<u>Stop Scams UK's response to the Ofcom consultation: Protecting people from illegal harms online</u>

Stop Scams UK is grateful for the opportunity to contribute to Ofcom's consultation on protecting people from illegal harms online. Our submission introduces the work of Stop Scams UK and sets out our position on the proposed duties. Our response complements the consultation responses submitted by our members and should be read in conjunction with those. This response also provides answers to specific questions asked by the consultation. These are at **Annex A.**

We fully recognise the breadth of online harms covered by the consultation but note that as a membership organisation set up with the express purpose of stopping scams at source, our response to the questions in this consultation is limited to those that have explicit relation to scams and fraud.

Stop Scams UK

Stop Scams UK is an industry-led collaboration made up of responsible businesses from across the banking, technology and telecoms sectors who have come together to help stop scams at source. Stop Scams UK exists to facilitate cross-sector collaboration.

For a scam to be successful, it will touch on at least two, if not each, of the banking, technology, and telecoms sectors. We believe that it is only through enabling, leading, and delivering collaboration across these sectors that systemic solutions to scams will be realised. Stop Scams UK provides the resource, leadership, and trusted space for our members to share problems, identify opportunities, overcome barriers and drive projects forward to the benefit of consumers and business.

Stop Scams UK has 27 members, with more in the process of joining. Current members include: ANNA Money, Amazon, AnyDesk, Barclays, BT, Chase, the Co-operative Bank, Gamma, Google, HSBC, Lloyds Banking Group, Meta, Metro Bank, Modulr Finance, Monzo, Nationwide Building Society, NatWest, Santander, Starling, Paragon, TalkTalk, TeamViewer, Three, Tide, TSB and VISA.

Our members cover over 95% of the UK's online searches, 80% of online advertising and 70% of messaging services used in the UK, as well as significant mobile and fixed broadband connectivity.

Our work focuses on measures that either protect consumers or prevent scams from happening in the first instance. In September 2021, we launched 159, an easily memorable short code phone service that connects the customers of the majority of UK retail banks directly, safely and securely with their bank, should they receive an unexpected or suspicious call about a financial matter. Over 450,000 calls have now been made to 159.

In addition to 159, Stop Scams UK is delivering a substantive programme of work to enable and pilot improved data sharing between our members. This includes work on Scam Intelligence, engaging directly with the scammers, which has already successfully identified over 7000 active mule accounts, with annualised savings estimated at £8.8m. Data Sharing has been identified by policymakers and industry as key to tackling the scams emergency, including in the recently published UK Fraud Strategy. Our work in this area also includes enabling Banks to report fraudulent content to technology companies, specifically through our FIRE project with Meta.

Introduction to Stop Scams UK's position

Stop Scams UK strongly supports the ambitions of the Online Safety Act and the proposed plans for implementation put forward by Ofcom for consultation. Fraud accounts for almost 40% of reported crime and unfortunately, online services are all to often the conduit through which such fraud and scams are perpetrated despite the consistent efforts of many service providers.

We commend Ofcom's thorough assessment of the causes and impacts of online harms in the UK. These attest to the urgent need for the more effective regulation of the UK's digital environment. In the face of these harms, we support the content and purpose of Ofcom's proposed duties, recognising the importance of more robust governance processes, accountability measures, and comprehensive oversight in combating scams and fraudulent activities online.

We share Ofcom's confidence that mandating specific governance processes and oversight for scams and fraud in the largest firms offering online U2U and Search platforms will help ensure a more robust response to fraud online, ensuring the issue becomes and remains a priority concern for those organisations' most senior decision makers. In conjunction with other legislation either under way or pending but set out in the government's fraud strategy published in May 2023, we believe the proposed duties have the potential to reduce the threat of scams currently faced by all UK consumers, who in a digitised post-covid world depend on the internet for many of their professional and social interactions.

However, Stop Scams UK, in line with the views of our members affected by the proposals, advocate for a dynamic and flexible approach when it comes to prescribing the specific systems and techniques organisations should use for moderation and content removal. While techniques such as keyword search and hash matching are useful tools, many of the largest 'category 1' services will already use these techniques to a degree, and in some instances have already developed more efficient and effective technologies.

