Money and Mental Health Policy Institute — submission to the Joint pre-legislative scrutiny Committee on the Draft Online Safety Bill

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, our response 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

Summary

Money and Mental Health is part of a coalition of consumer groups, charities and industry bodies, including:

- Age UK
- The Association of British Insurers
- Carnegie UK Trust
- Innovate Finance
- The Investment Association
- MoneySavingExpert
- Personal Investment Management & Financial Advice Association (PIMFA)
- B&CE Ltd, provider of the People's Pension
- TheCityUK
- UK Finance
- Victim Support
- Which?

Our united view is that the government's current approach to tackling online fraud is flawed. It will likely lead to complex and muddled regulations and far worse consumer outcomes than an Online Safety Bill with a comprehensive approach to online fraud.

While we welcome the recent inclusion in the draft Bill of fraud carried out through user generated content and fake profiles on social media websites, there is a long way to go. Failing to include online advertising in the Bill leaves too much room for criminals to exploit online systems.

Contact: conor.darcy@moneyandmentalhealth.org

This view is backed by the FCA, Bank of England, City of London Police, Work and Pensions Committee and Treasury Committee, who have all commented that the scope of the Online Safety Bill should be expanded to include fraud carried out via online advertising.

We do agree with the government that the impact of these frauds is often devastating, not just financially but also emotionally. That's why we urge ministers to reconsider their current plan, and make sure the Bill protects as many consumers as possible from the full extent of the devastation caused by scams.

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.[3]
- The internet can be a lifeline for people experiencing 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.[4] 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.[5]
- The draft Bill's omission of scams carried out through paid-for advertising is a major obstacle to the government's goal of making the UK the safest place to be online. Scam ads are both extremely common - half of adults report having seen a scam advert on social media at least once a month (50%).[6] They are also damaging, with four in ten (40%) online scam victims reporting having felt stressed and three in ten (28%) having felt depressed as a result of being scammed.[7]
- To ensure that the UK's internet users, including those with mental health problems, are not left exposed to professional scammers, scam adverts should be included within the scope of the Bill and considered as a priority harm, requiring social media companies and search engines to reduce the number of scams appearing on their services in the first place.

Objectives

[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] McManus S et al. Mental health and wellbeing in England: Adult Psychiatric Morbidity Survey 2014. NHS Digital. 2016.
[4] Holkar M. Seeing through the fog. Money and Mental Health Policy Institute. 2017.
[5] Holkar M and Lees C. Caught in the web. Money and Mental Health Policy Institute. December 2020
[6] D'Arcy C, Holkar M and Lees C. Safety Net. Money and Mental Health Policy Institute. March 2021
[7] Holkar M and Lees C. Caught in the web. Money and Mental Health Policy Institute. December 2020

Contact: conor.darcy@moneyandmentalhealth.org

Will the proposed legislation effectively deliver the policy aim of making the UK the safest place to be online?

The decision to exclude scams carried out through paid-for advertising undermines the aim of making the UK the safest place to be online. The Bill cannot cover each and every harm that internet users face. But the scale of scam adverts and the severity of the harm they can cause - as explored in more depth in our responses to later questions - means their omission is a missed opportunity to tackle a major threat to safety online and will leave millions of internet users at risk of being scammed.

Does the draft Bill make adequate provisions for people who are more likely to experience harm online or who may be more vulnerable to exploitation?

People with mental health problems are significantly more likely to experience harm online. For instance, nationally representative polling found that people who have experienced mental health problems are three times more likely than the rest of the population (23% versus 8%) to have been the victim of an online scam.[8] This suggests that despite comprising a minority of the total population, people with mental health problems make up the majority of those who have been scammed online.

Our research indicates that a number of factors contribute to this, including common symptoms of many health problems, such as difficulties concentrating and low motivation. This means that while efforts to educate people on how to protect themselves are welcome, a period of poor mental health can greatly increase our risk of harm, even to dangers which we may be aware of and able to avoid when healthy. Greater preventative action from online services - including stopping scams from appearing on their platforms in the first place - is therefore crucial to protect the one in four of us who experience a mental health problem in any given year.

We do not believe that people with mental health problems or other adults who are at greater risk of harm online should be treated differently by online services. But where people with protected characteristics are disadvantaged in their use of a service, this is likely to mean the provider of that service - in this case online firms - are at risk of breaching the Equality Act 2010. Whether in the Bill or through subsequent regulatory activity by Ofcom, reminding firms of their duties under the Equality Act should - in tandem with effective enforcement and penalties - lead to firms taking action to ensure that people do not suffer a disadvantage online due to a disability or other protected characteristic.

Is the "duty of care" approach in the draft Bill effective?

