Money and Mental Health's response to the DCMS sub-committee inquiry on online safety and online harms

The Money and Mental Health Policy Institute is a research charity established by Martin Lewis to break the vicious cycle of money and mental health problems. We aim to be a world-class centre of expertise developing practical policy solutions, working in partnership with those providing services, those who shape them, and those using them, to find out what really works. Everything we do is rooted in the lived experience of our Research Community, a group of thousands of people with personal experience of mental health problems.

This written submission has been informed by this powerful, lived experience testimony, as well as our wider body of research. Unless otherwise specified, all quotes in this response are drawn directly from our Research Community. In particular, it makes reference to a number of recent publications we have published on the issue of online harms, including:

- Safety first: Why the Online Safety Bill should tackle scam adverts - July 2021
- Safety net: Breaking the link between online financial harms and mental health problems - March 2021
- Caught in the web: Online scams and mental health - December 2020

Background

- In any given year, one in four people will experience a mental health problem,[1] and over a lifetime this rises to nearly half the population[2]. However, we do not always know when we are unwell, or receive treatment. Over a third (36%) of people with a common mental disorder have never received a diagnosis, and 62% are not currently receiving treatment.
- Online services can be a lifeline for people with mental health problems, offering them easier access to services and shopping at a time when it may be difficult to leave the house or carry out basic tasks.
- But common symptoms of mental health problems, like low motivation and limited concentration, can make people more vulnerable to online harms.[3] For instance, people with mental health problems are at particularly high risk of losing money or personal information to a scam. Nationally representative polling found that people with mental health problems were three times more likely to have been scammed online than people without such conditions.[4]

How has the shifting focus between 'online harms' and 'online safety' influenced the development of the new regime and draft Bill?

[1] McManus S et al. Adult psychiatric morbidity in England, 2007. Results of a household survey. NHS Information Centre for Health and Social Care. 2009.
[2] Mental Health Foundation. Fundamental facts about mental health. 2016.
[3] Holkar M. Seeing through the fog. Money and Mental Health Policy Institute. 2017.
[4] Holkar M and Lees C. Caught in the web. Money and Mental Health Policy Institute. December 2020

Contact: conor.darcy@moneyandmentalhealth.org

The terms ‘online harms’ and ‘online safety’ may be interpreted differently by the various actors involved in this space. However, our perspective is that the effectiveness of efforts to tackle the dangers present in some online spaces will primarily be determined by the requirements placed on firms and the powers and resources given to the regulator and Secretary of State. The change of focus to ‘safety’ from ‘harms’ therefore does not strike us as a cause for concern in itself or necessarily leading to different responses.

Is it necessary to have an explicit definition and process for determining harm to children and adults in the Online Safety Bill, and what should it be?

While we do not have a preferred approach, a shared understanding of how harm is defined and assessed would be valuable. We believe that as part of such an exercise, specific consideration should be given to people with mental health problems, in light of their higher risk of experiencing some online harms as well as the more damaging impact that such experiences can have.

This points towards an approach which takes into account factors that may make some people more likely to be harmed by a specific event or interaction, recognising that a single ‘harm threshold’ for everyone would not represent reality. In nationally representative polling, we found that four in ten (40%) online scam victims have felt stressed and three in ten (28%) have felt depressed as a result of being scammed.[5] But the mental health impacts of falling victim to a scam online can be particularly severe for those already experiencing a mental health problem.

“Very stressful and made me feel stupid for falling for the scam as I think I’m stupid anyway this made me have terrible negative thoughts about myself and so annoyed”
Expert by experience

Harm can also go beyond the immediate impact, restricting people’s ability to make the most of the opportunities that the internet can offer.

“Very shaken and felt as if I had been personally attacked, for a long time I was unable to use the internet and to this day I do not have internet banking”
Expert by experience

“I become scared of clicking on certain links. Rationally I am sure they are OK, but I still dare not go there. This limits my access to sites I may need to use.”
Expert by experience

The extent to which financial harm is considered in the Bill has been blurred somewhat. Some forms of financial scams included, with the government drawing attention to romance and investment scams, but with the financial impact of the harm being explicitly out of scope. The financial damage that can be done, either directly or indirectly, through missing out on services and opportunities as in the quotes above, can be huge. This clearly applies when the amount of money lost is large. But for people with mental health problems who on average have lower

[5] Ibid.

incomes and are more at risk of being in problem debt, losing even relatively small sums to a scam can have major consequences. In nationally representative polling, we found that 13% of online scam victims cut back on essential spending such as groceries as a result of being scammed.[6]

"Financially I really struggled for a few months, had to borrow money and use food banks, ultimately had to sell my car to pay it off."
Expert by experience

Does the draft Bill focus enough on the ways tech companies could be encouraged to consider safety and/or the risk of harm in platform design and the systems and processes that they put in place?

Platform design, systems and processes are vital considerations for efforts to reduce harms online. While the Bill should avoid going into too much detail on design considerations, expectations and the outcomes that are desired would be helpful. For instance, friction in online journeys which slows a user's journey, and potentially gives them more time to consider whether this is trustworthy information would be helpful. Similarly, as explored further in our response to the next question, reporting suspicious or harmful content can be a difficult task, with it being unclear where to do so and what action was taken in response. This poor design disincentivises users from raising such content with websites and means potentially harmful content remains accessible for longer.

