Euroconsumers' Response to the Call for Evidence: Action Plan on Fighting Online Fraud

February 2026

Introduction

Euroconsumers, and its European member organisations in Belgium (Testachats/Testaankoop), Italy (Altroconsumo), Spain (OCU), Portugal (DECOPROteste) and Poland (Euroconsumers Polska), welcome the European Commission's initiative to develop an Action Plan on Fighting Online Fraud. This represents a critical opportunity to address what has become one of the most pressing challenges facing European consumers and the wider economy.

Fraud and scams represent not just a consumer protection issue, but a major structural challenge for the EU. Each year, billions of euros are siphoned from consumers and businesses through fraudulent schemes that could otherwise support innovation, social inclusion, investment in the twin transitions and Europe's competitiveness. It is not just consumers, but the European economy as a whole that suffers when fraud is rife. These crimes do not operate in isolation: they move fluidly across digital platforms, payment systems, and communication channels, exploiting every weak link in what we call the 'scam chain.'

Our extensive research and frontline work with fraud victims gives us unique insights into the consumer-facing dimensions of this crisis. Our surveys show that 74% of consumers believe tackling online financial scams should be a top priority for this legislative term[1], and 4 out of 5 respondents report having encountered a scam online[2]. The emotional and financial impacts are often severe, with some experiencing long-term distress and insecurity. Yet our work reveals alarming gaps in how victims are supported, how platforms prevent fraudulent advertising, and how different stakeholders coordinate their responses.

This response draws on our research, complaint handling experience, and advocacy work, including our collaboration with the Global Anti-Scam Alliance, to provide evidence-based recommendations for the Action Plan. We focus particularly on areas where we have deep expertise: victim support and protection, platform accountability for fraudulent advertising, and coordination mechanisms that can bridge the gaps between stakeholders.

The Victim Support Crisis: Why Current Frameworks Are Failing

Nowhere is the inadequacy of current responses more apparent than in the treatment of victims of fraud. Our research reveals a system that is failing at every level. Just over half of the victims we surveyed did not seek help after being scammed. When we asked why, over one in five said they didn't think anything could be done. Among those who did report to police, 25% of cases were closed without follow-up, and one in five victims received no response at all.[3]

1 https://www.euroconsumers.org/wp-content/uploads/2024/05/Euroconsumers-Election-Survey-report.pdf
2 https://www.euroconsumers.org/wp-content/uploads/2024/12/Caught-in-the-web-Navigating-the-digital-maze-of-scams.pdf
3 https://www.euroconsumers.org/wp-content/uploads/2024/12/Caught-in-the-web-Navigating-the-digital-maze-of-scams.pdf

These statistics reflect more than bureaucratic inefficiency. They represent real people experiencing trauma, financial hardship, and a profound sense of abandonment by the systems meant to protect them. The emotional and financial impacts of fraud are often severe and long-lasting, yet victim support remains patchy or absent in many Member States. There is no consistency in how victims are treated, no guarantee that they will receive the help they need, and no systematic approach to preventing re-victimisation.

The Scale of the Problem: Real Cases from the Field

To understand the urgency and scale of this crisis, consider just a sample of cases that reached our Belgian member organisation Testachats in a single week:

- A scam using a fake compliance service of a well-known Belgian bank: €100,000
- Investment fraud via a fraudulent investment company called Arbitrum: €25,000
- A call impersonating CardStop (Belgium's card blocking service) to 'secure' accounts: €13,000
- An email impersonating Argenta bank to update personal data: €4,000
- Fraudulent advertisement on a second-hand goods platform (2ndHand.be): €2,270

This is merely a quick anthology from one week in one country. Behind these numbers are real people, including elderly victims who have lost their entire life savings to sophisticated fraud schemes. Each case represents not just financial loss, but profound psychological trauma, shattered trust, and in many cases, devastating impacts on victims' quality of life and sense of security.

