

Your response

Please refer to the sub-questions or prompts in the [Annex](#) of our Call for Evidence.

NB we have shaded questions identified in the Call for Evidence as being aimed at providers of services in grey.

Question	Your response
Question 1: Please provide a description introducing your organisation, service or interest in Online Safety.	<p>Confidential? – N</p> <p>As the financial services and markets conduct regulator, as well as the money laundering supervisor for the financial sector, we have a keen interest in reducing fraud. Our statutory objective of protecting and enhancing the integrity of the UK financial system expressly includes ensuring that the financial system is not used for purposes connected to financial crime.</p> <p>Our work to tackle fraud takes a variety of forms but includes action to address:</p> <ul style="list-style-type: none">• fraudulent activity undertaken, or facilitated by, firms which we authorise or regulate• unauthorised persons describing themselves or holding themselves out as authorised• unauthorised persons unlawfully engaging in regulated activities or communicating financial promotions. <p>We protect consumers through a broad range of consumer awareness initiatives designed to ensure consumers are less susceptible to financial services scams, including those which they may encounter online. We do this by empowering consumers to better protect themselves from scams. This is a two- step process – firstly communicating the warning signs of a scam, such as with time pressures, unsolicited contact, too good to be true offers etc, and secondly, driving the use of our tools such as the Warning List and FS Register.</p> <p>FCA and online fraud</p> <p>The threat from online fraud continues to grow, with fraudsters finding it easier to reach potential victims online than with more traditional channels. We had over 36,300 enquiries about possible scams from March 2021 – March 2022, an increase of a third on enquiries over the same period in 2020 (27,700).</p> <p>We have engaged intensively with platforms to help drive reductions in online investment fraud. Some have recently taken action to help prevent illegal advertising on their sites and we expect others to implement solutions this year.</p> <p>However, while this is welcome, negotiation and persuasion can only get us so far. Substantial and permanent change requires clear legal obligations to be</p>

placed on platform operators to protect consumers. The Online Safety Bill includes vital measures to tackle fraud related offences in user generated content and on search engines. This includes:

- Designation of content relating to fraud-related offences as priority illegal content; and
- Inclusion of a standalone duty on certain platforms to tackle fraudulent content contained within paid-for advertising

We look forward to continuing to work with the Government to support the Bill continuing its passage through Parliament at the earliest opportunity in the Autumn, in order to ensure that consumers have much needed protection against online fraud.

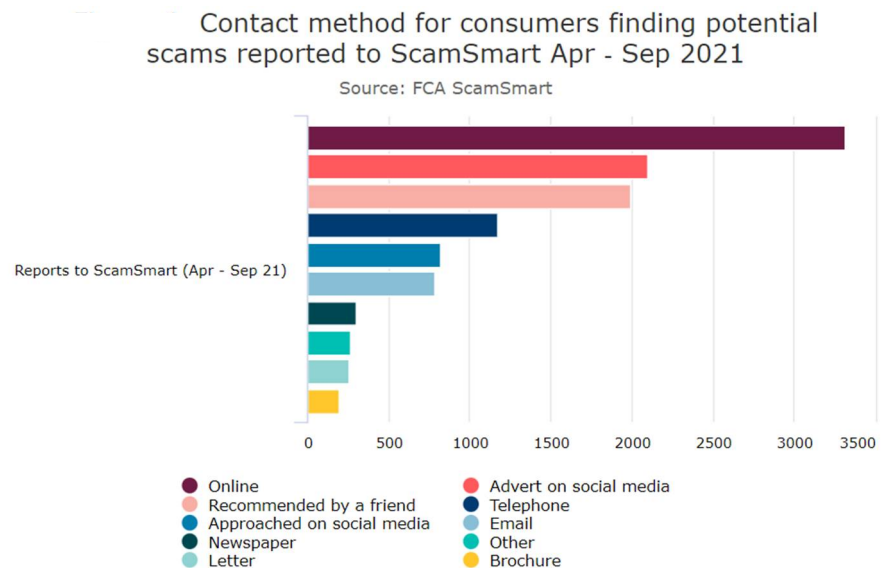
Question 2: Can you provide any evidence relating to the presence or quantity of illegal content on user-to-user and search services?

Confidential? N

Evidence re the presence of illegal content on services.

The rapid growth of online platforms over recent years has created new opportunities for criminals. These platforms provide low-cost and fast access to potential victims on an industrial scale which was not previously possible through traditional, offline channels.

The figure below shows that ScamSmart¹ users report online channels as the most common method of encountering potential scams (29%), with adverts on social media (19%) the next most common method.