Placing a duty of care on online services and platforms communicates the responsibilities that such firms have to protect their users. That said, ultimately the impact on users will be determined by what companies are and are not required to do and how that is enforced. Ensuring that legislation is clear on what firms must do - and the penalties they will face if they

[8] Holkar M and Lees C. Caught in the web. Money and Mental Health Policy Institute. 2020.

fail to comply - are, along with effective monitoring and enforcement, the most important considerations.

Does the Bill deliver the intention to focus on systems and processes rather than content, and is this an effective approach for moderating content? What role do you see for e.g. safety by design, algorithmic recommendations, minimum standards, default settings?

Safety by design, algorithmic recommendations, minimum standards and default settings all offer routes through which online services and platforms can help keep their users safe. Importantly, they place the emphasis on steps that firms can take to reduce the odds of users being harmed in the first place, rather than relying primarily on users reporting concerning content.

The Bill itself should avoid going into too much detail on these design considerations, in order to avoid being overtaken by changes in the online experience which then require updates to legislation in order to tackle emerging harms. But Ofcom's regulation of services covered by the Bill could be informed by such principles, as well as the outcomes that are desired. For instance, appropriate friction in online journeys allows users more time to consider whether information or an offer is trustworthy. Expectations around this could be introduced without being overly prescriptive. Similarly, reporting suspicious or harmful content can be a difficult task, with it being unclear where to do so. This poor design disincentivises users from flagging such content and means potentially harmful content remains accessible for longer. On such issues, minimum standards or expectations, as the Financial Conduct Authority (FCA) has recently put forward in relation to it being as easy to sign up to a service as it is to leave it, could also be considered by Ofcom, requiring it to be as easy to report content as it is to post it.

Content in Scope

The draft Bill specifically includes CSEA and terrorism content and activity as priority illegal content. Are there other types of illegal content that could or should be prioritised in the Bill?

Scams - both user-generated or paid-for adverts - must be considered as priority illegal content. The prevalence, severity and variety of harm caused by scams mean that, without giving them priority treatment, internet users will continue to be at much higher risk.

Whichever form they come in, scams are all too common online. In nationally representative polling conducted in February 2021, half of adults (50%) reported they had seen a scam advert on social media at least once a month and four in ten (43%) had seen a user-generated scam in the same period.[9]

[9] Holkar M, Lees C and D'Arcy C. Safety Net. Money and Mental Health Policy Institute. 2021.

Polling also 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.[10] But the mental health impacts of falling victim to a scam online can be particularly severe for those already experiencing a mental health problem.

"[It was] 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

As well as the scale and seriousness of the harm caused by scams, another reason to designate them as priority illegal content - therefore requiring much more proactive efforts from online firms - is the difficulty involved in reporting scams. 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 health problem.[11] 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 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. As such, requiring more proactive steps from firms, through better identification of fraudulent posts and adverts before they appear on their platforms, is needed to genuinely tackle the threat posed by scammers online.

---

[10] Ibid.
[11] Holkar M and Lees C. Caught in the web. Money and Mental Health Policy Institute. 2020.

Are there any types of content omitted from the scope of the Bill that you consider significant e.g. commercial pornography or the promotion of financial scams? How should they be covered if so?

The major notable omission in the draft Bill is scams that are carried out through paid-for advertising. While the government has included user-generated scams in the scope of the draft Bill, scams carried out through adverts or other promoted content are not covered.

As noted in response to the previous question, half of adults reported they had seen a scam advert on social media at least once a month (50%), even more than the four in ten (43%) who had seen a user-generated scam in the same period.[12] But with only user-generated scams being targeted by the draft 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[13] - seek to reassure users that it is safe to provide financial or personal information. 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.[14]

"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 0took 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.[15] 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.

---

[12] Holkar M, Lees C and D'Arcy C. Safety Net. Money and Mental Health Policy Institute. 2021.
[13] See for instance https://www.bbc.co.uk/news/technology-57051546
[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: 149 people with lived experience of mental health problems.
[15] Which? Connecting the world to fraudsters? 2020.

"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.[16] 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

As discussed in response to the previous question, relying primarily on users to report scams is ineffective. With scams widespread, an approach which fails to prevent so many fraudulent adverts from appearing, and relies on individuals to avoid 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.[17] 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.[18]

The government itself recognised this unclear boundary when it explained that promotional posts by 'influencers' would be covered by the Bill as "these are often indistinguishable from other forms of user-generated content".[19] 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.

---

[16] Ibid.
[17] Ipsos Mori. Research on the Labelling of Influencer Advertising. On behalf of the Advertising Standards Authority. 2019.
[18] 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.
[19] Department for Digital, Culture, Media and Sport. The Online Safety Bill - Impact Assessment. 2021.

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 checks that online services will have to adopt for user-generated content.