The Action Plan must recognise that addressing fraud is not only about preventing crimes or prosecuting criminals. It is fundamentally about supporting the people who have been harmed. At the 2024 and 2025 Global Anti-Scam Summits, we consistently stressed the need for long-term assistance to those affected, not just reactive responses.[4] Our work has documented the ongoing trauma and vulnerability experienced by scam victims and the critical lack of follow-up services to support recovery.

Breaking Down Silos: Coordination and Information Sharing Across the Scam Chain

Perhaps the most fundamental challenge in combating online fraud is that responses remain fragmented while frauds themselves operate seamlessly across platforms, payment systems, and jurisdictions. No single stakeholder can effectively combat fraud alone. The scam chain involves advertisers and platforms that facilitate initial contact, telecommunications providers whose networks carry spoofed calls and messages, payment processors that handle fraudulent transactions, and often multiple jurisdictions

4 https://www.youtube.com/watch?v=nExriWwmtNw ; https://www.gasa.org/post/victim-impact-building-support-for-scam-victims-global-anti-scam-summit-london-2025

where different elements of the operation are located. Without coordinated action, fraudsters simply shift to the weakest link.

Our work with the Global Anti-Scam Alliance and our advocacy for national fraud hotlines reflect a broader recognition that effective anti-fraud efforts require coordination mechanisms that currently do not exist. When a victim contacts a fraud hotline, that single entry point must be able to coordinate responses across law enforcement, financial regulators, payment providers, platforms, and telecommunications companies. When a platform identifies a fraudulent advertiser, that information should flow to payment providers who can freeze associated accounts, to telecommunications companies who can block associated numbers, and to other platforms where the same fraudster may be operating. In this way, it is critical that the Action Plan clarifies the obligations and liabilities of the different stakeholders across the scam chain, including proactive detection, scam takedown obligations, and escalation processes.

Coordinated Enforcement: From Individual Support to Collective Action

Effective coordination must extend beyond information sharing to include coordinated holistic enforcement action. For example, the Digital Services Act provides crucial tools for holding platforms accountable, but enforcement must be stepped up and coordinated across Member States. Similarly, we must ensure that enforcement does not target only one aspect of a scam. We need effective coordinated enforcement for the whole scam chain, up to taking down illegal scam compounds. All authorities, from telecommunications to financial, to law enforcement and beyond need to work together, seamlessly. To that, the Action Plan should strive to facilitate coordinated enforcement between the relevant authorities at a national, European and International level. Only then will we be successful in tackling international scam networks.

Euroconsumers is committed to enforcement actions at multiple levels:

First, on an individual level, we provide direct legal support to scam victims. Our Spanish member OCU has designed a specific legal service: for small-scale fraud cases, formal intervention with banks, pointing out their legal duties under the Payment Services Directive often leads to quick resolution. For higher-value or more complex cases, OCU provides full legal support, including representation by OCU lawyers through judicial proceedings.[5]

Second, by handling individual cases, we identify structural problems requiring systemic responses. Our Belgian member Testachats, for instance, identified patterns with specific banks that consistently refused to reimburse victims. Rather than continuing only on an individual basis, Testachats selected exemplary cases against two specific Belgian banks

5 https://www.ocu.org/phishing

and brought them to court. These court decisions create strong judicial precedents that can be used whenever these banks refuse reimbursement again, making them think twice before denying legitimate claims. Both cases were won, though one bank continues to appeal.[6]

Third, we pursue collective action when platforms or services facilitate fraud at scale. The Booking.com case exemplifies this approach. When we began receiving significantly more complaints about the booking platform, scammers impersonated Booking.com after obtaining user data from the platform's environment. We filed a complaint with the Dutch Data Protection Authority and launched a call for other victims to come forward. Many did and now we are working to ensure compensation for all victims, hold Booking accountable, and deliver a sense of justice to those who were harmed harmed.[7]

This multi-level enforcement strategy, from individual legal support to strategiclitigation to collective action, demonstrates what is possible when consumer organisations have the resources and legal frameworks to hold bad actors accountable. The Action Plan should support and strengthen such enforcement mechanisms across the EU.

