumers International produced *A Global Action Agenda to Protect Consumers from Online Scams* ("the *Global Action Agenda*") with a self-assessment checklist across four pillars: Prevent and Disrupt, Empower and Defend, Report and Act, Recover and Deter – helping stakeholders benchmark progress, identify gaps and prioritise next steps in their own jurisdictions. The four-pillar checklist shows the national policies and regulations that consumer representatives say are required – the **consistency** – and is accompanied by a corresponding global action – the **coordination** – that contributes meaningfully to global cooperation against scams.

With endorsement from 25 leading national consumer associations around the world, the *Global Action Agenda* can be considered an authoritative representation of the minimum expectations that consumer representatives have around what constitutes a strong global policy response. Naturally, other frameworks could be used.

Although primarily directed at governments, the *Global Action Agenda* emphasises the roles and responsibilities of multiple actors within the scam ecosystem. Indeed, a complete and effective response to online scams must extend beyond formal regulations to include, for example, informal and voluntary coordination structures between stakeholders, infrastructure and mechanisms for data sharing, capabilities and incentives to perform advanced detection, and meaningful enforcement against criminal activity.[1]

A global policy scan

At the same time, without a measure of whether consumer advocates' minimum expectations for policy and regulations are met, it is difficult for stakeholders to assess the state of, and push for improvements in, national and international responses to scams, whether formally or informally.

To this end, this report focuses primarily on reviewing policymaker-driven measures to combat online scams against the four pillars of the *Global Action Agenda*. Looking at 28 jurisdictions, it attempts to do so by evaluating both the extent to which a measure aligns with the checklist item, as well as the *level of implementation* of that measure.[2]

1 There are national, regional and global organisations undertaking efforts on behalf of consumers to prevent, detect and respond to online scams. Some of these organisations convene in forums where governments, regulators, industry players and civil society actors exchange experiences, share initiatives, and explore innovative approaches to preventing consumer harm. Such forums include, but are not limited to, the United Nations Office on Drugs and Crime's (UNODC) Global Fraud Summit, summits of the Global Anti-Scam Alliance (GASA), and thematic scam-related meetings organised by the United Nations Conference on Trade and Development (UNCTAD) and the Organisation for Economic Cooperation and Development (OECD).

2 See Annex 1, for further details on Methodology. The policy scan was conducted between September and December 2025. All reasonable efforts have been made to check for accuracy and completeness in the 28 jurisdictions covered, including a subsequent review by trusted national consumer associations, government agencies, and independent and private sector experts in consumer protection. This is fast-moving area, and how scams are treated and defined at the jurisdictional level varies, which requires a necessary element of subjectivity in assessment. We encourage interested parties to contact us at impact@consint.org to discuss any queries.

Assessing the ultimate effectiveness of the measures identified is not in scope for this report; in fact, their mere existence does not guarantee a reduction in consumer harm.[3] However, by highlighting promising approaches, gaps and lessons in different countries, the report complements the *Global Action Agenda* to offer both a diagnostic and illustrative tool for what might lead to progress.

Consumers International recognises that the burden on governments is high, and expectations to protect consumers from online scams exist within a dynamic and complex digital environment. It is easy to say, for example, that transnational criminal enterprises should be dismantled, or that scams intelligence should be shared across borders. The capacity and resources of governments to respond in practice, however, is variable. Together with our global network of 200 consumer organisations around the word, we stand ready to support the various government agencies that are being called on to act, and will continue to advocate for meaningful, appropriate and ongoing resources to be directed accordingly to help them.

A spread of approaches under each pillar

The scan of policies show that policymakers in all jurisdictions have taken some action under all four pillars, but approaches differ widely, and implementation is often incomplete. To put it bluntly, the **consistency and coordination** required is falling short.

Across a diverse sample of 28 jurisdictions, we observed that, against the checklist in our *Global Action Agenda*:

1) In the Prevent and Disrupt pillar, the greatest coverage relates to requirements for secure communication and data, where all 28 jurisdictions have measures that concord with this item on the checklist. Positively, 23 of those 28 have complete concordance, and 17 of those 23 have implemented those requirements fully. The biggest gap is in the obligation for online platforms to prevent scam content from appearing within their environments. Although 17 jurisdictions have at least some measures in place to require this, only six have fully implemented them, and there remain 11 jurisdictions with no measures at all.

2) In the Empower and Defend Pillar, the greatest coverage relates to education campaigns. All 28 jurisdictions have some measure in place for this, and 16 of 28 of those measures concord with the expectations in our checklist. There are two areas showing large gaps. At the national level, ten jurisdictions do not have national portals with clear, consistent scams advice that links across sectors and platforms. At the global level, there is an equivalent gap of ten jurisdictions that do not have any measures to share scam intelligence internationally in order to trigger global alerts.

3 For example, BEUC, the European Consumer Organisation, notes that the existence of frameworks specifying redress mechanisms does not mean consumers always get reimbursed when they are victims of fraud. In the European Union, fraud victims still bear 85% of the financial losses despite there being rules in place. See more: https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202512.en.pdf.

3) In the Report and Act pillar, it is positive to see that, in 27 of the 28 jurisdictions, there are legal frameworks that enable businesses to share relevant data safely with governments, law enforcement and trusted partners to protect consumers. However, only four of those 27 fully align with our checklist, and 15 of them are yet to progress to full implementation. The notable gap in this pillar is in the presence of one-stop reporting centres that feed into national scams databases. Here, only 12 have any concordance with the checklist, and among those, two jurisdictions have yet to fully implement their measures.

4) In the Recover and Deter pillar, there is a significant gap in the presence of reciprocal agreements to recall or freeze funds across borders. Only one country has some concordance with our checklist on this measure, and it has not been fully implemented. In addition, only seven of the sample country frameworks include consumer redress mechanisms that specifically provide redress for scams, although, reassuringly, broader consumer redress mechanisms exist in most countries. Almost all jurisdictions (26) provide access to specialist help, such as financial advice, mental health support or other recovery services, for victims of scams.

Four imperatives for consistency and coordination

Acknowledging that a successful strategy to combat scams requires a whole-of-society response, including effective law enforcement and a combination of non-regulatory actions by multiple stakeholders, this assessment identifies four gaps for governments[4] that support a consistent national and a coordinated global response to online scams. These are:

1. Requiring online platforms to prevent scam content from appearing within their environments.

2. Creating a national consumer portal with clear and consistent advice across sectors, as well as one-stop reporting centres that feed into national databases.[5]

3. Developing international coordination mechanisms to share scam intelligence and trigger alerts across borders, as well as cross-border agreements to recall or freeze funds when scam activity is suspected.

4. Assessing whether existing consumer redress mechanisms appropriately provide redress for scams.

4 The authority taking the lead may differ across jurisdictions, depending on institutional structures and consumer protection approaches.

5 Given the link between education and reporting, these gaps could potentially be addressed together.

CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

CONTENTS

List of Figures

List of Boxes

1. INTRODUCTION

Scams are increasingly common and sophisticated. Online scams are a type of fraud in which highly coordinated criminal organisations, often relying on trafficked and forced labour, use sophisticated methods through digital channels[6] to manipulate or deceive individuals into authorising payments, in good faith, to a recipient reasonably believed to be a legitimate payee.

This 'authorised push payment fraud' is spreading rapidly worldwide and global losses are projected to reach $331 billion by 2027 (LSEG Risk Intelligence, 2025). To this is added severe psychological and emotional distress (Innovations for Poverty Action, 2025).

Increasingly, Artificial Intelligence (AI) is referenced in the context of online scams and presents a double-edged dynamic. It may support stronger detection, monitoring, and risk-analysis that can help identify fraud patterns earlier and at scale. At the same time, AI might enable criminals to create more convincing, automated and personalised attacks, increasing the sophistication and reach of fraud risks (Duflos, 2025).

Isolated businesses efforts are insufficient. In recent years, the landscape of scams has shifted profoundly due to changes in payment technology, global connectivity and evolving criminal tactics (Rogers, 2024). Online scams are a cross-ecosystem crime, with consumers often exposed to risk long before a payment is made to a criminal behind a scam, and various parts of the scams 'life-cycle', including telecoms providers, online platforms[7] and financial service providers are taking steps to prevent fraud and scams, increasingly in a coordinated way.[8]

Private sector actors have played a central role in developing many of the most advanced scam prevention tools. These efforts, while essential, all operate within an existing public policy framework, which could be considered as enabling structures that support and scale effective operational responses across sectors. In isolation, companies may still lack incentives or legal clarity to cooperate with others. Research shows that banks and payments providers optimise their own efforts, often yielding individual improvements but without mitigating overall market-wide impacts (Mosk, Balasubramaniam, & Uettwiller, 2025). Moreover, financial service providers owe a duty to their customers to carry out their instructions for authorised payments. Finally, online platforms, and particularly those focused on social media, may earn substantial advertising revenue from fraudulent or scam inducing content (Horwitz, 2025).

Governments – policymakers, regulators, ministries and enforcement agencies – must take the lead. Only governments can make and enforce the law, providing the kind of strong deterrence and accountability necessary to address scams. Governments can also change incentives for the private

6 Activity to manipulate consumers into authorised push payment scams can also originate via phone calls and text messages.

7 Online platforms are defined as 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. (Consumers International, 2025).