What are the key omissions to the draft Bill, such as a general safety duty or powers to deal with urgent security threats, and (how) could they be practically included without compromising rights such as freedom of expression?

As noted above, a wider definition of harms which recognises financial impacts would be welcome. However, the major notable omission in the Bill is paid-for scams. While the government has included user-generated scams in the scope of the Bill, scams carried out through adverts or other promoted content are not covered.

Whichever form they come in, scams are all too common online. Half of adults reported they had seen a scam advert on social media at least once a month (50%) and four in ten (43%) had seen a user-generated scam in the same period.[7] But with only user-generated scams being targeted by the Online Safety Bill, the prevalence of scam adverts presents a huge barrier to the government's aim of making the UK the safest place to be online.

Scam adverts come in a variety of guises. Links leading to websites that replicate the design of well-known companies or that claim to have celebrity endorsements - with Martin Lewis among the most-used high-profile names[8] - seek to reassure users that it is safe to provide financial or personal information.

---

[6] Holkar M and Lees C. Caught in the web. Money and Mental Health Policy Institute. 2020.
[7] Holkar M, Lees C and D'Arcy C. Safety Net. Money and Mental Health Policy Institute. 2021.
[8] See for instance https://www.bbc.co.uk/news/technology-57051546

In a survey of our Research Community, we found that many have been the victim of a scam that is currently not included in the draft Bill. For example, 15% said they had lost money or personal information to a scam advert on social media, 11% were scammed by a promoted or sponsored item on a marketplace and 11% were the victim of a scam advert which appeared at the top of search engine results.[9]

"The advert was on Facebook. It was to enter a competition which I now know they use to get your email details and social media information."
Expert by experience

"I purchased a paper to enter into Canada which should have been £5 but the search engine took me to another address. I ended up paying £184 each for me and my husband and I could not do a thing about it"
Expert by experience

While leading online platforms and websites report that they do analyse the adverts they carry before publication and stop much fraudulent content from appearing, it is clear that their current efforts are ineffective. With patchy prevention, the onus is placed on users to spot scam adverts. But recent research by Which? discovered that many people, including those who believed they could spot a scam online, were unable to identify a scam advert on a social media feed.[10] Our Research Community survey found similar issues, with many people saying they were wary of adverts on social media sites but had still fallen victim to scam adverts, and that being unwell at the time can increase this risk.

"I am often a bit sceptical of these adverts. I tend to ignore them. [But] if they catch my attention, I sometimes don't remember to check if they're legitimate."
Expert by experience

An added contributor to this harm could be the trust that many people place in social media platforms to protect their users.[11] One of our Research Community respondents explained that they had fallen victim to an online scam advert, believing that the platform would have prevented such content from appearing.

"*I did trust adverts on social media, but no longer. I believed that the companies (Facebook/Instagram) would protect their users."*
Expert by experience

It is possible for internet users to report scams they see online, though our previous research has found this can be an arduous and unclear task, particularly for those experiencing a mental

[9] Money and Mental Health Survey of 175 members of our Research Community, carried out between 4th and 14th June 2021. Base for this question: 149 people with lived experience of mental health problems.
[10] Which? Connecting the world to fraudsters? 2020.
[11] Ibid.

health problem.[12] With different organisations involved in policing scams, knowing which bodies to alert presents an initial challenge. Research Community members told us how the process itself can be a struggle, with a lack of clarity over how exactly concerns should be flagged, locating the reporting tool and what category they fall into in pre-populated lists of potentially harmful content.

Even if users do manage to report a scam advert, the follow-up action taken by online services can often appear minimal or non-existent.

"You can report scam adverts but even though you ask not to see them again they come up time and time again. These companies don't seem to care or take notice. I have never been contacted after reporting a scam."
Expert by experience

With scams widespread, an approach which fails to prevent so many fraudulent adverts from appearing, and relies on individuals to avoid often sophisticated scams - and report them when they see them - places too much responsibility on users and not enough on online firms.

Against this backdrop of prevalent and serious harm, the government's commitment to tackle user-generated scams online is a welcome start. But the distinction drawn in the draft Bill between user-generated scams and scam adverts is unclear, unhelpful and could incentivise online platforms and services to focus on some kinds of fraudulent content but not others.

While in other media, there is a clearer dividing line between what is an advert and what isn't, that difference is much blurrier online. Adverts and sponsored content are frequently built into the user experience of many websites and are often only identifiable by a small tag saying 'Ad' or 'Promoted'. Research for the Advertising Standards Authority (ASA) found that two-thirds of people (66%) were able to identify that a post on social media was definitely an advert but this still leaves many who were uncertain.[13] Differentiating between adverts and other content can be even more difficult when someone is unwell; eight in ten (82%) Research Community respondents agreed that it can be difficult to tell the difference between the two types of content when experiencing a mental health problem.[14]

The government itself recognised this unclear boundary when it explained that promotional posts by 'influencers' would be covered by the Online Safety Bill as "these are often indistinguishable from other forms of user-generated content".[15] Despite this, other promotional content - where the online *platform,* rather than an individual influencer, is paid to host and promote the content - will be excluded under current plans.