A Multi-Stakeholder Coordination Framework

Alongside this, the Action Plan should outline a new multi-stakeholder framework for coordination. This should include digital platforms and marketplaces, payment service providers, telecommunications operators, law enforcement and regulatory authorities, consumer protection organisations, and victim support services. The mechanism should not be merely consultative but operational to facilitate real-time information sharing, joint response protocols for large-scale fraud incidents, and coordinated enforcement action.

Such coordination requires common frameworks that currently do not exist. Stakeholders use different definitions of fraud, different classification systems, different reporting formats, and different timelines for action. The Commission should develop common definitions and typologies for fraud classification that allow stakeholders to communicate clearly about what they are seeing and what responses are needed. Joint response protocols should establish who does what, when, and how information flows between parties during fraud incidents.

Creating a centralised contact point for fraud victims, as we have advocated through national fraud hotlines, would also facilitate this coordination.[8] Rather than victims navigating complex referral chains between different authorities and private sector entities, a single point of contact could coordinate responses across all relevant stakeholders, ensuring nothing falls through the cracks and that each party takes appropriate action within their sphere of responsibility.

6 https://www.test-achats.be/argent/comptes-a-vue/news/phishing-les-banques-rechignent-a-rembourser
7 https://www.euroconsumers.org/fraud-booking-com-share-scam-stories/ ; https://www.euroconsumers.org/wp-content/uploads/2025/06/Booking.com-complaint.pdf
8 https://www.euroconsumers.org/urgent-back-up-needed-introduce-national-fraud-hotlines-for-scam-victims/

Critically, these hotlines must be more than crisis response mechanisms. They need to provide long-term support, including counselling services to address psychological trauma, financial advice for managing post-fraud situations, ongoing protection from re-victimisation through scam awareness education, and connection to peer support networks. This should be done in collaboration with consumer organisations, like ours, who have on-the-ground experience in working with fraud victims during these difficult periods.

National Scam Centres: A Comprehensive Coordination Model

Euroconsumers believes the Action plan must go beyond a victim-focused perspective to actively shape the broader infrastructure needed to tackle scams systematically. Euroconsumers has been at the forefront of advocating for National Anti-Scam Centres (NASCs). These are comprehensive coordination hubs that go far beyond simple victim reporting hotlines. Together with the Global Anti-Scam Alliance (GASA), Cifas, and PwC, we contributed to the report 'Uniting Against Fraud: How Anti-Scam Centres Can Strengthen National Fraud Defences', which sets out a detailed blueprint for how these centres can transform fragmented national responses into coordinated, effective anti-fraud ecosystems.[9] National Anti-Scam Centres represent a structural response that matches the sophistication and cross-border nature of modern fraud.

Beyond Hotlines: The NASC Model

While victim support hotlines are important, National Anti-Scam Centres address the fundamental challenge that responses to fraud remain fragmented while frauds themselves operate seamlessly across platforms, payment systems, and jurisdictions. As our research with PwC identified, no single organisation holds all the data, capabilities, or authority needed to tackle fraud effectively. NASCs provide the missing infrastructure to combine data, intelligence, resources, and expertise from multiple organisations into a response greater than the sum of its parts.

National Anti-Scam Centres can serve multiple critical functions:

- Facilitating centralised fraud reporting with 'report it once' models, eliminating the need for victims to navigate complex referral chains across multiple organisations
- Coordinating intelligence and data sharing across public and private sectors, enabling faster detection of emerging fraud patterns and more coordinated responses
- Supporting public-private collaboration on anti-fraud strategy, standards, and best practices, ensuring all stakeholders work from common frameworks
- Providing access to consistently high-quality victim support, ensuring victims receive appropriate care regardless of which organisation they first contact

9 https://www.euroconsumers.org/wp-content/uploads/2025/11/Uniting-against-fraud.pdf

- Leading awareness and prevention campaigns with coordinated messaging across sectors
- Driving disruption initiatives including takedowns of fraudulent websites, blocking of scam phone numbers, and rapid freezing of accounts across multiple institutions
- Supporting law enforcement with enhanced analytical capabilities, cross-sector intelligence, and coordination for investigations
- Enabling international cooperation through clearly defined points of contact for cross-border anti-fraud activities.