8 Some financial service providers undertake real-time scam checking and intervention, for example, Visa Scam Disruption Service and Mastercard Consumer Fraud Risk solution. Some telecommunications companies have developed codes to address spoofing, for example the Fraud Sector Charter: telecommunications, in the United Kingdom and the New Zealand Telecommunications Forum Scams Prevention Code. Some online platforms, including Amazon, use Artificial Intelligence (AI) to detect suspected fake online reviews, manipulated ratings and fake customer accounts before consumers see them.

sector – by lowering barriers to robust and effective scam prevention. In addition, governments alone have the authority to convene and compel cooperation across and between sectors at the national level, as well as access to multiple mechanisms to collaborate at the international level.

Increasing consumer losses and harm, along with the evolving digital landscape, mean that scams are front of mind for regulators and policymakers. Responses range from consumer education and consumer recourse, to enforcement, information sharing, and safeguards around instant payments. However, to date there has been no detailed analysis of the regulatory and policy responses to scams, and no clear understanding of the gaps.

While this report focuses on assessing whether consumer advocates' minimum expectations for policy and regulations are met or even present, it is noted that a complete and effective response to online scams must extend beyond formal legal measures once they are in place. Online scams are addressed through multiple policy lenses, including consumer protection, financial crime enforcement, cybersecurity and telecommunications regulation. In addition, the real-world challenges of governments are not to be underestimated: expectations on policymakers and regulators are high, and they operate in a dynamic and complex digital environment.

This report examines the issue primarily through the lens of consumer protection frameworks and cross-sector coordination. It therefore complements, rather than replaces, analyses focused on criminal enforcement or financial crime supervision.

What will it take to consistently evaluate and measure the incidence of scams?

Developing evidence-based guidance and tools for authorities and other stakeholders, such as consumer associations, is in CGAP's DNA. In 2022, we published a report presenting global evidence that fraud was a fast-growing risk for digital finance users. We have now completed new research on the recent evolution of digital finance consumer risks, which shows that the use of AI, the rise of organised crime, and the rapid exchange of consumer data are further increasing these risks.

In all the countries where we engage, we see market monitoring by financial sector authorities (and sometimes consumer associations) as essential to evaluate and measure the incidence of fraud, including scams. Our team has developed a comprehensive market monitoring toolkit to help identify and better understand fraud/scams, as well as to measure progress. In India, together with the Reserve Bank of India Innovation Hub and Decodis, we have tested social media monitoring using AI and successfully identified fraudulent digital credit apps. Nationally representative consumer surveys are the most comprehensive of these tools. We see them as an entry point to assess consumers' experiences and to understand the extent of the risk they face while using digital finance. CGAP surveys have now been conducted in six countries (Burkina Faso, Côte d'Ivoire, Niger, Peru, Rwanda and Senegal). All six surveys revealed that fraud and scams were very frequent and provided information on people's financial losses.

Having this kind of "measurement" is critical to taking action and measuring progress. As part of our responsible digital finance ecosystem project, we have supported authorities in these countries in designing action plans collaboratively to address these issues. In Côte d'Ivoire, ecosystem-wide action plan implementation has contributed to a notable reduction in losses from fraud among digital finance users (from 14% to 5% of users). We are designing several tools to reduce fraud and other consumer risks, including a paper to make digital credit more responsible.

Eric Duflos, *Consumer Protection Lead, CGAP*

Four pillars for global action. Consumers International, with support from a Working Group of its Consumer Coalition to Stop Scams, has created A Global Action Agenda for Protecting Consumers from Online Scams. The *Global Action Agenda* calls for governments to build and strengthen national anti-scam frameworks, unite stakeholders for coordinated protection and drive global cooperation to protect consumers. To support them in doing so, the *Global Action Agenda* includes a checklist of 18 measures that policymakers can drive to respond to the growing scams problem. With endorsement from 25 leading national consumer associations around the world, the *Global Action Agenda* can be considered an authoritative representation of the minimum expectations that consumer representatives have around what constitutes a strong global policy response. It is organised according to four pillars:

Prevent and disrupt: Stopping scams early, before they reach consumers, is key to maintaining consumer trust and confidence in digital and financial systems. This pillar covers actions such as securing communication channels, strengthening data protection, and ensuring platforms stops scam content within their environments. It also includes working with payment providers to build safer systems.

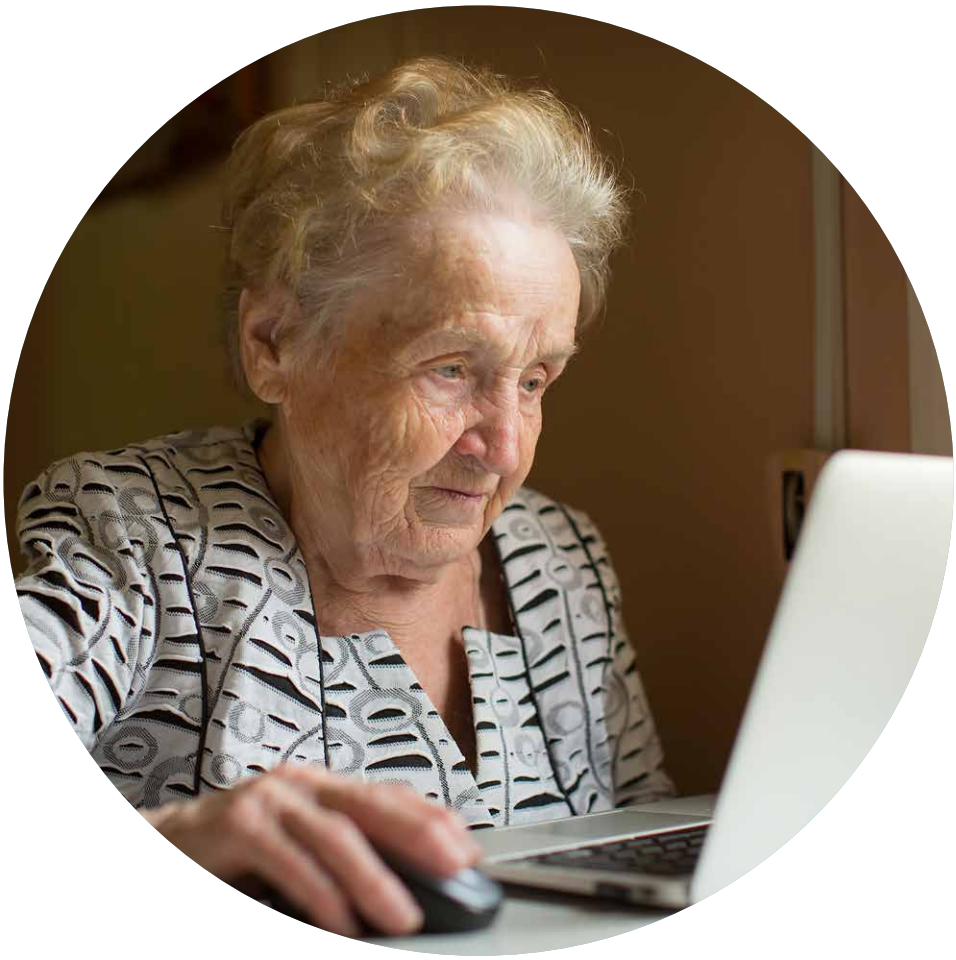
Empower and defend: This pillar refers to providing consumers with the knowledge, tools and confidence to recognise, avoid, and resist scams. It includes targeted awareness campaigns, a national portal with clear consumer guidance, easy ways to verify businesses, and sharing scam intelligence globally so people are warned early.

Report and act: Consumers should know where to report scams, and it is reasonable that they would expect swift, coordinated action to follow. The pillar covers national reporting portals, real time response hubs, safe data sharing between sectors, and rapid investigations – both nationally and across borders.

Recover and deter: What happens after a scam takes place is also important. This pillar focuses on supporting victims, recovering losses, and holding responsible parties accountable. It includes accessible complaint channels, fair redress schemes, and international cooperation to freeze or return funds.

Weighing up the scams response to identify priorities. This report analyses how 28 jurisdictions[9] at different levels of development and regulatory maturity are progressing to implement these priority measures.[10]

- Section 2 starts by providing a snapshot of what different jurisdictions are doing across the globe.
- Section 3 evaluates cross-jurisdictional progress towards implementation of the priority actions of the policy action checklist against each pillar.
- Section 4 sets out the key areas on which national action and international collaboration is needed.



9 Australia, Botswana, Brazil, Canada, Chile, China, Egypt, Eswatini, the European Union (EU), Ghana, India, Indonesia, Kenya, Malaysia, Mexico, New Zealand, Nigeria, Pakistan, Peru, Rwanda, Singapore, South Africa, Tanzania, Thailand, the United Arab Emirates (UAE), Uganda, the United Kingdom (UK) and the United States of America (USA).

10 See Annex 1 for more details on the research methodology.

2. GLOBAL STOCK TAKE: JURISDICTIONS ARE ACTING, BUT FROM DIFFERENT BASELINES

Figure 1 provides a global snapshot of common policy and regulatory responses called for by consumer advocates. The figure makes no evaluation of the individual effectiveness of these examples.

