Money and Mental Health submission to Ofcom's call for evidence on the first phase of online safety regulation

Introduction

The Money and Mental Health Policy Institute is a research and policy charity, established in 2016 by Martin Lewis to break the link between financial difficulty and mental health problems. The Institute's research and policy work is informed by our Research Community, a group of over 4,500 people with lived experience of mental health problems or of caring for someone who does.

This written submission has been informed by research we conducted on people with mental health problems' experiences of online scams. This included powerful lived experience testimony and nationally representative polling. Unless otherwise specified, all quotes in this response are drawn directly from our Research Community.

In this response we answer questions 2, 5, 7, 11, 14, 18 and 27.

Q2. Can you provide any evidence relating to the presence or quantity of illegal content on user-to-user and search services?

We are interested in briefings, investigations, transparency reports, media investigations and research papers that provide more evidence about how such content might vary across different services or types of service, or across services with particular groups of users, features or functionalities.

As part of our research, we looked at the prevalence of online scams. In nationally-representative online polling, half of adults (50%) reported they had seen a scam advert and four in ten (43%) had seen a user-generated scam on social media at least once a month.[1] When we asked our Research Community, a group of 4,500 people with lived experience of a mental health problem, six in ten (59%) had seen something that they thought was a scam on a social media site, three in ten (28%) on a search engine, 17% on a dating site and one in ten (9%) on an online forum.[2]

Q5. What can providers of online services do to enhance the clarity and accessibility of terms of service and public policy statements?

Please submit evidence about what features make terms or policies clear and accessible.

Common symptoms of mental health problems can affect how someone processes, understands and acts on information. This can be exacerbated by badly designed

[1] Lees C and D'Arcy C. Safety first: Why the Online Safety Bill should tackle scam adverts. Money and Mental Health Policy Institute. 2021.
[2] Holkar M and Lees C. Caught in the web. Money and Mental Health Policy Institute. 2020.

communication which uses legalese and buries key pieces of information within large bodies of text. Through speaking to people with lived experience of mental health problems we have created a set of principles for making information easy to understand which would apply to terms of service and public policy statements:

- Remove technical language, or explain it in nontechnical terms
- Minimise the quantity of content as much as possible and leave plenty of space between content
- Highlight key messages or action points
- Use bullet points to break down complex tasks or processes

Providers of online services should also make sure that the customer journeys for reading and accepting terms of services and public policy statements optimise someone's ability to process the information and not use design features to push someone to rush through. For example, the option to accept the conditions should not be more prominent than the option to decline.

Q7. What can providers of online services do to enhance the transparency, accessibility, ease of use and users' awareness of their reporting and complaints mechanisms?

Please submit evidence about what features make user reporting and complaints systems effective, considering:

- ***reporting or complaints routes for registered users;***
- ***reporting or complaints routes for non-registered users; and***
- ***reporting routes for children and adults.***

In our research we found that people can often face difficulty when trying to report a scam on an online platform. For example, the button to report content can be small and the wording used unclear, making it harder to determine whether it would be classed by the platform as scam content.

From speaking with our Research Community, we came up with a set of principles online services should use when designing reporting tools:

- Involve people with mental health problems in the design and testing of reporting tools.
- Make the reporting tool prominent and easy to find.
- Clearly signpost users to support services, including Victim Support and other reporting services that may be able to help.
- Provide information at the start of reporting processes to manage users' expectations.
- Use simple language throughout and explain any technical terms that are required.
- Recognise that reliving being scammed, in order to report it, can be a traumatic experience.
- Offer a variety of ways for users to report.
- Adopt a 'safety first' approach to content flagged as a scam, for instance instantly freezing or removing flagged content, until it is reviewed.

Q11. Could improvements be made to content moderation to deliver greater protection for users, without unduly restricting user activity? If so, what?
Please provide relevant evidence explaining your response to this question. Please consider improvements in terms of user safety and user rights, as well as any relevant considerations around potential costs or cost drivers.

We think platforms should ensure they have reliable and robust systems to prevent scams appearing on their platform. This could include vetting for adverts and promoted posts, and systems for identifying and blocking suspicious content. Increased vetting of adverts and content could lead to false negatives where an advert or post is taken down but it isn't a scam or increased time to have an advert placed. However, the current prevalence of scams and the impact they can have outweighs the inconvenience greater content moderation would have.

"Social media should definitely be more proactive in stopping scams at all, and removing them quickly so they don't spread."
Expert by experience

Q14. How are sanctions or restrictions around access (including to both the service and to particular content) applied by providers of online services?
Please provide evidence around the application and accuracy of sanctions/restrictions, and safeguards you consider should be in place to protect users' privacy and prevent unwarranted sanction.

When we and other organisations have raised concerns about the level of scams on online platforms, providers have said that they have systems in place to stop such content from appearing. This includes tools that allow users to report content which is then taken down. However, in our research we found that scams were quite common on social media sites and a frustration we found among people who had managed to report a scam on an online platform was that they continued to see the same scam after reporting. The perception that reporting tools are ineffective is a key driver of under-reporting, so providers should create tools that encourage greater user policing of online spaces.

"[Social media companies'] reporting schemes are not remotely fit for purpose – I don't think anything I've reported has ever been removed, and when others have got scams removed, it's taken ages to do so."
Expert by experience

Q18. Are there any functionalities or design features which evidence suggests can effectively prevent harm, and could or should be deployed more widely by industry? Please provide relevant evidence explaining your response to this question

One feature that online platforms should introduce is displaying warnings when searching for certain terms such as debt advice or investments, to make sure users know the content they see isn't a scam. Twitter introduced something similar in conjunction with Citizens Advice, which offers a pop-up of support if someone searches for the term 'online scams'. Similarly, Google has a feature which brings up information about Samaritans if someone searches for something related to suicide. These examples highlight that the functionality exists. This feature could help educate and prepare users for online scams alongside preventative and reactive work by the platforms.

"More information on Facebook... Facebook sponsored ads telling people what to look out for. Google could also put something at the top of their search page telling you how to avoid scams."
Expert by experience

It would also be beneficial for providers to proactively warn users who may have been exposed to scams – for example users who have engaged with scam content on social media or bought from a seller who was later identified as a scammer.

Most platforms have the ability to restrict or limit the amount of adverts that a user sees, but this functionality is often not known about or hidden away. Given the prevalence of scam adverts, it would be useful if this functionality was better advertised and easier to find.

Q27. For purposes of transparency, what type of information is useful/not useful? Why?

In particular, please consider:

- ***Any evidence of public information positively or negatively affecting online user safety or behaviours, how this information is used, and by whom;***
- ***What information platforms should make available, considering frequency, format and intended audiences;***
- ***What information Ofcom should make available through its transparency report, considering frequency, format, intended audiences and potential use cases by external stakeholders;***
- ***The benefits and/or drawbacks of standardised information and metrics; and***
- ***Any negative impacts or potential unintended consequences of publishing certain types of information, and how these may be mitigated.***

We believe it is important that information related to how service providers approach online safety is made public to allow Ofcom and others to hold them to account. It would be useful to be able to see information on the number of scams detected and taken down, as well as the number of scams reported and taken down. This, in tandem with independent research and monitoring, would allow for an assessment of how well providers are tackling scams on their sites both proactively and reactively when they are alerted to it. It would also give an indication of how effective the reporting system is. This reporting of information would have to take the different sizes of providers into account. There could be potential unintended consequences with scammers being able to use this information to know which platforms are the worst performers and should therefore be targeted. Ofcom should think carefully about how to best present this information to make sure platforms are accountable but there is limited risk of unintended consequences.