In our 'Uniting Against Fraud' report, we identify how NASCs can address eight critical challenges in current fragmented approaches: siloed ecosystems, misaligned standards and investment decisions, slow data sharing, confusing fraud reporting, lack of victim support, inconsistent public awareness campaigns, limited scope for disruption, and purely national responses to increasingly transnational threats.

Crucially, NASCs must include experienced consumer organisations, like Euroconsumers, as equal partners in their governance and operations. Consumer organisations bring irreplaceable perspective and capabilities to the anti-fraud ecosystem: we maintainvictims; trusted relationships with victims; we understand the practical barriers that prevent reporting and recovery; we identify patterns from ground level complaints that may not appear in official statistics; and we provide ongoing support through the complex aftermath of fraud. Without genuine consumer organisation involvement in NASCs' strategic decision-making, coordination mechanisms and victim support pathways, these centres risk becoming technocratic structures disconnected from the human realities of fraud. This is evident in international NASC models across the globa. For example, Australia's NASC explicitly involves consumer advocacy groups both on its advisory board and in its fusion cells.[10]

The Role of AI: Challenges and Opportunities

Artificial intelligence has fundamentally transformed the fraud landscape, creating both severe challenges and promising opportunities for consumer protection.

AI as an Enabler of Fraud

Scammers have rapidly adopted AI tools to enhance their operations. Thanks to ChatGPT and similar large language models, phishing emails no longer contain telltale spelling and grammar mistakes that once helped consumers identify scams. Technology enables scammers to meticulously duplicate bank websites with pixel-perfect accuracy. Most concerningly, AI-powered deepfakes can now convincingly replicate the faces and voices of people we trust including family members, colleagues, or public figures.

10 https://www.nasc.gov.au/what-we-do/how-were-run

The sophistication has reached a point where traditional 'spot the signs' advice is becoming obsolete. If phishing emails have become indistinguishable from legitimate communications thanks to ChatGPT, if bank websites can be meticulously recreated, if catfishers and fake profiles on dating websites can be manipulated through in-depth social engineering, we must acknowledge that AI-generated content is already too good to be reliably recognised by average consumers, and will only improve further.

AI as a Tool for Protection

However, the same technologies that empower scammers can also strengthen consumer defenses. Emerging research and applications demonstrate AI's protective potential:

- Early studies show that large language models could help consumers detect and prevent phishing emails. In experiments, LLMs have successfully encouraged users who received attractive discount offers to verify them with companies' official websites.
- AI-powered chatbots can empower people against scams around the clock. Since scammers work continuously across borders and time zones, 24/7 access to support is essential.
- AI can recognise unusual behaviour patterns in banking apps and flag suspicious transactions. For instance, an 80-year-old suddenly spending €30,000 on cryptocurrency might trigger protective interventions.
- There are even proposals to 'scam the scammers' using AI, by monitoring dark web conversations to learn and predict scammer tactics, creating fake profiles to waste scammers' time, and actively disrupting their operations.

Despite these opportunities, deepfakes remain a significant challenge. We must acknowledge that we don't yet have software solutions that can reliably protect consumers against sophisticated deepfakes. However, history provides reason for optimism. Twenty years ago, computer viruses represented the greatest threat to digital security, and we developed increasingly effective antivirus solutions. Similarly, we believe and indeed have a moral duty to ensure that effective countermeasures to deepfakes will emerge in the coming years.