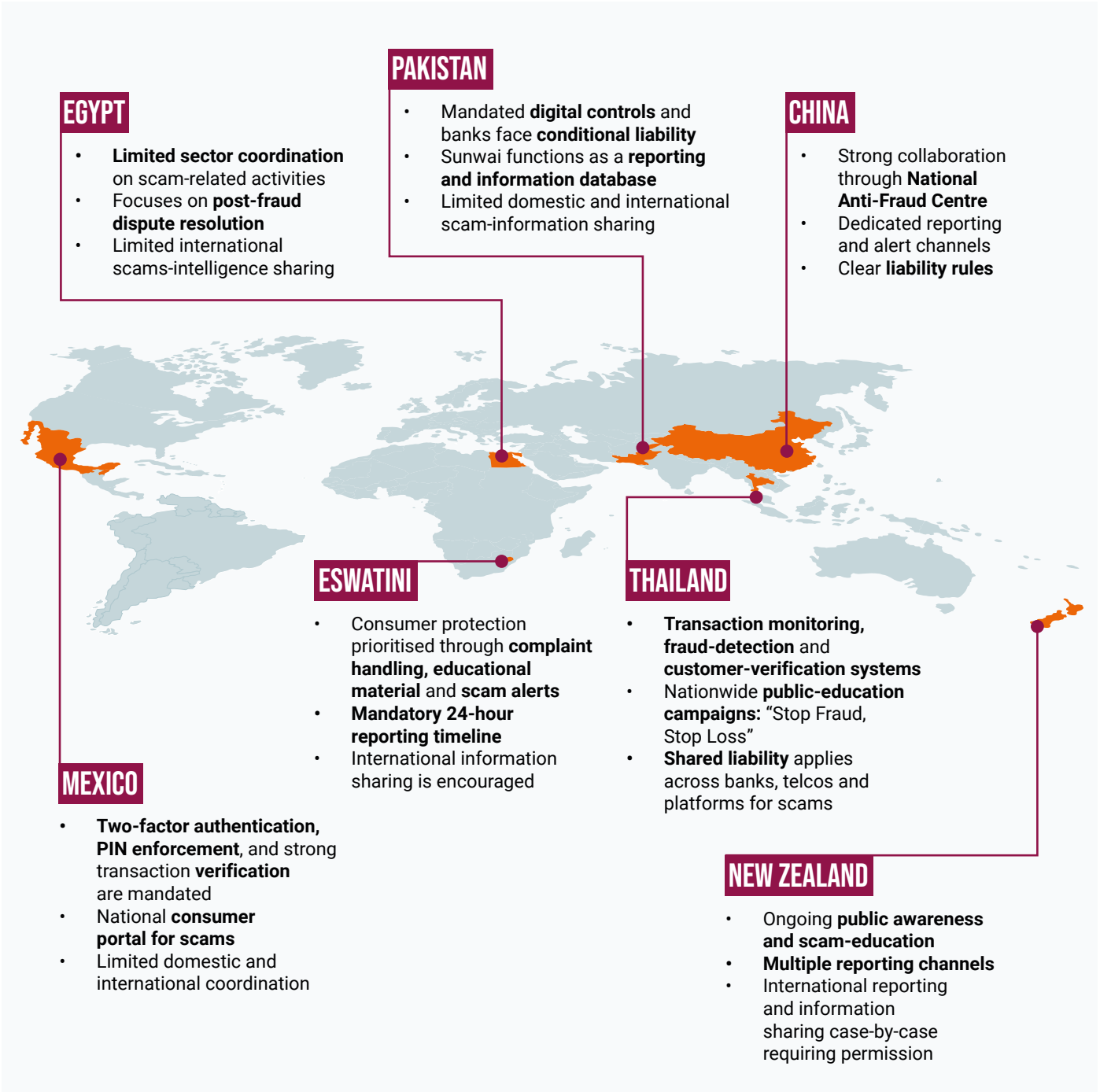


Figure 1: Examples of common responses to scams called for by consumer advocates

3. PILLAR ASSESSMENT

This section summarises the findings on how well policymaker-driven anti-scam measures in the sample jurisdictions fare against the checklist contained in the *Global Action Agenda*. For each pillar, the assessment evaluates both the extent to which a measure aligns with the checklist item, as well as the *level of implementation* of that measure.

When reading the assessment:

The **colour** of the box indicates the extent to which a measure concords with the checklist item:

- A dark blue box indicates complete alignment with the checklist item;
- A pale blue box indicates limited or less comprehensive alignment;
- A grey box indicates that no measure has been identified.

A **progress symbol** is only present for dark or pale blue boxes, and indicates the level of implementation of the measure identified:

- ✓ A check mark indicates full implementation – that is, the measure is in place in law;
- A progress arrow indicates that the measure is an announced policy but not yet in law;
- ✗ No progress symbol is used if there is no measure in place or announced.

While recognising that jurisdictions' responses to scams are strengthened by important voluntary and multi-stakeholder initiatives,[11] to improve comparability, this analysis focuses specifically on policymaker-driven anti-scams measures that have been explicitly called for by consumer advocates. As a result, voluntary anti-scams actions undertaken by private sector actors, civil society organisations and others, are not reflected in the assessment. Readers should not assume that this omission is an intentional disregard of their worth.

Rather, this reflects the purpose of this report: to examine the extent to which the protection against scams called for by consumer advocates is embedded in formal policy frameworks. Policy and regulation are shown to be durable, system-wide mechanisms that create consistent expectations, accountability and protections for consumers over time, while voluntary initiatives play an important complementary role by supporting innovation and operational responses within this broader framework, though they may vary across contexts and evolve alongside changing incentives and priorities. Future work could build on this analysis by assessing voluntary initiatives more systematically.

The policy scan was conducted between September and December 2025. All reasonable efforts have been made to check for accuracy and completeness in the 28 jurisdictions covered, including a subsequent review by trusted national consumer associations, government agencies, and independent and private sector experts in consumer protection. This is a fast-moving area, and how scams are treated and defined at the jurisdictional level varies, which requires a necessary element

11 A wide range of voluntary and multi-stakeholder initiatives are currently contributing to anti-scam efforts across jurisdictions. Given the breadth of activity, this report does not attempt to list them exhaustively: these initiatives could be explored more fully in future work.

of subjectivity in the assessment. We encourage interested parties to contact us at impact@consint.org to discuss any queries. See Annex 1 for a more detailed explanation of the methodology.

Figure 2 provides a snapshot of the assessment. These aggregated numbers show the jurisdictions where a policymaker-driven measure is identified and aligns fully with the corresponding checklist item in the *Global Action Agenda*. It is worth recognising that some jurisdictions may still have policymaker-driven measures in place which correspond to the checklist item, even if they do not align fully, and this progress is worth recognising. See the individual pillar assessments for details.

PILLAR 1: PREVENT & DISRUPT	Are there mandatory secure communictaion and data requirements?	Are there specific obligations for online platforms to stop scam content within their environments?	Are consumers always required to use certain security measures (two-factor authentication, secure PINs etc.)?	Does the framework specify international sharing of scams intelligence?	
	23/28	**6/28**	**12/28**	**10/28**	
PILLAR 2: EMPOWER & DEFEND	Does the framework mandate scams education or targets education from a national authority?	Is there a single national consumer portal with clear consistent scams advice that links across sectors and platforms?	Are there schemes by sector to verify authenticity of businesses and providers?	Are specific payment frictions ensured by payment service providers?	Is scam intelligence shared across borders building a structured international scam-alert system with rapid notification triggers?
	16/28	**8/28**	**5/28**	**13/28**	**3/28**
PILLAR 3: REPORT & ACT	Is there a single one-stop reporting centre that feeds into a national scams database?	Is there a 24/7 inter-agency scams hub that links all sectors (police, regulators, banks, etc.)?	Are there clear legal frameworks that enable businesses to safely share relevant scam-data with governments, law enforcement and trusted partners?	Does the framework enable consumer reports to remove scam content, trigger instant checks, freezes or investigations?	Is there specific demonstrated cross-border enforcement on scams?
	9/28	**5/28**	**4/28**	**7/28**	**13/28**
PILLAR 4: RECOVER & DETER	Does the law specify consumer redress mechanisms such as a dedicated body and timeframe for reimbursement?	Does the authority require or provide specific spaces for consumer support?	Does the law address accountability for scams specically?	Are there specific reciprocal agreements to recall or freeze funds across borders?	
	7/28	**14/28**	**10/28**	**0/28**	

Figure 2: The Global Action Agenda: Where is progress being made? Assessment of number of jurisdictions with policymaker-driven measures in place.

1) PREVENT AND DISRUPT

Stopping scammers in their tracks. Stopping scams early saves money, avoids emotional harm and helps maintain consumer trust and confidence in digital and financial systems. It is also more effective than trying to trace and recover funds after the fact. Via the *Global Action Agenda*, consumer representatives have called for three national-level actions within this pillar:

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

2. **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.

3. **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.

In addition, the *Global Action Agenda* includes a fourth action focused on global coordination:

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

Is account onboarding and mule account prevention the true starting point for tackling scams?

Most modern scams rely on access to regulated financial accounts through which funds can be received and moved. This calls into question whether a scam starts with consumer deception or actually at the point of account opening. Scammers falsify information to open an account, take over accounts or convince genuine account holders – either knowingly or unknowingly – to launder the funds through their account.