Furthermore, scammers are dynamic and sophisticated criminals, and are often able to find ways to bypass or beat detection and moderation systems through ingenuity and innovation. We would therefore suggest Ofcom ensures that there is adequate flexibility in duties that prescribe specific technologies or systems in order to enable organisations who are on the front line to keep pace with the sophisticated and evolving nature of online scams and fraud in the UK.

For this reason, Stop Scams UK underscores the need for continuous collaboration, monitoring, and adaptation throughout the process of the duties implementation, to take account for the dynamic and evolving nature of scams and other types of online harm. We also recognise that the regulatory approach is untested so urge caution and a proportionate approach to implementation.

Ongoing partnership between regulators, industry stakeholders, and law enforcement agencies will be key to the success of the new regulatory regime. Stop Scams UK was formed to bring about collaboration of this sort, across different sectors affected by fraud, and we remain committed to collaborating with all concerned parties to develop and maintain a comprehensive and effective framework that allows firms the space to be dynamic, while enforcing stricter governance and accountability processes that help keep consumers safe. Getting this balance right will ensure a fair and balanced digital environment for all.

Your response

Volume 2: The causes and impacts of online harm

Ofcom’s Register of Risks

Question 1:

i) Do you have any comments on Ofcom’s assessment of the causes and impacts of online harms?

Response: Ofcom's assessment of the causes and impacts of online harms is comprehensive and well evidenced. The identification of over 130 priority offences and the categorisation of these into 15 broad kinds of illegal harm provides for a structured approach to understanding the landscape of online harm. The statistics presented, such as those on the prevalence of scams and frauds encountered by adult internet users and the increase in URLs containing Child Sexual Abuse Material reported to the IWF, effectively highlight the severity and urgency of addressing the issue.

ii) Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.

Response: While the analysis covers a wide range of illegal harms, there may be some areas that warrant further exploration. For instance, while the report acknowledges the role of pseudonymity and anonymity in emboldening offenders, further research could explore the nuances of such factors.

Understanding how different levels of anonymity contribute to specific types of harmful behaviour could provide useful insights that provide for more targeted mitigation strategies. Additionally, given the evolving nature of technology and its impact on online harms, it might be beneficial to include discussion of emerging risks (as well as the benefits) associated with technologies like generative AI, which, used inappropriately, have the potential to exacerbate existing challenges.

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

Question 2:

i) Do you have any views about our interpretation of the links between risk factors and different kinds of illegal harm? Please provide evidence to support your answer.

Response: Ofcom's interpretation of the links between risk factors and different kinds of illegal harm aligns with our understanding of the scams landscape and the most up to date research on scam types and journeys.

Similarly, the recognition of pseudonymity and anonymity as emboldening offenders corresponds to our understanding of how fraudsters exploit such technology and services to conceal their identities and perpetrate scams.

The identification of file-sharing services and specific functionalities like recommender systems as posing risks for disseminating fraudulent content also correlates with our understanding of scammers methods.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Volume 3: How should services assess the risk of online harms?

Governance and accountability

Question 3:	
i)	Do you agree with our proposals in relation to governance and accountability measures in the illegal content Codes of Practice?
Response: Stop Scams UK supports Ofcom's proposals regarding governance and accountability measures as set out in the illegal content Codes of Practice. Robust governance processes are crucial for effectively identifying and managing online safety risks, particularly in the context of combating scams. By ensuring services are accountable to senior governance bodies and mandating the implementation of measures such as written statements of responsibilities for staff, tracking evidence of illegal content, and establishing Codes of Conduct for employees, these proposals provide a structured framework for embedding accountability, that will help ensure services are proactive in managing the risks and protecting users from online fraud and scams.	
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 4:	
i)	Do you agree with the types of services that we propose the governance and accountability measures should apply to?
Response: Yes	
ii)	Please explain your answer.
Response: Stop Scams UK agrees with the types of services that Ofcom proposes the governance and accountability measures should apply to. These measures are essential for ensuring that all services, regardless of size, play a role in mitigating online harms and combating scams. We recognise the importance of a proportional approach, which minimises the regulatory burden on smaller platforms, but are clear on the role that even smaller services can play in helping halt (or enable) the dissemination of fraudulent content. Therefore, the inclusion in the duties, of a requirement for a senior accountable officer for all services, including U2U and search services, helps promote accountability across the digital landscape. By implementing these measures universally, Ofcom is able to foster a collective responsibility among all service providers to uphold online safety standards and protect users from scams.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