Rather than use the 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 DCMS consultation on advertising regulation.[20] 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 the meantime. 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 harmful user-generated content. 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.[21] 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, 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

[20] The FCA 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.
[21] DCMS. The Online Safety Bill - Impact Assessment. 2021.

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'.[22]

"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

What would be a suitable threshold for significant physical or psychological harm, and what would be a suitable way for service providers to determine whether this threshold had been met?

We believe that in setting a threshold, an approach which takes into account factors that may make some people more likely to be harmed by a specific event or interaction would be helpful. This would allow for a recognition that a single 'harm threshold' for everyone would not represent reality. As noted in response to previous questions, for people with mental health problems being scammed online can have devastating psychological consequences. In setting out a threshold, any legislation should take account of groups with protected characteristics, and the ways in which firms are required under the Equality Act to ensure that customers are not disadvantaged because of their characteristics.

More broadly on harm, we believe that explicitly stating content is not in scope if the harm arises from the "potential financial impact" is unhelpful and in conflict with the government's decision to include user-generated scams in the draft Bill. A strict reading of this would suggest that someone who falls victim to an investment scam is only covered by the Bill with respect to the physical or psychological harm this has caused them. In the case of scams, while the shame and embarrassment that can be caused by a scam is often serious, trying to separate this out from the financial impact is not possible.

The financial damage that can be done, either directly or indirectly, through missing out on services and opportunities, can be huge. This clearly applies when the amount of money lost is

[22] 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.

large. But for people with mental health problems who on average have lower 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.[23]

"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

The draft Bill could be changed in a number of ways to address this inconsistency. For instance, "financial" harms could be specifically added alongside "physical" and "psychological", or "physical" and "psychological" could be removed, reflecting that any significant harm is in scope. Alternatively, if the intention is to avoid overlaps between the scope of this Bill and existing duties which sit with the FCA or other regulators of financial products, an exclusion could be added to place "regulated financial products" outside the scope of the Bill.

Algorithms and user agency

What role do algorithms currently play in influencing the presence of certain types of content online and how it is disseminated? What role might they play in reducing the presence of illegal and/or harmful content?

Algorithms could play a major role in reducing the appearance of scams - and particularly scam adverts - online. Work by the Advertising Standards Authority (ASA) has employed algorithms to identify fraudulent adverts and report them to the websites that host them.[24] While this is welcome action, services hosting ads are much better placed to use such technology to prevent ads. And while firms are likely to already have some mechanisms in place, the prevalence of scam ads online suggests algorithms need to become much more effective. If online services - often very large and well-resourced companies - had a sufficient impetus to improve the accuracy of these algorithms through regulation, this could lead to more effective controls on scams.

The role of Ofcom

Is Ofcom suitable for and capable of undertaking the role proposed for it in the draft Bill?
Are Ofcom's powers under the Bill proportionate, whilst remaining sufficient to allow it to carry out its regulatory role? Does Ofcom have sufficient resources to support these powers?

[23] Holkar M and Lees C. Caught in the web. Money and Mental Health Policy Institute. 2020.
[24] https://www.politicshome.com/news/article/online-platforms-are-in-an-arms-race-with-scammers-asa-lord-currie

Contact: conor.darcy@moneyandmentalhealth.org

Overall, we support the decision to make Ofcom the online safety regulator. Creating a new regulator from scratch would be a lengthy and expensive process. That said, equipping Ofcom to take on the proposed new powers presents significant challenges. This is particularly true with regard to priority harms, for which online services in scope will be required to take more preventative action to put in place effective systems and processes. This presents a number of challenges for Ofcom.

Firstly, in recognition of the significance of the changes and the importance of balancing competing concerns like freedom of speech and protecting internet users, Ofcom will need to shift towards more active monitoring and compliance. Ofcom currently does relatively little of this, particularly in comparison to other regulators like the FCA. This is likely to require practical changes, including increased staffing budgets and the recruitment of employees with more monitoring and compliance experience. But to be successful, a cultural shift may also be needed, to reflect the different nature of the relationship between the online safety regulator and services in scope. Parliament and others like the NAO should review how Ofcom is adjusting to its new role and make recommendations as needed.

Secondly, the shift to online services presents similar challenges for regulators across diverse sectors. As regulators navigate this change and adapt their ways of working, there is huge potential for collaboration and sharing of best practice. The CMA, ICO and Ofcom have led the way, establishing the Digital Regulation Cooperation Forum (DRCF) to enhance cooperation on online regulation.[25] The DRCF could play an important role in facilitating collaboration as Ofcom takes on this new role, providing a space for regulators to reflect on common challenges and work together to address them.

