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?
Section 6N (Proceeds of Crime offences) makes the connection between money mule activity and the laundering of fraud proceeds. Although fraud is the largest predicate offence for money-laundering, it is important to note that money muling is also a method used to launder the proceeds of other proceeds-generating crimes, such as drug trafficking, human trafficking and cyber-crimes such as ransomware attacks. [See, for example: Money Mules (also known as Squaring) | West Yorkshire Police] Furthermore, there is some evidence of child financial exploitation, in the form of young money mule recruitment, in the laundering of the proceeds of online child sexual exploitation platforms (see for example: Money Mule Scheme Targets Teenagers and Young Adults — FBI.	
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 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: N/A	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

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: N/A	
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: N/A	

Question 4:	
i)	Do you agree with the types of services that we propose the governance and accountability measures should apply to?
Response: N/A	
ii)	Please explain your answer.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/A	

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: We would suggest a minor amendment to **Annex 5** (Service Risk Assessment Guidance) to add 'relevant industry groups' to the 'enhanced inputs' section.
ii) Please provide the underlying arguments and evidence that support your views.
We would suggest a minor amendment to **Annex 5** (Service Risk Assessment Guidance) in terms of the suggested 'enhanced inputs' under **section A5.100** ('What Information to Assess'). We would suggest amending the final category (Engaging with relevant representative groups) to include 'and relevant industry groups'. Evidence to support this inclusion – in the counter-fraud community there are a number of public-private groups (such as the Joint Money Laundering Intelligence Taskforce – JMLIT) and multi-sector intelligence communities (such as those run by Cifas and other 'Specified Anti-Fraud Organisations') who regularly convene to share information around fraud risk. These are key fora in the UK's counter-fraud defences and recognised in the government's Economic Crime Plan and Fraud Strategy. By including a reference to 'relevant industry groups' these specific fora can be considered as an enhanced input into the risk assessment framework.
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?

While we recognise that the wording of the Act places specific obligations on Ofcom to provide clear guidance on what constitutes compliance, we feel that the current approach to the development of the Codes – being very specific on inputs and measures, rather than outcome-focussed - may lead to a 'tick box' approach to compliance.

In our experience of the application of regulations in the anti-financial crime sphere, such an approach may lead to a 'lowest common denominator' approach to compliance, rather than one which genuinely shifts corporate cultures in the spirit which Parliament intended when passing the legislation.

To achieve the intended effect, it may be useful to consider supplementing the current measures in the Codes with a requirement that larger firms take a more outcomes-focussed approach to implementation. This could potentially be achieved by requiring firms, as part of the annual risk assessment process, to draw up an impact assessment of the impact of measures taken in the previous period and document these as part of the cycle of risk assessment.

We would also flag a general concern that the current approach in the Codes is overly focussed on business size as the primary indicator of risk and harm. We have seen in the anti-financial crime space, particularly as regards financial services regulation, that such an approach risks driving threats to smaller platforms over time.

Furthermore, in respect of online platforms – a rapidly evolving and increasing fragmented sphere - such an approach may fail to adequately take into account the way in which specific threat actors will naturally gravitate towards niche platforms to target specific demographics.

Finally, we would note that if a platform finds itself with a declining user base, thus falling below the threshold, it may, conversely, be at greater rather than lesser risk of abuse given that declining income may lead to a greater inclination to loosen controls and allow more risk onto the platform.

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?

In general, we agree that applying more onerous measures to businesses which present a higher risk is the right approach. Indeed, the application of a 'risk-based approach' to regulation is an

approach which has precedent in a number of other realms, including the anti-money laundering (AML) regime.

However, as we expand on below in our answer to question 14, we believe the current basis on which the more onerous measures are assigned is overly quantitative (user base, number of crime types) and, in the absence of more contextual and qualitative assessments, may be too blunt an approach for assessing the complex and often rapidly morphing range of societal harms which the legislation is seeking to challenge.