Financial institutions play an important role in stopping scams before they cause consumer harm. Robust due diligence is key to ensuring that accounts are not opened by illegal actors. Transaction analytics are essential for detecting mule accounts and stopping scams from continuing. Alongside, this sector wide data sharing (with appropriate safeguards) is an important foundation to prevent frauds from being repeated.

In the UK, the Payment Systems Regulator introduced mandatory reimbursement for victims to incentivise the industry to do more to stop fraud and scams. Victim reimbursement is spread equally (50/50) between the sending and the receiving firm. acknowledging receiving banks provide the accounts fraudsters use.[1]

Scam ecosystems are also shaped by wider economic pressures. Money mules are often recruited online with promises of easy income, particularly targeting students and those facing financial hardship. Limited awareness of legal consequences, combined with slow court processes in the digital age, can weaken deterrence. Credible and proportionate enforcement is essential, both to disrupt organised criminal networks and to prevent individuals from being drawn into fraud supply chains.

Faith Reynolds, *Devon Fields Consulting*

1 "We consider that receiving PSPs [Payment Service Providers] need adequate financial incentives to do more to detect fraud and prevent fraud losses, because they provide the accounts that fraudsters control and use." Payment Systems Regulator (2025) *APP (Authorised Push Payment) scams reimbursement*.

CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

PILLAR 1: SUMMARY OF JURISDICTIONAL FINDINGS

	Are there mandatory secure communication and data requirements?	Are there specific obligations for online platforms to stop scam content within their environments?	Are consumers always required to use certain security measures (two-factor authentication, secure PINs etc.)?	Does the framework specify international sharing of scams intelligence?
Australia	✓	↻	✓	✓
Botswana	↻	✗	↻	↻
Brazil	↻	✗	↻	✗
Canada	✓	✗	↻	✓
Chile	✓	✗	✓	↻
China	↻	↻	↻	↻
Egypt	↻	✗	↻	↻
Eswatini	↻	✗	↻	↻
EU	↻	✓	↻	↻
Ghana	✓	✗	↻	✓
India	✓	✓	✓	↻
Indonesia	↻	✓	✗	✗
Kenya	✓	✓	↻	✓
Malaysia	↻	↻	✓	↻
Mexico	✓	↻	✓	↻
New Zealand	✓	↻	↻	↻
Nigeria	✓	↻	↻	↻
Pakistan	↻	↻	↻	✓
Peru	✓	✗	✗	✗
Rwanda	✓	✗	↻	↻
Singapore	✓	✓	✓	✓
South Africa	✓	↻	✓	↻
Tanzania	✓	✗	✗	↻
Thailand	✓	↻	✓	↻
UAE	✓	↻	✓	✗
Uganda	✓	✗	✗	↻
UK	↻	✓	✓	↻
USA	↻	↻	↻	↻

Figure 3:
Summary of pillar 1 findings

Checklist concordance: None | Limited | Complete

Implementation progress: **None: ✗** **In progress: ↻** **Fully implemented: ✓**

Is platform accountability now the real frontier in online scams prevention?

As the fraud landscape evolves, cross-sector engagement and platform accountability are emerging as critical frontiers in scam prevention.

Liability frameworks in traditional, unauthorised fraud focus on verifying the payer's identity. Scams present a different challenge: they rely on deception and social engineering to induce authorised payments, manipulating victims into completing transactions in good faith to a receiver reasonably believed to be legitimate. The central question is no longer only who is paying, but who is being paid - and whether that recipient is legitimate or part of a coordinated criminal enterprise.

To preserve trust in the digital economy, payment providers continue to invest heavily in prevention, detection, consumer education, and intervention tools. At PayPal, this includes AI-driven scam alerts, enhanced customer education, and proactive intervention models designed to disrupt suspicious transactions before completion.

However, traditional fraud responses alone cannot mitigate the growing scam threat. Scams typically begin upstream - on online platforms, telecom networks, search engines, or messaging services - and by the time the payment is made the harm is already well underway. Victims have often been carefully groomed or pressured, making prior education and warnings at the point of payment less effective. While upstream actors profess ongoing efforts to remove scam content, given the scale and adaptability of scam networks, stronger upstream accountability and partnership is necessary.

Effective cross-sector frameworks should clarify roles and responsibilities aligned with risk and operational capability across the scam lifecycle. Reimbursement regimes should protect victims while preserving incentives for strong prevention, linking liability to demonstrated investment in robust safeguards, collaboration, and data sharing and recognising those who invest in prevention and imposing proportionate consequences where controls are insufficient. Assigning liability exclusively to one sector risks distorting incentives and weakening upstream controls.

Equally important is the ability for cross-sector intelligence sharing, at scale and at speed, so that signals detected upstream can inform real-time risk decisions at the point of payment. Timely, actionable information exchange - supported by clear legal frameworks and appropriate safe harbors - would allow payment providers and other intermediaries to incorporate upstream signals into real-time risk decisions while safeguarding privacy and encouraging collaboration.

Only a framework that connects upstream disruption, downstream controls, effective information sharing, strengthened collaboration among all stakeholders involved, and public-sector capability building will meaningfully reduce the scale and impact of scams.

No single actor can address this challenge alone. Success should not be measured solely by how financial losses are allocated, but by our collective ability to reduce the lifespan of scams and prevent harm to consumers.

Mathilde Bonneau, *Director, International Payments Policy, Government Relations, PayPal*

KEY PATTERNS AND GAPS: JURISDICTIONS ARE TAKING ACTION, BUT SCAM SPECIFIC MEASURES ARE LIMITED

- **Most advanced pillar.** Many of the jurisdictions are already taking measures to prevent and disrupt scams – more so than in any of the other pillars.

- **Progress is strongest in secure communication and data.** All of the sample jurisdictions encourage secure communication and data, and 23 of those do so in full alignment with our checklist.

- **Controls tend to focus on financial channels** Seventeen of the sample jurisdictions have measures to require online platforms to prevent scam content within their environments, although only six do so in complete concordance with our checklist. There are also delays in implementation.

- **Security-by-design is encouraged more than mandated.** Telecom measures such as subscriber identity module (SIM) registration[12] are in place in most jurisdictions for law enforcement purposes. Only 12 of the sample jurisdictions direct payment service providers embed safeguards to help block suspicious payments before funds reach the scammer and to disrupt the financial lifeline of scam operations.

- **Room for improvement in dedicated international scam intelligence sharing.** Cross-border intelligence sharing usually relies on anti-money laundering channels rather than dedicated scam-intelligence pipelines. Only 10 of the sample jurisdictions enable the international sharing of scam intelligence.[13]

CASE STUDY: AUSTRALIA'S SCAMS PREVENTION FRAMEWORK

Australia's Scams Prevention Framework is a legislative regime designed to create new obligations for businesses, including financial service providers, online platforms, and telecommunications providers, to prevent, detect, and disrupt scams before they reach consumers. The framework, together with the National Anti-Scam Centre, which coordinates efforts across scam education, data and intelligence, and outreach, forms the basis of Australia's nationwide approach to combatting scams. It also includes the Scamwatch reporting service and a mandatory short message service (SMS) sender identity (ID) registration system, which is currently in its beta phase until 1 July 2026. While the Framework establishes a solid foundation, it has not yet been operationalised; sectors are still in the process of being designated and data sharing is not yet fully operational.

Online platform accountability
Under the Framework, the Digital Platforms Code will introduce specific obligations for online platforms, which are expected to include obligations to verify new accounts and advertisers, identify and remove scam content, and freeze or block accounts when necessary.

Bank and telco obligations
Similarly, banks and telecommunications providers will be subject to additional obligations such as issuing consumer warnings, providing 24/7 reporting channels, delivering consumer education initiatives, and blocking fraudulent calls and SMS messages.

12 SIM registration requires every SIM to be linked to a person. Sender identification rules are in place in a few jurisdictions. These require any business sending a branded text message to be registered, otherwise the message might be labelled as 'unverified' or 'potential scam'. However, these measures are limited to telecommunications channels, and do not cover messages on online platforms.

13 Note that consumer protection authorities' part of the International Consumer Protection and Enforcement Network – ICPEN have designed Econsumer.gov, an initiative for consumers to report international scams and cross-border fraud. See more here: https://www.econsumer.gov/?lang=en-US

Website takedown
Australia's regulators are also working collaboratively to take down scam websites and advertisements. Scamwatch receives daily scam reports, with consumer consent, which are shared with the National Anti-Scam Centre and the Australian Securities and Investments Commission (ASIC) to facilitate the rapid removal of fraudulent websites. The Australian Securities and Investments Commission reports that around 130 scam websites are being shut down each week.

Intelligence sharing
Finally, the Framework enhances intelligence sharing by establishing mechanisms for both local and international data exchange. Recognising that businesses often only see part of the scam landscape, the Scams Prevention Framework requires them to share scam intelligence with the Australian Competition and Consumer Commission. The Australian Competition and Consumer Commission then distribute this information to other businesses, law enforcement agencies, and international partners, enabling coordinated action to prevent, detect and disrupt scams more effectively.

Sources: Australian Competition and Consumer Commission, N.D.; The Commonwealth of Australia, 2025; Australian Securities and Investments Commission, 2025; Australian Communications and Media Authority, N.D.