¹ FCA’s campaign providing information on how to avoid investment and pension scams

<p>Question 3: How do you currently assess the risk of harm to individuals in the UK from illegal content presented by your service?</p>	<p>Confidential? – Y / N N/a</p>
<p>Question 4: What are your governance, accountability and decision-making structures for user and platform safety?</p>	<p>Confidential? – Y / N N/a</p>
<p>Question 5: What can providers of online services do to enhance the clarity and accessibility of terms of service and public policy statements?</p>	<p>Confidential? – Y / N N/a This has not been the focus of our work with online platforms. We are however very happy to share with Ofcom the results of our own work on consumer understanding and strengthening of financial promotions regulation.</p>
<p>Question 6: How do your terms of service or public policy statements treat illegal content? How are these terms of service maintained and how much resource is dedicated to this?</p>	<p>Confidential? – Y / N N/a</p>

<p>Question 7: What can providers of online services do to enhance the transparency, accessibility, ease of use and users' awareness of their reporting and complaints mechanisms?</p>	<p>Confidential? N</p> <p>Users of online services should make it as easy as possible to report problem content. All platforms should provide easy to access portals or alternative reporting tools and mechanisms where concerns can be flagged. These should be easy to find and easy for consumers to complete.</p> <p>Salience and users' awareness:</p> <ul style="list-style-type: none"> • Platforms could use pop-up windows to remind and encourage consumers to report problematic content. • Platforms should ensure that tools used to report harms are prominently displayed and easy for vulnerable consumers to use. For example, information located near the top of a page is likely to be more effective at getting attention than information positioned at the bottom of a page (Bergstrom & Schall, 2014 - Eye tracking in user experience design). FCA research found increasing text size, displaying text on a red background and featuring it in the main body of a communication as opposed to the small print – appeared to increase comprehension (FCA research note – Going beyond “capital at risk”.) <p>Ease of use and accessibility:</p> <ul style="list-style-type: none"> • Platforms could also reduce the number of steps involved in reporting and complaints mechanisms. For example, they could also try to reduce friction by avoiding requiring further logins or redirection to a third party where the customer must register or use other logins. • Where information is needed from the customer, platforms could provide a list upfront of what they will need to have to complete the report and/or complaint.
<p>Question 8: If your service has <u>reporting or flagging</u> mechanisms in place for illegal content, or users who post illegal content, how are these processes designed and maintained?</p>	<p>Confidential? – Y / N</p> <p>n/a</p>
<p>Question 9: If your service has a <u>complaints</u> mechanism in place, how are these processes designed and maintained?</p>	<p>Confidential? – Y / N</p> <p>n/a</p>

<p>Question 10: What action does your service take in response to <u>reports</u> or <u>complaints</u>?</p>	<p>Confidential? – Y / N</p> <p>n/a</p>
<p>Question 11: Could improvements be made to content moderation to deliver greater protection for users, without unduly restricting user activity? If so, what?</p>	<p>Confidential? – N</p> <p>We think that there are many improvements which could and should be made to content moderation to deliver greater protection for users, without restricting user activity unduly. An important principle should be that, if platforms do not have the technology to successfully complete automated checks of content, then human moderation must be introduced to provide adequate protection. It will therefore be essential to have clear and timely processes for escalating to human moderators when appropriate.</p> <p>The following are all examples of improvements which could be made to content moderation without unduly restricting user activity:</p> <p>Effective ID verification checks:</p> <p>Comprehensive checks to verify the identity of persons who seek to advertise. The nature of these checks will depend on the nature of the person and the products they wish to advertise but may include any or all of the matters covered in the below bullet points.</p> <ul style="list-style-type: none"> • Checking that promotional content relating to regulated financial services, including adverts are from/approved by an FCA authorised person (in line with s21 Financial Services and Markets Act 2000). Platforms can use the FCA’s online FS Register which is a public record of firms regulated by us, to check whether the firm wishing to advertise is authorised. They can also use the FS Register to check the firm approving the advert is authorised. • The platform could check claims that an advert has been approved by a particular authorised firm by double-checking with the approving firm directly. • Verifying the identity and credentials of an advertiser (both FCA authorised and non-authorised) by checking details at Companies House and checking that the firm is not on the FCA warning list. • Checking if the firm is registered with the Charities Commission (since scammers will sometimes claim to be a charity). • Checking with the Insolvency Practitioner’s register if they claim to be a registered Insolvency Practitioner and the Solicitors Regulation Authority if they claim to be a practicing solicitor. • Having appropriate measures/systems in place to check an FCA authorised person is who they say they are, rather than a clone. <p>Effective content verification checks</p> <p>Effective and comprehensive checks of advertisements prior to ‘going live’. The nature and extent of the checks will depend on the products or services that are intended to be advertised. Having clear criteria to establish the risks</p>

