Communications Consumer Panel

Response from the Communications Consumer Panel and ACOD to Ofcom's Consultation: Combatting Mobile Messaging Scams

Who we are

The Communications Consumer Panel, established by the Communications Act 2003, is a group of independent experts with direct sectoral experience. We ensure the citizen and consumer voice is represented in communications policy development and we have dual membership with Ofcom's Advisory Committee for Older and Disabled People.

The Panel pays particular attention to underserved communities, people with access requirements, and people who may be more susceptible to harm, and the needs of micro businesses, which have many of the same challenges as individual consumers.

We commission research, provide advice, and encourage Ofcom, governments, industry, and others to look at issues through the eyes of consumers, citizens, and micro businesses.

Four members of the Panel also represent the interests of consumers in England, Northern Ireland, Scotland, and Wales, respectively. They consult with the key stakeholders in each Nation to understand the perspectives of consumers in all parts of the UK and input these perspectives to the Panel's consideration of issues.

Our response

In October 2025, we welcomed the opportunity to respond to Ofcom's consultation on proposals to strengthen protections against scam calls originating from abroad that spoof UK mobile numbers, changing its guidance to set out how it expects providers to process calls from abroad that appear to come from UK mobile (+447) numbers.

We strongly supported Ofcom's continued efforts to reduce the harm caused by scam calls and commended the proposed amendments to the Caller Line Identification (CLI) Guidance, urging Ofcom to continue to use its robust research and analysis and regulatory powers, to strengthen consumer protection from scams.

Ofcom's latest consultation document highlights that scammers are still able to reach victims "at mass scale" using mobile messaging via SMS ('text' messages), OTT messaging (over-the-top messaging services), spoofed sender IDs, and malicious links across channels.

We believe that Ofcom's proposals to set new rules and guidance aimed at combatting mobile messaging scams, represents a proposed additional layer in the protective armour of UK consumers, citizens, and micro-businesses, against exploitation from criminals intercepting and misusing systems that were designed to enable innocent people to connect with each other and with the services to which they require access.

January 2026

We support Ofcom’s depth of analysis into consumer harms from scams and the clarity of expectations set out in their guidance for providers and third parties. The proposed new General Conditions and accompanying guidance aim to create a consistent, mandatory baseline of protections across mobile operators and business messaging aggregators, tackling both access routes used by scammers and weaknesses in current industry practice. This is consistent with Ofcom’s observation that one of the sector’s most persistent problems is *inconsistent application of counter-scam measures* across providers.

The Panel strongly supports this objective and would advise Ofcom to proceed to implementation without delay. However, we also stress the need to ensure that implementation does not inadvertently harm legitimate users, particularly microbusinesses (including sole traders), who depend on low-cost messaging solutions and underpin the economic growth of the UK.

Overall Assessment of Ofcom’s Proposals

The Panel agrees that the proposed direction of travel - mandatory rules, clearer obligations, and enhanced enforcement - is vital, given the volume and impact of scams, the variety of methods and channels used, and the inconsistency of industry approach to tackling scams.

Scams cause deep emotional and financial harm, with victims often being older people, digitally excluded groups, and the smallest of the UK’s businesses with limited resilience and resource.

As highlighted in our response to Ofcom’s previous consultation, the effect of scams on a consumer or business is not solely felt at the time of impact but can be experienced more deeply through a lack of trust in communications services or providers and an underlying feeling of shame and self-distrust.

While mandatory counter-fraud measures are welcome, we encourage Ofcom to ensure the overall regime remains:

- Accessible and fair for legitimate microbusiness users, many of whom rely on low volume bulk messaging or cost-effective PAYG SIMs for operational purposes.
- Transparent, so consumers and microbusinesses not familiar with technical jargon understand why messages may be blocked or challenged.
- Non-discriminatory, avoiding unintended consequences for minority-language messaging (including the Welsh language), accessibility related services, or small third sector organisations.
- Flexible enough to distinguish and allow legitimate, genuine calls, such as from UK residents roaming abroad, while stopping fraudulent traffic.
- Funded by industry, without the costs being passed on to consumers – particularly PAYG customers, who are often less able to benefit from the full range of details offered in the marketplace, due to poor credit.

Person to Person Fraud Disruption Measures

Ofcom proposes that mobile operators must implement volume limits on new Pay as you Go (PAYG) SIMs to prevent criminals from using cheap SIM cards to send high volumes of fraudulent messages.

The Panel supports this measure with safeguards:

- Limits should be evidence based and adjustable, reviewed at least annually.
- Operators should provide clear escalation routes for legitimate high-volume PIN based or alert messaging by small charities, medical practices, community groups, and microbusinesses.
- Aggressive rate limiting must not disrupt high-volume accessibility uses—for example, assistive technology devices sending frequent automated texts.

We note that these measures draw on existing best practice already deployed by proactive operators, but which is uneven across the industry.