Box 1: Australia case study

2) EMPOWER AND DEFEND

In the shoes of consumers. This pillar covers measures called for by consumer representatives to empower consumers with the knowledge, tools and confidence to recognise and resist scams. In this pillar, there are four national-level actions:

1. **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.

2. **One-stop guidance:** Provide a national consumer portal with clear, consistent scams advice, linked across sectors, online platforms and businesses.

3. **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.

4. **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.

In addition, the *Global Action Agenda* includes a fifth action focused on global coordination:

5. **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.

PILLAR 2: SUMMARY OF JURISDICTIONAL FINDINGS

	Does the framework mandate scams education or targeted education from a national authority?	Is there a single national consumer portal with clear consistent scams advice that links across sectors and platforms?	Are there schemes by sector to verify authenticity of businesses and providers?	Are specific payment frictions ensued by payment service providers?	Is scam intelligence shared across borders building a structured international scam-alert system with rapid notification triggers?
Australia	✓	✓	↻	↻	✓
Botswana	↻	✗	✓	✗	✓
Brazil	↻	✗	✓	✓	✗
Canada	↻	✓	✓	✗	✓
Chile	↻	✓	↻	↻	✗
China	↻	↻	✓	✓	✓
Egypt	✓	↻	✗	↻	↻
Eswatini	✓	↻	✓	↻	✓
EU	↻	✗	✓	✓	✓
Ghana	↻	✓	↻	↻	✓
India	✓	✓	✓	✓	✗
Indonesia	↻	↻	↻	↻	✓
Kenya	✓	✗	✓	✗	✓
Malaysia	↻	✓	✓	✓	✓
Mexico	↻	↻	✓	↻	✗
New Zealand	✓	✓	↻	✗	✗
Nigeria	↻	✗	↻	✓	✓
Pakistan	↻	↻	↻	↻	✗
Peru	↻	✗	↻	✗	✗
Rwanda	↻	✗	↻	✗	✓
Singapore	✓	✓	✓	✓	✓
South Africa	↻	✗	↻	✓	↻
Tanzania	✓	✗	↻	✗	✓
Thailand	✓	✓	✓	↻	✓
UAE	✓	✓	✗	✓	✓
Uganda	✓	✗	↻	✗	✗
UK	↻	✓	✓	✓	✗
USA	↻	↻	↻	✗	✗

Figure 4:
Summary of pillar 2 findings

Checklist concordance: None | Limited | Complete

Implementation progress: **None: ✗** **In progress: ↻** **Fully implemented: ✓**

KEY PATTERNS AND GAPS: CONSUMERS BEAR THE BURDEN OF SCAM DEFENCE, BUT LACK THE TOOLS

- **Consumer education is widespread.** All of the sample jurisdictions already mandate education campaigns or are currently implementing such measures. In many jurisdictions, private entities and non-governmental organisations are also taking initiatives to educate consumers. However, messaging is uneven across sectors and not always tied to a central, trusted source.[14]

- **National consumer portals not yet common.** Only eight of the sample jurisdictions already have, or are implementing, a national portal where consumers can receive accurate, up-to-date information regarding protection measures and scams prevention.

- **Not easy to tell what can be trusted**. Formal schemes to verify online businesses only exist in five of the sample jurisdictions.

- **Friction in payments is gaining ground.** Thirteen of the sample jurisdictions have incorporated compulsory payment frictions such as warnings, holds and confirmation-of-payee.

- **Scam alerts tend to be domestic only, and mostly after the fact.** International alerts on emerging scams are limited and is only seen in three of the sample jurisdictions.

CASE STUDY: SINGAPORE'S WHOLE-OF-SOCIETY RESPONSE

Singapore has taken a whole-of-society approach to preventing and responding to scams. The Protection from Scams Act empowers the police to issue banks with restriction orders that can prevent potential victims from completing scam-related transactions. Under the Shared Responsibility Framework, there is a waterfall liability system that assigns responsibility to both telecommunications providers and financial service providers, encouraging shared accountability for preventing and responding to phishing scams.

Targeted education

Singapore has a multi-layered, government-led targeted education programme, which focuses particularly on elderly and vulnerable populations. Initiatives include Mass Rapid Transit advertising campaigns and community police outreach programmes, including in person and on social media, designed to raise public awareness and build citizens' capacity to recognise and report scams.

ScamShield

ScamShield serves as Singapore's one-stop scams portal, offering consumer education and tools to help citizens report and manage scams. Through its mobile application, users can check and submit suspected scam messages and calls to authorities. The app also automatically blocks and filters scam calls and messages, helping to reduce exposure to fraudulent content.

14 There is a growing debate to suggest that a focus on consumer education diverts effort and attention away from other solutions, such as fixing detection systems, or establishing liability frameworks. Emphasising such initiatives also risks shifting the blame to consumers for not being "educated" enough. Organisations such as Innovations for Poverty Action have tested typical educational messages and shown they do not work. See for example https://poverty-action.org/evaluating-digital-fraud-prevention-methods-small-businesses-nigeria and https://poverty-action.org/can-providing-information-consumers-about-scams-mitigate-victimization-evidence-kenya.

Positive friction
The Monetary Authority of Singapore (MAS) requires payment service providers to introduce multiple positive friction measures that help prevent unauthorised transactions. These include a 12-hour cooling-off period for new device logins, additional confirmation for high-risk or large-value transfers, default transaction and top-up limits, real-time detection and blocking, outbound alerts, and a self-service "kill switch" allowing customers to immediately freeze their accounts if they suspect fraud.

Short Messaging Service (SMS) and Sender Identity (ID) Registration
The SMS Sender ID Registry mandates that telecommunications companies register legitimate sender IDs and block unregistered IDs. This requirement ensures that only verified entities can send SMS messages using recognisable sender names, significantly reducing the risk of spoofing and phishing attempts.

Source: Yap, 2025; Monetary Authority of Singapore, 2022; Leon, 2025; Government of Singapore, N.D.

Box 2: Singapore case study

3) REPORT AND ACT

A quick response to limit harm. Timely reporting and action enables responses to emerging threats, stops harm spreading to others and helps authorities to identify and disrupt scam networks (Federal Trade Commission, 2025). This pillar focuses on measures called for by consumer representatives that make sure consumers know where to report scams and that real action follows.

It contains four national-level actions:

1. **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.

2. **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.

3. **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.

4. **Rapid investigations:** Ensure consumer reports trigger instant checks, freezes or investigations, as appropriate.

In addition, the *Global Action Agenda* includes a fifth action focused on global coordination:

5. **Cross-border enforcement:** Secure international agreements for joint investigations, takedowns and enforcement actions.

CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

PILLAR 3: SUMMARY OF JURISDICTIONAL FINDINGS

	Is there a single one-stop reporting centre that feeds into a national scams database?	Is there a 24/7 inter-agency scams hub that links all sectors (police, regulators, banks, etc.)?	Are there clear legal frameworks that enable businesses to safely share relevant scam-data with governments, law enforcement and trusted partners?	Does the framework enable consumer reports to remove scam content, trigger instant checks, freezes or investigations?	Is there specific demonstrated cross-border enforcement on scams?
Australia	✓	✓	✓	✗	✓
Botswana	✓	↻	↻	✗	✓
Brazil	✗	✗	✓	↻	↻
Canada	✓	↻	✓	✗	↻
Chile	✗	↻	↻	✗	↻
China	✓	✗	✓	✓	✗
Egypt	✗	✗	↻	✓	✓
Eswatini	✗	✗	↻	↻	✓
EU	✗	✗	✓	✓	↻
Ghana	✗	↻	↻	✓	✓
India	✓	✓	↻	↻	↻
Indonesia	↻	↻	↻	✗	✓
Kenya	✗	✓	↻	✓	✓
Malaysia	✓	✓	✓	✓	↻
Mexico	✓	✓	↻	✗	↻
New Zealand	✗	✗	✓	✓	✓
Nigeria	✗	↻	✓	✓	✓
Pakistan	✗	✗	↻	✓	✗
Peru	✗	✓	✗	✗	↻
Rwanda	✗	↻	↻	✓	✓
Singapore	✓	✓	✓	✓	↻
South Africa	✗	↻	↻	↻	✓
Tanzania	↻	↻	↻	↻	↻
Thailand	✓	✓	↻	✓	✓
UAE	✗	✗	✓	✗	✗
Uganda	✗	✗	↻	✗	✗
UK	✗	↻	✓	✗	↻
USA	✓	↻	✓	↻	✓

Figure 5:
Summary of pillar 3 findings

Checklist concordance: None | Limited | Complete

Implementation progress: **None: ✗** **In progress: ↻** **Fully implemented: ✓**

KEY PATTERNS AND GAPS: A FRAGMENTED APPROACH TO REPORTING AND ACTING

- **One-stop reporting centres are still rare.** Many of the sample jurisdictions do have some systems for scam reporting, yet the assessment finds that only nine out of the 28 meet the policy action checklist requirement of having – or making progress towards – a one-stop reporting centre that feeds into a national scams database.

- **Biggest gap is in scam coordination hubs.** Several examples were identified, but only five completely align with the policy action checklist – either because they do not connect to a national database, or because they lack a front-door portal. Many of the examples are also still in the initial stages of development.