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

Response: We recognise that introducing more qualitative factors into such a broad ranging document would be challenging. However, we feel it is important to supplement the quantitative approach with some qualitative measures to ensure that smaller platforms where a high volume of very specific threats crystallise are adequately captured by the provisions.

One way to ensure that the Codes could remain responsive to high volume/single threats would be to allow room in the Codes for Ofcom to reduce quantitative thresholds (such as user base) in respect of specific functionality and/or industry segment in the event that law enforcement and industry evidence suggests that the real-world harms facilitated by a particular functionality/segment make it proportionate to do so.

For example, in the case of fraudulent content, if a specific new fraud modus operandi emerges on a specific type of U2U platform which has under 7 million users, but can be shown by law enforcement data to be causing significant harm and loss to victims, the Codes should be flexible enough to apply the more onerous measures to this specific platform type.

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: No – we believe the bar set in the draft Codes is too high and may exclude a number of high-risk sectors for fraud. We also do not agree with the assessment that revenue cannot be used as a basis for assigning higher onus measures, given precedents available in the AML regime which use revenue as a basis.

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

Although we understand the reasons for arriving at the figure of 7 million monthly users, we do not agree that this figure will, in and of itself, in all instances, achieve the policy intention of ensuring that those most able to bear the costs apply the more onerous measures.

We disagree with the consultation's conclusion that the user base assessment should not be balanced against some calculation of available resources. For example, other areas of government regulation, such as the Economic Crime Levy (see: Prepare for the Economic Crime Levy - GOV.UK (www.gov.uk)) have adopted a balance between revenue and business size as their basis.

We believe that simply adopting a user basis as the sole measure of a 'large service' may result in unfair outcomes in some circumstances. For example, theoretically a social interest company presenting a low risk of illegal content, but with a 7 million user base could be required to apply

greater measures than a high revenue company with a 6 million user base presenting a high risk of a single threat.

Furthermore, from the specific perspective of fraud, according to research by Which?, the proposed definition of a 'large service' currently excludes the majority of dating platforms and a number of the major e-commerce marketplaces, both of which could be said to be a medium to high risk for fraud.

While dropping the current threshold on a wholesale basis to account for very specific risks and harms may not be proportionate, as with our response to question 12, it would be desirable to build in some flexibility into the Codes to combine qualitative and quantitative factors where necessary and proportionate. This could include reducing user thresholds in certain sectors and segments in response to evidence of real-world harms.

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, but using this in isolation of qualitative factors as the basis for more onerous measures may lead to unintended outcomes.
ii) Please provide the underlying arguments and evidence that support your views.
Although the definition itself – being of medium to high risk of two or more different types of illegal content - appears to strike the right balance, we have wider concerns (as noted also in our answer to question 14) about the general gap created by only applying the more onerous measures to large and/or multi-risk services. For example, by using 'multi-risk' as the basis for some of the higher-level measures, there is a risk that platforms which neither meet the definition of a 'large' service nor the 'multi-risk' threshold, but which present a high risk for one specific type of illegal content may be out of scope of more onerous measures. From a fraud and financial crime specific perspective the two following examples may illustrate this point: - A social media service is consistently shown by data to be the primary conduit for young money mule recruitment in the UK but does not display any risk for other priority illegal content and has a user base of 6 million per month. - A dating service with a user base of 2 million per month is consistently targeted by scammers to reach victims but does not display any other priority crime type risk. Although these examples are theoretical, they serve to illustrate the impact of relying too heavily on quantitative measures alone. Therefore, as our above response to question 13, we believe the Codes should have the flexibility to apply more onerous measures to platforms who present a high-volume risk of a single form of illegal content, either via a new 'high volume' category or by allowing for a flexible approach to user base definition in a specific area.
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?
<u>Specific comments on the fraud measures</u> We support the inclusion of fraud-specific measures in the Codes of Practice given the scale and impact of fraud on UK consumers and businesses. However, we do not believe that the measures proposed in the Codes go far enough to provide the 'proportionate response' required of firms by the Online Safety Act 2023.