	<p>associated with the financial product/service being promoted will be key to understanding the nature of the checks that are proportionate to be carried out on the proposed content.</p> <p>Proactive monitoring</p> <p>Platforms should have systems to facilitate proactive monitoring of illegal content so that if illegal content does slip through ID and content verification/gateway checks, it is nevertheless likely to be picked up once the content has gone live. This is important to support reporting by consumers or other third-party users and will be key to implementing appropriate protections for consumers, given that it is unlikely that all illegal content will be stopped prior to it going live without making the verification/gateway process unwieldy.</p>
<p>Question 12: What automated moderation systems do you have in place around illegal content?</p>	<p>Confidential? – Y / N</p>
<p>Question 13: How do you use human moderators to identify and assess illegal content?</p>	<p>Confidential? – Y / N</p>
<p>Question 14: How are sanctions or restrictions around access (including to both the service and to particular content) applied by providers of online services?</p>	<p>Confidential? – N</p> <p>One of the key changes we have seen by providers of online services was Google’s new policy, which they implemented in late summer 2021. This aimed to prevent advertisers who were not authorised by the FCA, or whose advert had not been approved by an FCA authorised firm, from being able to place adverts for regulated financial services.</p> <p>This has proved to be successful in preventing fraudulent adverts on their site, as highlighted by research from TSB. This research found that none of TSB’s account holders had fallen victim to any illegal adverts on Google since they changed their policy. The success of Google’s policy change shows the potential positive impact of the OSB, should all platforms be required to adopt a similar approach.</p> <p>Other platforms, however, have not fulfilled their public commitment to prevent fraudulent content on their sites. Therefore, we believe that criminals may be migrating from Google to other platforms’ advertising services. We engage regularly and intensively with these platforms but are</p>

	<p>disappointed that the pace of change is slow. The OSB is therefore needed to be enacted as soon as possible to ensure that they are subject to clear, legal requirements and drive the major changes which are needed.</p>
<p>Question 15: In what instances is illegal content removed from your service?</p>	<p>Confidential? – Y / N</p>
<p>Question 16: Do you use other tools to reduce the visibility and impact of illegal content?</p>	<p>Confidential? – Y / N</p>
<p>Question 17: What other sanctions or disincentives do you employ against users who post illegal content?</p>	<p>Confidential? – Y / N</p>
<p>Question 18: Are there any functionalities or design features which evidence suggests can effectively prevent harm, and could or should be deployed more widely by industry?</p>	<p>Confidential? N</p> <p>As highlighted above (Q14), Google’s change in policy (to only allow adverts from FCA authorised firms or approved by one) has proved to be successful in preventing fraudulent adverts and so we would welcome more platforms taking this approach. TSB found that none of its account holders had fallen victim to an illegal advert on Google since they changed their policy.</p>
<p>Question 19: To what extent does your service encompass functionalities or features designed to mitigate the risk or impact of harm from illegal content?</p>	<p>Confidential? – Y / N</p>

<p>Question 20: How do you support the safety and wellbeing of your users as regards illegal content?</p>	<p>Confidential? – Y / N</p>
<p>Question 21: How do you mitigate any risks posed by the design of algorithms that support the function of your service (e.g. search engines, or social and content recommender systems), with reference to illegal content specifically?</p>	<p>Confidential? – Y / N</p>
<p>Question 22: What age assurance and age verification technologies are available to platforms, and what is the impact and cost of using them?</p>	<p>Confidential? – Y / N</p> <p>N/a</p>
<p>Question 23: Can you identify factors which might indicate that a service is likely to attract child users?</p>	<p>Confidential? – Y / N</p> <p>N/a</p>
<p>Question 24: Does your service use any age assurance or age verification tools or related technologies to verify or</p>	<p>Confidential? – Y / N</p> <p>N/a</p>

<p>estimate the age of users?</p>	
<p>Question 25: If it is not possible for children to access your service, or a part of it, how do you ensure this?</p>	<p>Confidential? – Y / N</p> <p>N/a</p>
<p>Question 26: What information do you have about the age of your users?</p>	<p>Confidential? – Y / N</p> <p>N/a</p>
<p>Question 27: For purposes of transparency, what type of information is useful/not useful? Why?</p>	<p>Confidential? N</p> <p>Transparency is important for making platforms accountable to internet users, regulators and the public. We believe that the following metrics would be helpful:</p> <ul style="list-style-type: none"> • Numbers of complaints • Broad reasons for complaint/type of complaint • Action the platform has taken e.g. removing content, closing accounts etc and the nature of the content that was removed or otherwise acted on. • How long they have taken to remove fraud related content, close account etc. • How the illegal content was found e.g. from own proactive monitoring, user reports, regulator reports, other platforms etc. • The platform’s own assessment of the scale of illegal content on their site and the proportion which they have removed. <p>We know that fraudsters can easily and quickly move from one platform to the next and so as well as helping consumers know which services are safest, this data would also help the platforms monitor the extent to which their service is being exploited by criminals and act as a warning flag that further action was needed. It would also help other stakeholders, such as regulators, identify where best to deploy their resources.</p> <p>It would be helpful if the measures were consistent across service providers otherwise it may be difficult to compare and could prevent people from making an informed choice about which services they use.</p> <p>Published transparency measures could also help journalists and other commentators make consumers aware of platforms’ relative safety.</p>

Question 28:
Other than those
in this document,
are you aware of
other measures
available for
mitigating risk
and harm from
illegal content?

Confidential? N

We would like to reiterate that effective mitigation requires platforms to implement controls to prevent illegal content “going live” as well as proactive monitoring of their platforms to pick up content that slips through.

We are making greater use of technology in this area to prevent online fraud and so platforms themselves could also do so. For example, we are scanning approximately 100,000 websites every day to identify newly registered domains that show characteristics of a scam and we are also working with a third party that specialises in identifying and removing illegal content from the web.

Please complete this form in full and return to OS-CFE@ofcom.org.uk