Joint investigations between regulators with concerns about online spaces may be one route through which this could be achieved. While one of the government's arguments against including scam adverts in the Bill is that both the ASA and the FCA have some responsibilities in this area already. But rather than simply giving Ofcom new powers in these areas, a more concerted collaborative approach to such shared issues should be taken. This could mean that whichever body encounters an issue, it can raise it with the other regulators in this space, allowing for a more rounded, joined-up response, rather than trying to solve what are often large and complex problems alone.

Technical expertise is another key challenge for many regulators that could also be addressed through greater collaboration. Data scientists and artificial intelligence experts are increasingly sought after, and regulators compete for this talent, both with each other and the private sector. All regulators face financial constraints and competing priorities, and smaller regulators may particularly struggle to develop the technical expertise they need in this context. Some regulators already struggle to attract and retain technical staff, and this problem is likely to grow as demand for these skills grows.[26]

To address this, regulators should pool their expertise in the DRCF and use this as a specialist body to support them with digital transformation. This approach could help regulators to more

[25] CMA, ICO and Ofcom. Digital Regulation Cooperation Forum. 2020.
[26] NAO. A short guide to regulation. 2017.

efficiently fill skills gaps and would ensure that lessons from one sector are learnt by others. The DRCF could act as an enabler, working with regulators on projects and building their capacity while doing so, similar to the way that the Behavioural Insights Team works with other bodies on behavioural economics. Internationally, there are a number of examples of governments taking a similar approach to digital transformation:

- In Estonia, the Chief Information Officer leads and coordinates digital initiatives across government[27]
- In Saudi Arabia, the National Digital Transformation Unit works with government entities and the private sector on digitalisation[28]
- In Singapore, GovTech is a statutory body responsible for the delivery of the Singapore government's digital services.[29]

There is a huge opportunity for UK regulators to lead the way on the digital transformation of regulation. This approach could help to reduce duplication, enable regulators - and particularly Ofcom - to respond to technological change across society more efficiently and ultimately lower the cost of regulation on firms and their customers.

How will Ofcom interact with the police in relation to illegal content, and do the police have the necessary resources (including knowledge and skills) for enforcement online?

Focusing solely on online fraud, it is clear that the police do not have sufficient resources to effectively tackle the issue or support those affected.

In a survey of 50 of our Research Community who had reported being scammed, Action Fraud was the body most commonly reported to (38%), with nearly three in ten (28%) victims reporting to the police. With Action Fraud being wound up and online scams increased, an increase in policing resources - both monetary as well as knowledge and skills - is badly needed.

Understanding of what it is like to be scammed online is particularly important for victims. Many Research Community respondents found it incredibly difficult to open up and tell someone about their experience of being scammed. Just one in five (18%) respondents felt supported when reporting, while over half (54%) disagreed.

"Police said no crime committed as I didn't give money away. Said I was foolish for trusting someone who lived in another country. Reported to scam sites at the time but wasn't worth the effort."
Expert by experience

Reliving being scammed, in order to report it, is often a painful experience for victims and can negatively impact people's mental health. This can be particularly harmful when victims feel

[27] https://e-estonia.com/cio-of-estonia-siim-sikkut-opens-the-countrys-tech-stack-to-the-world/
[28] https://ndu.gov.sa/en/
[29] https://www.tech.gov.sg/

embarrassed, only to be not taken seriously, or when they have a frustrating experience and are not able to recoup any losses.

"I told Action Fraud but as I didn't report it to the police at the time they couldn't do anything. I felt it was a waste of time reporting it. I didn't want them to do anything about my case, I wanted to stop it happening to someone else but they didn't understand that."
Expert by experience

Are the media literacy duties given to Ofcom in the draft Bill sufficient?

People with mental health problems often struggle to spot scams and, as a result, can feel unprepared and anxious online. Many of our Research Community respondents felt that providing people with information about how to identify and avoid scams could help address these feelings, and give people with mental health problems a better chance of protecting themselves.

A range of online scams education and awareness campaigns do exist, such as UK Finance's Take Five to Stop Fraud and efforts led by Citizens Advice and the National Trading Standards. But the experience of our Research Community respondents suggests that many people with mental health problems are not currently being reached. Given people with mental health problems comprise the majority of those who are scammed online, campaigns around literacy with regard to scams should:

- Partner with mental health services or support charities to help direct their existing messages towards people with mental health problems
- Develop scam awareness content specifically for people with mental health problems, explaining how common symptoms can make us more vulnerable
- Run targeted advertising campaigns.

However, it is important to note that no amount of media literacy initiatives can replace proactive work to prevent scams appearing on platforms in the first place. As our research has shown, when we are unwell with our mental health it can be particularly challenging to spot and report scams, even if we are well informed about how to do so. Media literacy initiatives should always be a complement to, rather than a replacement for, action by platforms and regulators to prevent and take down scams.

Contact: conor.darcy@moneyandmentalhealth.org