In detail, although we support the inclusion of the fraud keyword searching proposal, we would point out that this measure serves to mitigate only one of the identified priority fraud offences (making or supplying articles for use in frauds) and other 'crime as a service' postings. Postings and messages in relation to other offences, such a fraud by misrepresentation (e.g. online scams) rarely have identifiable keywords and work by masquerading as legitimate posts or businesses. These posts would be unlikely to be detected by keyword detection technology. Please see our response to question 20 for more detail.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

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: 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

Content moderation (Search)

Question 19:
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

Automated content moderation (User to User)

Question 20:
i) Do you agree with our proposals?
- We believe URL detection should be extended to fraudulent websites - We believe the keyword detection technology in isolation will have limited impact and should be supplemented with an outcomes focussed/technology agnostic approach.
ii) Please provide the underlying arguments and evidence that support your views.
URL Detection We believe that URL detection technology should also be extended to the area of fraud. We believe this could be implemented in a cost-effective way by firms linking into an existing scam website services freely available online, including those supported by Cifas, the Cyber Defence Alliance and others. See: Free Website Scam Checker - Check a website by Get Safe Online **Keyword searching for fraud:** As noted in our response to question 16, we are of the view that this measure will only impact one specific form of fraud occurring on platforms. We therefore believe this should be supplemented with other measures. As regards the specificity of the proposal we would raise two issues regarding the proposed measure itself. First, the success of a keyword detection tool will be dependent on live and active knowledge of the terminology being used by the criminal community. In our experience, criminals in the fraud fraternity are quick to adapt to system changes and will simply change wording to evade controls. The proposed 6-monthly review of keywords is therefore likely to be insufficient. We would propose a more frequent review period. As well as your proposal that platforms engage with 'relevant experts' to inform their keyword detection process, we would suggest that relevant platforms should be required to consider engagement in existing multi-sector data and intelligence sharing mechanisms to keep their understanding of the prevailing terminology up to date. Second, we have concerns that by stipulating a single specific technology solution, the Codes may have the unintended consequence of stifling innovation in the counter-fraud technology field. We would recommend that the Codes take a technology-agnostic approach, focussing the requirements on achieving specific outcome (identifying fraudulent content), rather than focussing on a single piece of technology. In this way the Codes may have the effect of actively driving innovation in this field, rather than stifling it. In terms of an outcome-focussed approach, the technologies should be focussed on identifying perpetrators via 'red flag' indicators rather than exclusively focussing on the content in isolation. Again, we believe that these solutions can be provided by innovation in the market and supported by intelligence available via existing multi-sector fora.
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: As per our response to question 20 we believe it would be easy and cost effective to include known scam websites in automated search content moderation and de-indexing by linking to the free online scam website checker data. Free Website Scam Checker - Check a website by Get Safe Online	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: This information is already collected and readily available.	
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: **Direct Complaints from Consumers – Identity Fraud** We think it is proportionate for larger platforms to put in place specific processes and complaints channels for dealing with account takeover and identity fraud. **Trusted Flaggers** We believe that Specified Anti-Fraud Organisations (SAFOs) and relevant industry bodies with an intelligence function should be added to the list of 'trusted flaggers' for the purposes of the dedicated reporting channel. We also think that there should be an onus on two-way intelligence sharing.	

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

Direct Complaints from Consumers – Identity Fraud

As regards direct complaints from consumers, we think it is proportionate for larger platforms to put in place specific processes and complaints channels for dealing with account takeover and identity fraud.

Our views are based on Cifas data which shows a year on year increase in identity fraud – in 2022 alone we received 277,000 reports of identity fraud, 86% of which occurred through online channels (See for evidence: Fraudscape 2023 - Cifas).

There are also numerous cases and reports showing the role social media account hacking places in fraud, particularly investment fraud (See for evidence: Instagram scams: "I was hacked and blackmailed on social media" (stylist.co.uk)).