---

[12] Holkar M and Lees C. Caught in the web. Money and Mental Health Policy Institute. 2020.
[13] Ipsos Mori. Research on the Labelling of Influencer Advertising. On behalf of the Advertising Standards Authority. 2019.
[14] Money and Mental Health Survey of 175 members of our Research Community, carried out between 4th and 14th June 2021. Base for this question: 146 people with lived experience of mental health problems.
[15] Department for Digital, Culture, Media and Sport. The Online Safety Bill - Impact Assessment. 2021.

Contact: conor.darcy@moneyandmentalhealth.org

Beyond the inconsistency and confusion this is likely to cause, the different treatment of content could create a perverse situation in which a scammer could evade scrutiny by paying to promote a user-generated post, moving it out of scope of regulation. Romance scams - which the government has specifically signalled will be in scope - are often carried out through dating websites and apps. Some of those services, however, allow users to pay to promote their profile so it features more prominently, leading more people to see it. Following the logic of the government's outlined approach, scams initiated through such paid-for promotion would be out of scope. This means that if a romance scammer is able to pay to reach even more potential victims, they could avoid the new user-generated checks that online services will have to adopt.

Rather than use the Online Safety Bill to address the harm caused by scam adverts, the government plans to pursue other avenues. This includes a Home Office fraud action plan and a Department for Digital, Media, Culture and Sport (DCMS) consultation on advertising regulation.[16] To date, regulation of advertising has focused on the advertiser and the content of the advert, such as what can be included in a gambling advert. Less has been asked of the publisher of the advert. It is clear that this approach has failed to prevent the epidemic of online scam adverts.

While the content of the DCMS consultation is unknown, meaningful change to advertising regulation - for instance, placing much greater responsibility on online platforms for the content of the adverts - would mark a major shift in the UK's approach to advertising regulation, moving further away from the current model of self-regulation. Such a change would naturally involve an extended period of consultation, responses and drafting of legislation, as well as potentially a new regulatory body or changes to the ASA's remit, structure and funding. Through this approach, even *if* the changes proposed are sufficient - which remains to be seen - we would expect significant action on scam adverts to take several years, leaving vulnerable people at risk. In contrast to the uncertainty and long lead-in time required to redesign advertising regulation, the Online Safety Bill offers the government an ideal opportunity to take concrete action much sooner.

Under the government's current plans, online services will be required to have systems and processes to minimise the presence of illegal user-generated content. For harms deemed a priority - these will be set out in secondary legislation outside of the Online Safety Bill - there will be a duty placed on online services to prevent such content from appearing publicly in the first place. For both these harms and others classed as non-priority, online firms will need to have effective reporting channels, allowing users who spot such content to alert the service and remove it swiftly.[17] Given their prevalence and the wide-ranging and severe impact they can have on those affected, all online scams should be treated as a priority area for action. Ensuring the Online Safety Bill duties covers scam adverts as well as user-generated fraud would

[16] The Financial Conduct Authority has also indicated its intention to take greater action on online services who allow fraudulent financial promotions to appear. While welcome, this would only affect a subset of scam adverts.
[17] DCMS. Draft Online Safety Bill. 2021.

introduce a legal backstop to enable companies to be heavily penalised if they fail to more effectively protect their users.

This will lead to increased costs for online platforms and services. But as the government recognised when it committed to tackling user-generated scams through the Bill, the costs to such businesses will be insignificant compared to the current cost of online scams.[18] In particular, this cost falls most sharply on vulnerable people, including those of us with mental health problems who are more likely to be scammed. The systems and processes online firms will have to implement are also unlikely to be dramatically different from those for user-generated content, potentially reducing the time and cost of doing so compared to building a different approach for the two types of scams.

The cost of increased scrutiny of adverts may be passed by online services onto businesses wanting to advertise. These could include false negatives where an advert is taken down but it isn't a scam or increased time to have an advert placed. However, the lack of action on scam adverts is leading some people to not trust adverts at all. For example, four in ten (43%) Research Community respondents said they would be unlikely to trust an advert on social media by a well-known company that they don't currently 'follow' or 'like'.[19]

"Companies lose out as well when scam adverts are being used and it makes people less trustful of legitimate adverts from honest companies"
Expert by experience

There is strong public support for more action to be taken by online services to prevent harm from scam adverts. Nationally, eight out of ten (81%) people think that online services should be required to prevent scams from appearing on their sites, with backing from our Research Community too.

"I would like to see more accountability from the big companies as they have the money and resources to stop these adverts being posted. Also the government should implement more laws to force these companies to take down these adverts and penalise them for not doing enough."
Expert by experience

[18] DCMS. The Online Safety Bill - Impact Assessment. 2021.
[19] Money and Mental Health Survey of 175 members of our Research Community, carried out between 4th and 14th June 2021. Base for this question:154 people with lived experience of mental health problems.