Mandatory Blocking and Traffic Monitoring

We understand that Ofcom requires both Mobile Network Operators (MNOs) and aggregators to:

- Block numbers, URLs (links) and sender IDs identified in scam reports.
- Identify scam messages "in transit" based on malicious patterns.
- Use customer, law enforcement, and third-party reports to trigger blocking actions.

The Panel strongly supports this requirement, but recommends:

1. **Transparency obligations**
   Consumers and microbusinesses should receive meaningful explanations when messages they send or receive are blocked, including routes for appeal. This avoids confusion and reassurance seeking behaviours that scammers might exploit.

2. **Accessible redress**
   Ofcom should require operators to maintain a fast, low burden review process for legitimate senders who are incorrectly blocked and should unblock legitimate traffic expeditiously without financial detriment to senders.

3. **Recordkeeping and audit trails**
   We support Ofcom's emphasis on recordkeeping as mentioned in industry summaries of the consultation and encourage Ofcom to standardise audit requirements to ensure accountability. We believe that this should include monitoring against unintended consequences, as set out in this response.

Application to Person (A2P "Business Messaging") Due Diligence Requirements

Ofcom proposes strengthened requirements such as:

- Enhanced Know Your Customer (KYC) at onboarding.
- Verification and protection of sender IDs.

- Ongoing traffic monitoring to detect ‘abnormal’ patterns.

The Panel supports these proposals; however:

- Microbusinesses must not face disproportionate onboarding burdens or costs.
- A2P aggregators should be required to provide plain language onboarding guidance for microbusiness senders.
- Ofcom should explore a tiered approach, where very small organisations undergo simplified but still robust checks.
- There should be a simple Allow-List verification process to authenticate genuine traffic using KYC checks.
- Given the role A2P channels play in impersonation scams, strong ID validation is essential—but legitimate small entities must not be deterred from using secure communications channels due to administrative friction.

Proportionality for micro-businesses

We have briefly highlighted our concerns for microbusinesses. To unpack this, we would highlight to Ofcom that micro-businesses often have limited digital literacy, no dedicated IT/telecoms staff, and minimal margin for disruption. Some categories of micro-businesses rely more on mobile communications to run their business, for example, business owners that do not operate from an office, or that operate from a location where broadband connectivity is unreliable. All communications with such businesses should be capable of being performed on a mobile device.

We encourage Ofcom to mandate clear, accessible guidance from operators and aggregators explaining how KYC checks work, what traffic-monitoring flags mean, how to avoid inadvertent blocking and how to challenge mistaken labelling of legitimate traffic.

Consumer Awareness Measures

While Ofcom’s consultation focuses on operator responsibilities, clear consumer facing communication is essential.

We recommend a consistent, cross operator awareness campaign, with inclusion of accessibility formats (BSL, Easy Read). We also recommend targeted outreach to third parties that represent or support groups of consumers disproportionately targeted by scammers.

Experience shows that when scam traffic is denied using a particular technology or methodology, scammers quickly adapt and seek alternative means to continue operating. Operators should be prepared for such adaptations and be quick to brief both consumers and businesses on such novel scams.

Monitoring, Enforcement, and Continuous Evaluation

The Panel supports Ofcom’s proposed monitoring and enforcement under General Condition C.9 and Non-Provider Condition 3, supported by Ofcom’s existing statutory powers.

We recommend:

- Annual publication of scam blocking effectiveness metrics, including false positives and false negatives.
- A commitment to periodic review, recognising that scammers adapt rapidly and that measures must evolve accordingly.
- Industry-wide consistency checks to address current disparities in protective measures, which Ofcom has identified as a major issue.
- An agile approach to enforce mandatory protections to protect microbusinesses and consumers.
- Monitoring of the process to an extent where Ofcom can satisfy itself that costs of the changes are not passed on to consumers, particularly those who may be less likely to be able to afford additional costs.

Conclusion

The Communications Consumer Panel supports Ofcom's proposals to introduce stronger, mandatory protections against mobile messaging scams. These proposals clearly address the scale of harm caused to UK consumers and businesses, the gaps Ofcom has identified in the current voluntary, inconsistent approach and the need for robust action across both P2P and A2P messaging channels.

We believe Ofcom should proceed with its proposals and should not be deterred by industry pushback on these vital consumer protection measures.

We also emphasise the importance of ensuring that:

- Protective measures do not place disproportionate burdens on microbusinesses.
- Legitimate communications are not unintentionally disrupted,
- Consumers receive transparent explanations and accessible means of redress,
- Operators and aggregators maintain clear accountability for their anti-scam systems,
- Costs are not passed on to consumers,
- Networks still allow legitimate UK residents roaming abroad, calling home, to display their numbers

We look forward to continued collaboration with Ofcom to ensure that the final regulatory framework achieves the intended reduction in scam messaging, while preserving the accessibility and reliability of messaging services for all users.

January 2026