We believe that platforms should be required to support victims to 'repair' their identities, including by signposting to government guidance (see: Identity fraud victims' checklist (actionfraud.police.uk)).

Dedicated Reporting Channels ('Trusted Flaggers')

We agree with the proposal that larger platforms should be required to established dedicated reporting channels for 'trusted flaggers'. However, we feel that the list of trusted flaggers should include SAFOs and other relevant industry groups with an intelligence function.

In detail, section 68 of the Serious Crime Act 2007 established a category of bodies corporate known as 'Specified Anti Fraud Organisations' (SAFOs), who are bodies corporate designated by the Secretary of State for the Home Office by Order. (see: The Serious Crime Act 2007 (Specified Anti-fraud Organisations) Order 2008 (legislation.gov.uk)).

In effect the legislation creates a specific set of trusted organisations with whom public bodies may share counter-fraud information.

Information shared with SAFOs is covered by a statutory Code of Practice to ensure any information shared strikes the right balance between countering fraud and the rights of individuals. (See: Data Sharing for the Prevention of Fraud (publishing.service.gov.uk)).

SAFOs, in their role as data intermediaries, hold a unique position in the counter-fraud landscape enabling them to recognise and flag emerging threats and issues as they emerge, often more quickly than is visible to law enforcement.

Beyond this additional, we feel that the 'Trust Flagger' gateway should be reciprocal and not simply a one-way channel. By encouraging two-way data-sharing, the Codes can encourage platforms to play an active role in the counter-fraud community.

For this reason, are per our responses to questions above, we feel that larger platforms should be encouraged by the Code to engage in existing multi-sector data and intelligence sharing mechanisms. This will encourage them to flag new and emerging threats to other system participants further down the value chain and, in doing so, target harden the UK's defences against fraud.

It is our view that only by creating channels for reciprocal data and intelligence sharing between all system participants will the legislation be able to achieve its aim of reducing the harms of online fraud.

iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Terms of service and Publicly Available Statements

Question 29:	
i)	Do you agree with our proposals?
Response: It may be useful for services to include 'fair processing notices' regarding the sharing of data for fraud and anti-money laundering purposes.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: In addition to the existing terms of service statements suggested, it may be useful for larger platforms who wish to engage in multi-sector data and intelligence-sharing to consider including fraud 'fair processing notices' (FPN) within their standard user service statements. For an example of a fraud FPN see: Fair Processing Notices for Cifas FPNs for fraud data-sharing are a common standard for financial sector businesses and could easily be adopted as best practice by platforms within their terms of service.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

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: 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 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: Platforms with a medium or high risk of fraud should be required to offer users the option to block messaging from all non-connected accounts.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Direct messaging is a key way in which criminals perpetrating fraud make contact with their victims, particularly with regard to high-harm frauds such as romance and investment fraud. Offering users this ability may offer some control, particularly to prevent re-victimisation.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 38:
i) Do you think the first two proposed measures should include requirements for how these controls are made known to users?
Response: In line with our response to question 28 we feel that alongside the ability for consumers to flag potential illegal content and identity fraud, complaints channels should be required to offer specific advice to consumers on how to apply controls in such a way as to reduce fraud risk. More generally, we feel that the Codes should place a specific onus on high-risk platforms to proactively provide consumer education and guidance on how to protect themselves from fraud. This would bring the expectations in line other sector-led responses to consumer protection and education, such as the financial services sector.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 39:	
i)	Do you think there are situations where the labelling of accounts through voluntary verification schemes has particular value or risks?

It is important that any verification scheme adheres to a high set of common standards to avoid offering false authenticity. This is because of growing evidence than some monetised verification schemes are being abused by criminals to build their credibility.

For example, when social media company X/twitter implemented its monetised 'blue tick' verification scheme this was implemented without any mandated identity verification measures and, thus, created an illusion of authenticity and trust, which strengthen the scammers position. See: Elon Musk's Twitter Blue Verification Is a Gift to Scammers | WIRED UK

We do not believe it is sufficient to require platforms to simply have in place policies and procedures alongside public information as a means of mitigating this risk.