Question 5:	
i)	Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to requiring services to have measures to mitigate and manage illegal content risks audited by an independent third-party?
Response: N/A	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Question 6:	
i)	Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to tie remuneration for senior managers to positive online safety outcomes?
Response: N/A	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Service’s risk assessment

Question 7:	
i)	Do you agree with our proposals?
Response: Yes	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: Stop Scams UK largely agrees with Ofcom's proposals regarding risk assessments. The four-step risk assessment process outlined provides a structured and proportionate approach for services to identify and mitigate online harms, including scams. By understanding the specific risks associated with their platforms, services can implement targeted safety measures to protect users. Additionally, the provision of Risk Profiles and guidance on the types of evidence to consider in risk assessments offer valuable resources for services to navigate their legal obligations effectively.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Specifically, we would also appreciate evidence from regulated services on the following:

Question 8:	
i)	Do you think the four-step risk assessment process and the Risk Profiles are useful models to help services navigate and comply with their wider obligations under the Act?
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Question 9:	
i)	Are the Risk Profiles sufficiently clear?
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Do you think the information provided on risk factors will help you understand the risks on your service?
Response: N/A	
iv)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
v)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Record keeping and review guidance

Question 10:	
i)	Do you have any comments on our draft record keeping and review guidance?
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Question 11:	
i)	Do you agree with our proposal not to exercise our power to exempt specified descriptions of services from the record keeping and review duty for the moment?
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Volume 4: What should services do to mitigate the risk of online harms

Our approach to the Illegal content Codes of Practice

Question 12:	
i)	Do you have any comments on our overarching approach to developing our illegal content Codes of Practice?
Response: Stop Scams UK acknowledges and appreciates Ofcom's structured and systematic approach to developing the Illegal Content Codes of Practice, starting with the most egregious harm where most regulatory gain is to be had. It is evident that the proposed recommendations aim to address the diverse range of illegal harms prevalent in online spaces, promoting a safer digital environment for users.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 13:	
i)	Do you agree that in general we should apply the most onerous measures in our Codes only to services which are large and/or medium or high risk?
Response: Yes	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: Stop Scams UK largely agrees with the proposal to apply the most onerous measures in the Codes to services that are large and/or medium or high risk. This approach ensures that regulatory interventions are proportionate to the potential scale of the harm found on the services. This approach prioritises user safety while considering the operational capacities of different platforms. We believe that this approach strikes the right balance between the needs of business and the urgent need to ensure that consumers are better protected, and the gateways available to fraudsters are closed.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 14:	
i)	Do you agree with our definition of large services?
Response: Yes	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: Stop Scams UK supports the definition of large services proposed by Ofcom, which aligns with international standards such as those outlined in the Digital Services Act by the EU.	

This alignment facilitates consistency across regulatory frameworks and minimises the compliance burden on services operating in multiple jurisdictions. We believe this is crucial to help facilitate and enable common and shared approaches to tackling scams internationally.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 15:
i) Do you agree with our definition of multi-risk services?
Response: Yes
ii) Please provide the underlying arguments and evidence that support your views.
Response: Stop Scams UK agrees with the definition of multi-risk services proposed by Ofcom. Identifying services as multi-risk based on their susceptibility to multiple kinds of illegal harms demonstrates that Ofcom recognises certain services may pose diverse risks to users, that are not solely based on their size, requiring different mitigation strategies.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 16:
i) Do you have any comments on the draft Codes of Practice themselves?
Response: N/A
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A

Question 17:
i) Do you have any comments on the costs assumptions set out in Annex 14, which we used for calculating the costs of various measures?
Response: N/A
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A

Content moderation (User to User)

Question 18:
i) Do you agree with our proposals?
Response: In line with our members who run category 1 U2U services, Stop Scams UK supports a dynamic and flexible approach to content moderation, ensuring that platforms remain equipped

to combat forms of online harm that are likely to evolve quickly and, potentially, in unanticipated ways, effectively.
ii) Please provide the underlying arguments and evidence that support your views.
Response: The methods set out by Ofcom include hash matching and keyword search. We note the in the case of many large search services, these methods are either already in use or have been replaced by more complex and sophisticated moderation techniques. Ofcom will need to ensure that it takes account of such developments. As we note elsewhere in response to this consultation, fraudsters and scammers are dynamic and sophisticated criminals. They use innovative techniques and are often able to find ways to bypass or beat detection and moderation systems. We therefore suggest Ofcom make sure there is adequate flexibility in duties relating to search moderation, to make sure that the organisations who are on the front line, are able to keep pace with the sophisticated and evolving nature of scams and fraud.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Content moderation (Search)