- **Data sharing is enabled, but incomplete.** Most jurisdictions have some data sharing, with respect to payments for example, but only four specifically enable data sharing on scams with the express intention of protecting consumers.

- **Limited centrally defined rapid response procedures.** The assessment shows that only seven jurisdictions have a clear, binding playbook for rapid response that tells victims who to call, how to freeze funds, and how to escalate a scam case.

- **Cross-border enforcement relies on general cooperation tools.** In the sample, cross-border enforcement relies on general cooperation tools such as police- based cooperation, mutual legal assistance treaties and financial intelligence unit links, rather than scam-specific agreements. The frameworks in 13 of the sample jurisdictions allow for cross-border enforcement.

EXAMPLES OF COORDINATION MECHANISMS ACROSS PILLARS OF THE GLOBAL ACTION AGENDA

Uganda's Financial Sector Anti-Fraud Consortium
Mission: Compulsory intelligence sharing, regulatory and legal strengthening, capacity building and coordinated public awareness.
Launch date: April 2025
Sectors/entities involved: Uganda Bankers' Association, Bank of Uganda (BoU), Uganda Communications Commission, Payment Systems Providers Association, and Financial Intelligence Authority, Credit Reference Bureaus Association, Director of Public Prosecutions.
Source: Interview, Financial Sector Deepening Uganda (FSD), 2025; Financial Intelligence Authority 2025; NSTV interview with BoU, 2025

South Africa's Digital Banking Fraud Project
Mission: Banking focus. Longer-term, collaborative approach focused on intelligence sharing. Key goal is to understand the value-chain and identify where each participant can intervene. Enhanced international information sharing.
Launch date: Roundtable, September 2025
Sectors/entities involved: Led by South Africa's Financial Sector Conduct Authority. Memoranda of Understanding between the Financial Sector Conduct Authority (FSCA) and South African Banking Information Risk Centre; and Financial Sector Conduct Authority and South African Fraud Prevention Services.
Source: Interview, FSCA, 2025

Malaysia's Scam Response Centre
Mission: Operational centre to coordinate rapid responses to online financial fraud.
Launch date: 2022
Sectors/entities involved: National Anti-Financial Crime Centre, the police, the central bank, the telecommunications authority, financial service providers, and telecommunications businesses.
Source: Bank Negara Malaysia 2025; National Anti-Financial Crime Center n.d.

Box 3: Examples of coordination mechanisms

CASE STUDY: INDIA'S GOLDEN HOUR

India's Ministry for Home Affairs, through the Indian Cyber Crime Coordination Centre (IC4), operates on the principle that when reporting and response occur within 60 to 120 minutes of a fraudulent transaction, a sizeable portion of defrauded funds can be recovered. As a result, the national approach places strong emphasis on consumer education and rapid reporting through a dedicated hotline or online portal.

Citizen Financial Cyber Fraud Reporting and Management System
The National Cybercrime Reporting Portal and the 1930 telephone hotline provide a one-stop reporting system under the Citizen Financial Cyber Fraud Reporting and Management System. When a complaint is filed, a ticket is generated and pushed to relevant bank, wallet, or merchant teams, allowing funds to be frozen quickly during the so-called "golden hour." However, this process is not automatically triggered for scams flagged through the Unified Payments Interface (UPI), India's much-publicised payments digital public infrastructure which powers 640 million transactions daily. (Press Information Bureau Government of India, 2025) This gap illustrates the challenges of building effective scam safeguards into instant payment systems, a debate which is particularly relevant giving the growing emphasis on the establishment of digital public infrastructure.

Cyber police
Each district in India also has a cyber police unit that operates at the state level, using the same Citizen Financial Cyber Fraud Reporting and Management system to log and manage scam reports.

Cyber-crime coordination
The Indian Cyber Crime Coordination Centre facilitates interagency coordination, providing a shared platform for joint investigations, analytics, training, and broader cooperation among law enforcement agencies.

Limitations on freezing funds
Despite these advancements, there are ongoing limitations related to the freezing of funds, as the constitutionality of certain laws that enable rapid fund blocking continues to be legally challenged.

George, 2025, Indian Cybercrime Coordination Centre, 2024

Box 4: India case study

4) RECOVER AND DETER

What happens after a scam takes place is also important. The measures under this pillar are what consumer representatives call for to support victims by returning lost funds, including by recalling funds cross-border. They also ensure that those who are responsible are held to account. It includes three national-level actions:

1. **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.

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

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

In addition, the *Global Action Agenda* includes a fourth action focused on global coordination:

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

PILLAR 4: SUMMARY OF JURISDICTIONAL FINDINGS

	Does the law specify consumer redress mechanisms (a dedicated body and timeframe for reimbursement)?	Does the authority require or provide specific spaces for consumer support?	Does the law address accountability for scams specifically?	Are there specific reciprocal agreements to recall or freeze funds across borders?
Australia	✓	✓	✓	✗
Botswana	✗	✗	↻	✗
Brazil	↻	✓	✓	✗
Canada	✓	✓	✓	✗
Chile	✓	✓	✓	✗
China	↻	✓	✓	✗
Egypt	✗	✓	✗	✗
Eswatini	✗	✓	✓	✗
EU	↻	↻	↻	✗
Ghana	↻	✓	✗	✗
India	↻	✓	✓	✗
Indonesia	↻	↻	✗	✗
Kenya	✗	↻	↻	✗
Malaysia	✗	✓	✗	✗
Mexico	↻	✓	↻	✗
New Zealand	✗	✓	↻	✗
Nigeria	↻	✗	✓	✗
Pakistan	↻	✓	✓	✗
Peru	✗	↻	✗	✗
Rwanda	✗	✓	↻	✗
Singapore	✓	✓	↻	✗
South Africa	✗	↻	✗	✗
Tanzania	↻	✓	✗	✗
Thailand	↻	✓	↻	✗
UAE	↻	✓	✓	✗
Uganda	✗	✓	✗	✗
UK	✓	↻	✓	✗
USA	✗	✓	✓	↻

Figure 6:
Summary of pillar 4 findings

Checklist concordance: None | Limited | Complete

Implementation progress: **None: ✗** **In progress: ↻** **Fully implemented: ✓**

KEY PATTERNS AND GAPS: CONSUMERS ARE NOT GETTING THE SUPPORT THEY NEED.

- **Redress is incomplete.** Although consumer redress mechanisms exist in most jurisdictions, only seven of the sample frameworks include consumer redress mechanisms that specifically provide redress for scams.[15]

- **Progress towards the provision of victim support.** Victim support is present in 14 of the sample jurisdictions, mainly through ombuds and advice centres. It is often advisory rather than restitution oriented.

- **Variance in whether and how accountability is assigned.** Clear liability for scams is specified in 10 of the sample policy frameworks. There is a movement in some jurisdictions to reconsider how liability is assigned across the consumer and financial service provider.[16]

- **Cross-border funds recall is the biggest gap.** Reciprocal agreements to immediately freeze or recall funds cross-border were not identified in any of the sample.

CASE STUDY: THE UNITED KINGDOM'S MULTI-LAYERED APPROACH

The United Kingdom has implemented multiple measures to address and deter scams through a multipronged approach led by the Joint Fraud Taskforce. A new fraud strategy, launched ahead of the Global Fraud Summit organised by the United Nations Office on Drugs and Crime in March 2026, aims to strengthen international cooperation. The existing strategy targets seven key areas, including improved data sharing, closer collaboration with technology and telecommunications sectors, enhanced public awareness and victim support, responses to evolving threats such as artificial intelligence, stronger criminal justice outcomes, and efforts to tackle fraud affecting businesses and economic growth.

Report Fraud

Report Fraud serves as the central reporting and victim support centre for fraud and cybercrime in the United Kingdom. Operated by the police, it provides broad victim support through a charity partner and offers additional care to vulnerable victims via the National Economic Crime Victim Care Unit. However, Report Fraud does not provide direct assistance to recover lost funds.

Authorised push payment liability

The authorised push payment reimbursement scheme entitles victims of authorised push payment scams to compensation of up to GBP85,000, with the sending payment service provider covering

15 In many jurisdictions specific redress is provided for unauthorised transactions, but not for scams, which lead to authorised transactions.

16 Two notable examples are the United Kingdom (UK) and the European Union (EU):
- Under the UK's authorised push payment fraud reimbursement scheme, effective since October 2024, payment service providers must reimburse the customer up to a ceiling amount for any fraudulently induced transaction, not just unauthorised payments. This regime shifts the burden of proof onto the payment service provider to show gross negligence on the part of the consumer.
- In the EU, the proposed Payment Services Directive 3/Payments Services Regulation will see conditional reversal of liability resulting in compensation from the financial service provider for authorised push payments in specific situations, including spoofing. This would cover both authorised push payments and compromised credentials. The consumer must report without delay. The consumer will be liable where there is negligence (not gross negligence).

the full amount of which it can recover 50% from the receiving provider. Consumers are not held liable unless they fail to meet the "standard of caution," and the rule does not apply to consumers in vulnerability.

Accountability
In April 2025, possessing or supplying a Subscriber Identity Module (SIM) farm[17] without legitimate purpose became a criminal offence. Additionally, in September 2025, the United Kingdom introduced a new corporate criminal offence for failure to prevent fraud, particularly targeting insider fraud within large corporations.