We believe that monetised schemes should be required to adhere to the same set of standards required by identity service providers in the government's draft Digital ID Trust Framework in order to avoid a two-tier system of regulation. [UK digital identity and attributes trust framework alpha v1 (0.1) - GOV.UK (www.gov.uk)]

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

Response: No

User access to services (U2U)

Question 40:	
i)	Do you agree with our proposals?

Response: We believe that it would be proportionate to require platforms to block users who they can reasonably infer are perpetrating fraud or conspiring to perpetrate fraud.

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

Response: Given the scale of harm caused by fraud to UK consumers and businesses, we feel it would be proportionate for platforms to be required to block users who they can 'reasonably infer' are perpetrating or conspiring to perpetrate fraud against other users.

We respect that this measure requires a careful balance between protecting the public from harm and the rights of individuals. We would therefore suggest that the obligation is, in the first instance, limited to instances where a user has been flagged by a 'trusted flagger' via a 'Dedicated Reporting Channel' (see response to question 28) and the platform is given reasonable cause to infer that the user is perpetrating fraud.

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

Response: No

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: We agree with the proposal to require small businesses that find they have significant risks of illegal content to take more measures.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: As per our response to question 12, there is a risk of displacement of fraudulent content from larger to smaller platforms given the way in which the Code measures have been developed to focus on platform size as an indicator of risk. We can envisage a future situation where criminals adapt and move to smaller platforms to evade controls. It is therefore essential that where a small business is seen to have a very high risk that the Codes apply more measures to mitigate against this displacement risk.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 47:	
i)	We are applying more measures to large services. Do you agree that the overall burden on large services proportionate?
Response: Given the evidence of the scale of the harms to the public we believe the proposal to require the larger services to take more action to be proportionate.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: See above	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

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: Yes	
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: We agree with the proposal to create a 'filter' system to apply the judgement of fraud by false representation, in effect creating 'red flags' by which services can 'filter' content. However, we do not believe that the current approach taken in the Codes – that of Ofcom supplying a list of 'red flag' indicators – is right one as it will result in red flags being out of date by the time they are published.	
ii)	What are the underlying arguments and evidence that inform your view?
Response: We believe that it is proportionate to expect the larger platforms to participate in existing multi-sector data and intelligence sharing mechanisms, through which they are easily able to access live intelligence and indicators of risks to support them in developing their own context-specific red flag indicators. Relying on a 'point in time' list of red flag indicators will leave platforms at risk, when compared with access to live time data and intelligence from a cross-section of the counter-fraud community. Requiring platforms to take active steps to identify their own set of context-specific red flags (rather than relying on the supervisor) would bring this regulation into line with the regulation of other sectors, specifically the financial sector, in relation to their responses to financial crime risks. Furthermore, as per our general response regarding the use of proactive technologies, beyond fraud keyword detection technology, we believe that platforms should be working actively to develop in-house or procure external technologies which work specifically with their own individual contexts to identify risk within their user base.	

iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 50:	
i)	Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?
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 51:	
i)	What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?
Response: We believe existing counter-financial crime information and data sharing services, both in the public and private sectors, should be deemed 'reasonably available information' and should be referred to in the Illegal Content Judgement Guides. The counter-fraud community has a number of long-established data and intelligence sharing services in place to facilitate the sharing of knowledge, data and information relating to financial crime. This includes the National Crime Agency's Joint Money Laundering Intelligence Taskforce (JMLIT) and industry-led groups and data sharing mechanisms, including those administered by Cifas. These multi-sector fora have been facilitating the management of fraud risk across a number of sectors for many years and are a well-established part of the risk mitigation measures taken in the financial, communications and other sectors. We believe that the availability and long-established history of such responses means that they represent 'reasonably available information' for the larger platforms. As such, we believe that the availability of data and intelligence from such schemes should be referred to specifically in the Illegal Content Judgement Guide.	
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: 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	

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	