Question 19:
i) Do you agree with our proposals?
Response: In line with our members who run category 1 Search services, Stop Scams UK advocates for a dynamic and flexible approach to content moderation, ensuring that platforms remain equipped to combat evolving forms of online harm effectively. We refer Ofcom to the responses of those members which include Amazon, Google and Meta.
ii) Please provide the underlying arguments and evidence that support your views.
Response: See answer to question 18.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Automated content moderation (User to User)

Question 20:
i) Do you agree with our proposals?
Response: In line with our members who run category 1 U2U services, Stop Scams UK advocates for a dynamic and flexible approach to content moderation, ensuring that platforms remain equipped to combat evolving forms of online harm effectively.
ii) Please provide the underlying arguments and evidence that support your views.
Response: See answer to question 18
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

Question 21:	
i)	Do you have any comments on the draft guidance set out in Annex 9 regarding whether content is communicated 'publicly' or 'privately'?
Response: N/A	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Do you have any relevant evidence on:

Question 22:	
i)	Accuracy of perceptual hash matching and the costs of applying CSAM hash matching to smaller services;
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Question 23:	
i)	Ability of services in scope of the CSAM hash matching measure to access hash databases/services, with respect to access criteria or requirements set by database and/or hash matching service providers;
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Question 24:	
i)	Costs of applying our CSAM URL detection measure to smaller services, and the effectiveness of fuzzy matching for CSAM URL detection;
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.

Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Question 25:	
i)	Costs of applying our articles for use in frauds (standard keyword detection) measure, including for smaller services;
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Question 26:	
i)	An effective application of hash matching and/or URL detection for terrorism content, including how such measures could address concerns around 'context' and freedom of expression, and any information you have on the costs and efficacy of applying hash matching and URL detection for terrorism content to a range of services.
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Automated content moderation (Search)

Question 27:	
i)	Do you agree with our proposals?
Response: In line with our members who run category 1 Search services, Stop Scams UK advocates for a dynamic and flexible approach to content moderation, ensuring that platforms remain equipped to combat evolving forms of online harm effectively.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: See answer to question 18	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

User reporting and complaints (U2U and search)

Question 28:	
i)	Do you agree with our proposals?
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Terms of service and Publicly Available Statements

Question 29:	
i)	Do you agree with our proposals?
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Question 30:	
i)	Do you have any evidence, in particular on the use of prompts, to guide further work in this area?
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Default settings and user support for child users (U2U)

Question 31:	
i)	Do you agree with our proposals?
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: N/A

Question 32:

i) Are there functionalities outside of the ones listed in our proposals, that should explicitly inform users around changing default settings?

Response: N/A

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: N/A

Question 33:

i) Are there other points within the user journey where under 18s should be informed of the risk of illegal content?

Response: N/A

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: N/A

Recommender system testing (U2U)

Question 34:

i) Do you agree with our proposals?

Response: Yes

ii) Please provide the underlying arguments and evidence that support your views.

Response: We generally support Ofcom's proposal for U2U services to collect safety metrics during on-platform tests of their recommender systems, especially for those identified as medium or high risk for specified harms. Stop Scams UK is supportive of these measures. These safety metrics will enable services to assess whether changes to their recommender systems increase user exposure to illegal content, thereby allowing them to make more informed design choices and mitigate online harm effectively.

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

Question 35:

i) What evaluation methods might be suitable for smaller services that do not have the capacity to perform on-platform testing?

Response: N/A
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:- N/A

We are aware of design features and parameters that can be used in recommender system to minimise the distribution of illegal content, e.g. ensuring content/network balance and low/neutral weightings on content labelled as sensitive.