The critical caveat is that this will be an ongoing arms race: every time we deploy AI for protection, scammers will attempt to counter it with even more sophisticated techniques. The Action Plan must therefore support continuous research, development, and deployment of AI-based protective technologies, while recognising that technological solutions alone cannot substitute for robust legal frameworks and coordinated enforcement.

Beyond Education: A Realistic Approach to Awareness and Prevention

Our organisations[11] already work extensively on consumer awareness, but we must be realistic about what education can achieve. Fraudsters exploit behavioural biases and psychological vulnerabilities that cannot simply be overcome through better information. The sophistication of modern social engineering, the use of AI for impersonation, and the emotional manipulation tactics employed mean that even highly informed consumers can fall victim to well-executed scams.

This is not to say awareness campaigns have no value—they play an important supporting role and should be continued with adequate funding. However, the Action Plan must recognise that education alone is insufficient. Consumer protection cannot be solely the responsibility of consumers to protect themselves. This is why we emphasise structural measures: platform accountability for fraudulent advertising, payment system safeguards that create friction at critical moments, burden of proof shifts that recognise institutional responsibilities, and victim support systems that provide help when prevention fails.

Importantly, awareness efforts should be coordinated at EU level to ensure consistent messaging, avoid duplication of effort, and share best practices about what actually works. The Commission should provide funding that recognises prevention is more cost-effective than response, while maintaining realistic expectations about what awareness alone can achieve.

11 See: **OCU – Organización de Consumidores y Usuarios (2024)**, *Postura OCU: fraudes online*. https://www.ocu.org/info/postura-ocu-fraude-online; **Test Achats (2023)**, *Oplichterij via internet: bescherm jezelf*. https://www.test-aankoop.be/familie-prive/webshops/dossier/oplichterij-via-internet; **Altroconsumo (2020)**, *Phishing: 8 consigli per stare tranquilli.* https://www.altroconsumo.it/hi-tech/antivirus/consigli/phishing-8-consigli-per-stare-tranquilli; **DECO PROteste (2024)**, *Phishing: o que é e como se deve proteger*. https://www.deco.proteste.pt/dinheiro/contas-ordem/dicas/phishing-que-e-como-se-deve-proteger

Conclusion: Toward a Comprehensive Response

Online fraud is no longer a peripheral consumer protection issue—it is a structural challenge undermining trust in the digital economy and causing severe harm to millions of Europeans. The Commission's Action Plan represents a critical opportunity to establish a comprehensive, coordinated response that addresses the full scam chain rather than isolated elements.

Victims are being failed by fragmented support systems that leave many without help. The Action Plan must be ambitious in scope while practical in implementation.

We urge the Commission to:

1. Ensure the Action Plan addresses the entire scam chain with clear obligations for all intermediaries
2. Prioritise victim support and compensation
3. Establish robust coordination mechanisms among all stakeholders (e.g. national anti-scam centres involving consumer organisations)
4. Support research and deployment of AI-based protective technologies while maintaining robust legal frameworks to address AI-enabled fraud
5. Step up coordinated enforcement across industry sectors and support multi-level enforcement actions from individual legal support through collective action.

Euroconsumers stands ready to contribute our expertise and experience throughout the development and implementation of this Action Plan. Our research, complaint handling, and advocacy work provide valuable insights into both the scale of the problem and the practical measures needed to address it. We urge the Commission to seize this opportunity to fundamentally reimagine how Europe responds to online fraud—not as isolated institutions each doing their part, but as a coordinated ecosystem working together to protect consumers, support victims, and restore trust in the digital economy.

The cost of inaction continues to rise—not only for individual victims, but for the European economy and society as a whole. This Action Plan must be backed by political will, adequate resources, and sustained commitment to making meaningful change. We look forward to continuing engagement on this critical initiative.


euroconsumers
GROUP
Empower people,
improve the market.
ALTROCONSUMO
DECO PROTeste
ocu
testachats
testaankoop
euroconsumers | Polska