Cross-border enforcement
While the United Kingdom engages in cross-border enforcement, there is currently no proactive mechanism for cross-border fund freezing outside of specific investigations. This limits the ability to recover funds transferred abroad despite active international cooperation.

Source: City of London Police, N.D.; Payments System Regulator, 2025; Home Office, 2025; Government of the United Kingdom, 2025

Box 5: United Kingdom case study

17 Also known as SIM boxes, Subscriber Identity Module (SIM) farms hold multiple SIM 'cards' and allow mass messaging, and routing of calls to appear as though they are over local networks as well as set up 'verified' accounts online at scale.

4. DELIVERING ON THE GLOBAL ACTION AGENDA

No more time for inaction. As scams become increasingly sophisticated, and technology increasingly advanced, there is an urgent need for coordinated, multi-stakeholder action, putting consumer needs at the centre. This evaluation shows that many jurisdictions are taking meaningful steps across the four pillars of the *Global Action Agenda*. However, it also shows up several gaps and limited progress. As has been raised previously, this analysis does not assess effectiveness or impact of individual policies or regulations, and adoption does not necessarily correlate with reduced consumer harm. When combined with the *Global Action Agenda*, we hope it can offer both a diagnostic and illustrative tool for what might lead to progress.

Foundational measures in place, but gaps remain. Many jurisdictions have established regimes for cybersecurity, payments protections and anti-money laundering. While these areas are foundational to help combat scams, there are gaps in measures specifically targeted at scams, as well as in areas that require national or international cooperation. Overall, the picture is one of a global ecosystem ill equipped to address scams on a coordinated basis, but with pockets of better practice.

Four clear gaps emerge. Each jurisdiction has a different starting point. The types of scams prevalent, the existing structures for public and private collaboration, the specific legal distinctions between scams and other frauds, the level of consumer financial literacy and vulnerability, and the capacity of financial institutions, regulatory authorities and law enforcement agencies all shape which measures they prioritise. There is therefore no single solution that works for every jurisdiction.

From the perspective of consumer representatives, there are four elements which may help strengthen **consistency** and **coordination** in the fight against online scams. Our assessment identifies the following as the areas where the largest gaps in policy and regulation exist:

1. Requiring online platforms to prevent scam content from appearing within their environments.

2. Creating a national consumer portal with clear and consistent advice across sectors, as well as one-stop reporting centres that feed into national databases.

3. Developing international coordination mechanisms to share scam intelligence and trigger alerts across borders, as well as cross-border agreements to recall or freeze funds when scam activity is suspected.

4. Assessing whether existing consumer redress mechanisms appropriately provide redress for scams.

Governments cannot act alone. While it is important for governments to take the lead, the private sector and civil society also need to step up in the fight against scams: by being active participants and drivers of inter-sectoral cooperation, by advocating for change at all levels, and by sharing expertise and information. Indeed, while this report focuses on government-mandated initiatives, there are many examples of private sector and civil society-led initiatives that governments can leverage to improve the national scams responses.

It is not necessary to start from scratch. Governments can recognise and build upon existing initiatives, including private sector innovations. Effective regulation should enable and accelerate industry best practices while ensuring consistent, mandatory baseline protections.

Finding the balance between protection and participation. It is important to make sure that the drive to combat scams does not exclude some consumers from the financial system. Governments need to work with consumer groups and industry to ensure that scam protections do not lead financial services providers to view vulnerable consumers as too risky – or even too costly – to serve.

An existing base to leverage. It is not necessary to begin from nothing. Governments can both learn from existing regimes, such as those for cybersecurity and anti-money laundering, and add to them to specifically address scams.

ACKNOWLEDGEMENTS

This report was produced by Consumers International with the support of Cenfri. Consumers International is thankful to Stefan Hall, Brooke Kingsland, Helena Leurent and Andrea Vega Talledo.

We are particularly grateful to the organisations listed below, which critically reviewed a draft and provided valuable feedback. Appreciation is also due to the following experts who provided feedback in an individual capacity: Martyna Derszniak-Noirjean, Rafe Mazer and Faith Reynolds.

We note that the final version does not necessarily reflect the views of these organisations or individuals.

Organisation	Jurisdiction
Amazon.com, Inc.	Global
Australian Consumers' Association (CHOICE)	Australia
Australian Securities and Investments Commission	Australia
Center For Financial Inclusion	Global
Consumentenbond	Netherlands
Consumers Council of Canada	Canada
Consumer NZ	New Zealand
Consumer Reports	United States of America
Consumer VOICE	India
Gates Foundation	Global
Georgian Competition and Consumer Agency	Georgia
CGAP	Global
Innovations for Poverty Action	Global
National Consumer Commission	South Africa
PayPal, Inc.	Global
Tec-Check Digital Consumers Organization	Mexico
World Bank	Global
Which?	United Kingdom
Visa, Inc.	Global

REFERENCES

ACI Worldwide. (2022). *Growth in APP Scams Expected To Double by 2026: Report by ACI Worldwide and GlobalData.* ACI Worldwide. Retrieved from https://investor.aciworldwide.com/node/23941/pdf

Australian Communications and Media Authority. (N.D.). *ACMA*. Retrieved from Short Messaging Service Sender Identity Register: https://www.acma.gov.au/sms-sender-id-register

Australian Competition and Consumer Commission. (2024, July 9). *Criminals targeting victims of previous scams promising financial recovery.* Retrieved from ACCC: https://www.accc.gov.au/media-release/criminals-targeting-victims-of-previous-scams-promising-financial-recovery

Australian Competition and Consumer Commission. (N.D.). *Scam Watch.* Retrieved from About Scam Watch: https://www.scamwatch.gov.au/about-us/about-scamwatch

Australian Securities and Investments Commission. (2025, August 21). *ASIC*. Retrieved from Scammers on notice as ASIC steps up action to protect consumers from online investment scams: https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2025-releases/25-171mr-scammers-on-notice-as-asic-steps-up-action-to-protect-consumers-from-online-investment-scams/

Banco Central do Brasil. (2024, May). *Pix frequently asked questions.* Retrieved from Banco Central do Brasil: https://www.bcb.gov.br/en/financialstability/pixfaqen

City of London Police. (N.D.). *About.* Retrieved from Report Fraud: https://www.reportfraud.police.uk/what-is-report-fraud/

Cole, R. (2024). A qualitative investigation of the emotional, physiological, financial, and legal consequences of online romance scams in the United States. *Journal of Economic Criminology,* 2-6.

Consumers International. (2025, November 12). *Global Action Agenda to Protect Consumers from Online Scams.* Retrieved from Consumers International: https://www.consumersinternational.org/media/675471/consumers-international-global-action-agenda-to-protect-consumers-from-online-scams.pdf

DeNicola, L. (2024, December 20). *The Latest Scams You Need to Be Aware of in 2025*. Retrieved from Experian: https://www.experian.com/blogs/ask-experian/the-latest-scams-you-need-to-aware-of/#

Department of Finance Canada. (2025, October 2020). *Minister Champagne takes aim at financial scams and abuse, announces Anti-Fraud Strategy and new Financial Crimes Agency*. Retrieved from canada.ca: https://www.canada.ca/en/department-finance/news/2025/10/minister-champagne-takes-aim-at-financial-scams-and-abuse-announces-anti-fraud-strategy-and-new-financial-crimes-agency.html

Dhaliwal. (2025, 30 January). *How Scammers Steal Your Identity and What You Can Do About It.* Retrieved from McAfee: https://www.mcafee.com/blogs/privacy-identity-protection/how-scammers-steal-your-identity-and-what-you-can-do-about-it/

Duflos, E. (2025, April). *AI and Responsible Finance: A Double-Edged Sword.* Retrieved from CGAP: https://www.cgap.org/blog/ai-and-responsible-finance-double-edged-sword

Faster Payments Council. (2024). Faster Payments Fraud Trends and Mitigation Opportunties. Faster Payments Council. Retrieved from https://fasterpaymentscouncil.org/userfiles/2080/files/FPC%20Fraud%20Bulletin_01_01-24-2024_Final.pdf

Federal Trade Commission. (2025). *Why Report Fraud?* Retrieved from Federal Trade Commission: https://www.ftc.gov/media/why-report-fraud-0

Financial Industry Regulatory Authority. (2025). *Assisting Victims of Fraud*. Retrieved from Financial Industry Regulatory Authority: https://www.finrafoundation.org/assisting-victims-fraud

George, D. (2025, October 1). (Cenfri, Interviewer)

Government of Singapore. (N.D.). *Whole of Government*. Retrieved from Scam Shield: https://www.scamshield.gov.sg/whole-of-government-effort/

Government of the United Kingdom. (2025, September 1). *gov.uk*. Retrieved from New measures to tackle fraud come into effect: https://www.gov.uk/government/news/new-measures-to-tackle-fraud-come-into-effect

Greening, J. (2025, January 20). *Unveiling the Complexity of Cross-Border Fraud: Insights and Policing Strategies*. Retrieved from Global Anti-Scam Alliance: https://www.gasa.org/post/unveiling-the-complexity-of-cross-border-fraud-insights-and-policing-strategies

Home Office. (2025, April 24). *Major step for fraud prevention with landmark ban on SIM farms.* Retrieved from Gov.uk: https://www.gov.uk/government/news/major-step-for-fraud-prevention-with-landmark-ban-on-sim-farms