Question 36:
i) Are you aware of any other design parameters and choices that are proven to improve user safety?
Response: N/A
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A

Enhanced user control (U2U)

Question 37:
i) Do you agree with our proposals?
Response: Yes
ii) Please provide the underlying arguments and evidence that support your views.
Response: Stop Scams UK is strongly in favour of initiatives that give consumers greater control of their online experience. Empowering users with greater agency over what they see, who they can block and who gets to interact with their content, is a crucial part of rebuilding consumer trust in the UK's digital environment.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A

Question 38:
i) Do you think the first two proposed measures should include requirements for how these controls are made known to users?
Response: N/A
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A

Question 39:

i)	Do you think there are situations where the labelling of accounts through voluntary verification schemes has particular value or risks?
Response: N/A	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

User access to services (U2U)

Question 40:	
i)	Do you agree with our proposals?
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Do you have any supporting information and evidence to inform any recommendations we may make on blocking sharers of CSAM content? Specifically:

Question 41:	
i)	What are the options available to block and prevent a user from returning to a service (e.g. blocking by username, email or IP address, or a combination of factors)?
Response: N/A	
ii)	What are the advantages and disadvantages of the different options, including any potential impact on other users?
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Question 42:	
i)	How long should a user be blocked for sharing known CSAM, and should the period vary depending on the nature of the offence committed?
Response: N/A	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

There is a risk that lawful content is erroneously classified as CSAM by automated systems, which may impact on the rights of law-abiding users.

Question 43:	
i)	What steps can services take to manage this risk? For example, are there alternative options to immediate blocking (such as a strikes system) that might help mitigate some of the risks and impacts on user rights?
Response: N/A	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Service design and user support (Search)

Question 44:	
i)	Do you agree with our proposals?
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Cumulative Assessment

Question 45:	
i)	Do you agree that the overall burden of our measures on low risk small and micro businesses is proportionate?
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Question 46:	
i)	Do you agree that the overall burden is proportionate for those small and micro businesses that find they have significant risks of illegal content and for whom we propose to recommend more measures?
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.

Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Question 47:	
i)	We are applying more measures to large services. Do you agree that the overall burden on large services proportionate?
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Statutory Tests

Question 48:	
i)	Do you agree that Ofcom's proposed recommendations for the Codes are appropriate in the light of the matters to which Ofcom must have regard?
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Volume 5: How to judge whether content is illegal or not?

The Illegal Content Judgements Guidance (ICJG)

Question 49:	
i)	Do you agree with our proposals, including the detail of the drafting?
Response: Mostly	
ii)	What are the underlying arguments and evidence that inform your view?
Response: Stop Scams UK mostly supports the detail of the ICJG, but urges Ofcom to consider the unique difficultly in identifying fraudulent content. Unlike other forms of illegal content such as CSAM, fraudulent media is designed to appear as lawful content, and in many cases the advert or entry point for a scam journey will not be breaking the law at all. This is a vital distinction we urge Ofcom to consider as it finalises the guidance. Shaping the process of identifying and removing fraudulent content will require more time, collaboration and flexibility than any other form of illegal media, if inadvertent consequences such as unduly cautious approach that sees lawful content blocked or removed are to be avoided.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Question 50:	
i)	Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?
Response: Yes	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: We believe Ofcom’s guidance is sufficiently accessible, but due to the complexity around defining fraudulent content set out in our answer to question 49, it is likely that the guidance will need to be evolved. The accessibility and usefulness of the guidance, especially in relation to fraud, will be dependent on the consistent evaluation of its effectiveness, which must be done through constant collaboration between Ofcom and the firms subject to the ICJG.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Question 51:	
i)	What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?
Response: N/A	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: N/A

Volume 6: Information gathering and enforcement powers, and approach to supervision.

Information powers

Question 52:	
i)	Do you have any comments on our proposed approach to information gathering powers under the Online Safety Act?
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

Enforcement powers

Question 53:	
i)	Do you have any comments on our draft Online Safety Enforcement Guidance?
Response: Stop Scams UK appreciates the clarity provided in the draft Online Safety Enforcement Guidance. The emphasis on driving compliance, protecting users from harm, and holding wrongdoers accountable resonates with our mission to Stop Scams at Source. We also appreciate the clear timelines Ofcom have provided for enforcement actions, but we also encourage continued consultation with stakeholders to refine the guidance and address any potential gaps or ambiguities.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Annex 13: Impact Assessments

Question 54:	
i)	Do you agree that our proposals as set out in Chapter 16 (reporting and complaints), and Chapter 10 and Annex 6 (record keeping) are likely to have positive, or more positive impacts on opportunities to use Welsh and treating Welsh no less favourably than English?
Response: N/A	
ii)	If you disagree, please explain why, including how you consider these proposals could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	