Horwitz, J. (2025, November 6). *Meta is earning a fortune on a deluge of fraudulent ads, documents show*. Retrieved from Reuters: https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/

Indian Cybercrime Coordination Centre. (2024). *Cyber Digest*. Retrieved from ic4: https://cybercrime.gov.in/Default.aspx

Innovations for Poverty Action. (2025). *Financial Consumer Protection Survey (FCPS) Uganda 2025.* Retrieved from: https://poverty-action.org/sites/default/files/2026-01/Uganda-2025-Financial-Consumer-Protection-Survey-FCPS-Updated-Jan-2026.pdf

INTERPOL. (2025). *Growing threat of transnational scam centres highlighted at INTERPOL General Assembly*. Retrieved from https://www.interpol.int/News-and-Events/News/2025/Growing-threat-of-transnational-scam-centres-highlighted-at-INTERPOL-General-Assembly#

INTERPOL. (2025, September 24). *USD 439 million recovered in global financial crime operation.* Retrieved from Interpol: https://www.interpol.int/en/News-and-Events/News/2025/USD-439-million-recovered-in-global-financial-crime-operation

KPMG. (2025). *KPMG Global Banking Scam Survey*. KPMG. doi:https://assets.kpmg.com/content/dam/kpmgsites/au/pdf/2025/kpmg-global-banking-scam-survey-2025.pdf

Leon, N. R. (2025). Key Expert Interview. (Cenfri, Interviewer)

LSEG Risk Intelligence. (2025, September 9). *Defeating APP Fraud: Securing global payments in a risk-filled landscape*. Retrieved from LSEG: https://www.lseg.com/en/insights/risk-intelligence/defeating-app-fraud-securing-global-payments-in-a-risk-filled-landscape

Mazer, R., & Garg, N. (2015). *Recourse in Digital Financial Services: Opportunities for Innovation.* Washington, DC: CGAP.

Monetary Authority of Singapore. (2022, June 2). *Monetary Authority of Singapore*. Retrieved from Additional Measures to Strengthen the Security of Digital Banking: https://www.mas.gov.sg/news/media-releases/2022/additional-measures-to-strengthen-the-security-of-digital-banking

Mosk, T. C., Balasubramaniam, V., & Uettwiller, A. (2025). Who Pays for Payment Fraud? Detection and Liability Rules under Strategic Fraudster Adaptation. SSRN, 1-51. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5703762

OECD. (2025). *OECD Integrity Review of Brazil 2025: Consolidating Progress on Public Integrity*. Paris: OECD Publishing. Retrieved from https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/10/oecd-integrity-review-of-brazil-2025_4ccf6d1f/cfcce75d-en.pdf

Payments System Regulator. (2025, May). *Consolidated policy statement APP scams reimbursement.* Retrieved from Payment Systems Regulator: https://www.psr.org.uk/media/rhelv4op/ps25-5-app-scams-reimbursement-consolidated-policy-statement-may-2025.pdf

Press Information Bureau Government of India. (2025, July 20). *India's UPI Revolution*. Retrieved from Press Information Bureau Government of India: https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=154912&ModuleId=3#

Rogero, T. (2024, September 25). *Attempt to arrest Brazilian music star highlights boom in online gambling*. Retrieved from The Gaurdian: https://www.theguardian.com/world/2024/sep/25/arrest-overturned-gusttavo-lima-online-gambling

Rogers, S. (2024, November 7). *Global Anti-Scam Alliance*. Retrieved from International Scammers Steal Over $1 Trillion in 12 Months in Global State of Scams Report 2024: https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai

The Commonwealth of Australia. (2025, January). *Treasury*. Retrieved from Scams Prevention Framework, Protecting Australians from Scams: https://treasury.gov.au/sites/default/files/2025-01/p2025-623966.pdf

Times of India. (2025, July 20). *The Times of India.* Retrieved from UPI surge: India leads the world in fast payments; 18 billion monthly transactions power growth: https://timesofindia.indiatimes.com/business/india-business/upi-surge-india-leads-the-world-in-fast-payments-18-billion-monthly-transactions-power-growth/articleshow/122797610.cms

World Bank. (2025). *The Global Findex Database 2025*. Washington DC: World Bank. Retrieved from https://www.worldbank.org/en/publication/globalfindex

Yap, A. (2025). Consumer Protections to Uphold Trust in DPI. *Global DPI Summit*. Cape Town.

ANNEX 1: METHODOLOGY

The Foundation for the Evaluation: *A Global Action Agenda to Protect Consumers from Online Scams*

In 2025, Consumers International, with the support of a Working Group of 12 organisations from its Consumer Coalition to Stop Scams, developed A Global Action Agenda to Protect Consumers from Online Scams (*"the Global Action Agenda"*).

The *Global Action Agenda* contains a self-assessment checklist for policymakers across four pillars: Prevent and Disrupt, Empower and Defend, Report and Act, Recover and Deter. The four-pillar checklist shows the national policies and regulations that consumer representatives say are required and is accompanied by a corresponding global action that contributes meaningfully to global cooperation against scams.

With endorsement from 25 leading national consumer associations around the world, the *Global Action Agenda* can be considered an authoritative representation of the minimum expectations that consumer representatives have around what constitutes a strong global policy response.

Methodology for the evaluation

1. Selection of jurisdictions

To develop a global snapshot, 28 jurisdictions were selected in this report. The sample was selected to satisfy three criteria:

a. **Geographical coverage:** Representation from every major region was prioritised to ensure a truly global perspective.

b. **Spectrum of Development:** The selection includes jurisdictions at different levels of economic development and digital maturity to reflect varied challenges faced by different economies.

c. **Policy maturity:** Jurisdictions widely referenced as having more advanced scam prevention, detection, and response regimes (such as Australia, Singapore and the United Kingdom) were intentionally included. These jurisdictions can serve as benchmarks for more complete anti-scam frameworks.

2. Assessment framework

Following the sample selection, a two-part assessment was applied.

The first assessment considered the extent to which a policymaker-driven measure aligns with the checklist item.

Where a measure is identified, a blue box is used:

- Dark blue boxed indicate if the measure(s) completely satisfied the checklist item;
- Pale blue boxes indicate if the measure(s) in the jurisdiction partially satisfied the checklist item;
- Grey boxes indicate that no measure was identified that addressed the checklist item.

As described in the report, the evaluation does not assess other measures, such as those driven by the private sector, civil society or other actors. This omission does not by extension convey any judgement on the value of those measures, which could be analysed in future work.

The evaluation also does not assess the effectiveness of the policymaker-driven measures.

The second assessment considered – in cases where a measure was identified – the degree of implementation of the measure. That is, where on the implementation journey the measures can be placed.

Where a measure is identified, a progress symbol is used:

- A check mark indicates full implementation, if the measure is in place in law;
- A progress arrow indicates if the measure is an announced policy but not yet in law;
- No progress symbol is used if there is no measure in place or announced.

3. Expert interviews

To amplify the desktop research, better understand the nuances of the various approaches and gain cross- jurisdictional perspectives, we conducted ten expert interviews:

Organisation	Jurisdiction	Organisation	Summary of organisation/role
National Administration/ state bodies	Australia	Australian Competition and Consumer Commission	Australia's national regulator that promotes fair trading and competition, enforces consumer protection laws, and leads national efforts to detect, prevent, and address scams and market misconduct.
	Brazil	Banco Centrale do Brasil	Brazil's Central Bank
	Peru	Indecopi	National Institute for the Defense of Competition and the Protection of Intellectual Property.
	South Africa	Financial Sector Conduct Authority	South Africa's financial sector conduct regulator.

Experts	Uganda	Jackie Kitiibwa, Financial Sector Deepening (FSD) Uganda	FSD Uganda is the country's leading 'think and do tank' on financial inclusion and inclusive financial market development.
	Nigeria	Brian Mwesigwa, Innovations for Poverty Action	Global research and policy nonprofit committed to reducing global poverty with evidence.
	India	Deepti George, co-founder of Yutadhi	A think-and-action tank dedicated to conducting rigorous research that shapes policy, improving market outcomes, and driving innovation in financial services.
	Singapore	Assoc. Prof Nydia Remolina Leon, Assistant Professor of Law, Singapore Management University	Academic researching digital finance, regulation, and scam prevention, focusing on how technology and policy can strengthen consumer protection and financial integrity.
	United Kingdom	Prof. Mark Button, Director of the Centre for Cybercrime and Economic Crime, University of Portsmouth	Academic researching fraud and scams, focusing on prevention, victim support, and enforcement to improve global responses to financial crime.
	United Kingdom	Jonathan Frost, Director of BioCatch	Technical Collaborations Director at Stop Scams United Kingdom and Director of BioCatch.
	Global	Rafael Mazer, Director of Fair Finance Consulting	Independent advisory firm focused on consumer protection in digital finance, fraud prevention, and fair competition.

CONSUMERS INTERNATIONAL

COMING TOGETHER FOR CHANGE

Consumers International brings together over 200 member organisations in more than 100 countries to empower and champion the rights of consumers everywhere. We are their voice in international policy-making forums and the global marketplace to ensure they are treated safely, fairly and honestly.

consumersinternational.org
impact@consint.org
@consumers_int
/consumers-international