

DCMS and Home Office: Online Harms White Paper Barclays Response

Barclays is a transatlantic consumer and wholesale bank with global reach, offering products and services across personal, corporate and investment banking, credit cards and wealth management, with a strong presence in our two home markets of the UK and the US. With over 325 years of history and expertise in banking, Barclays operates in over 40 countries and employs approximately 85,000 people. Barclays moves, lends, invests and protects money for customers and clients worldwide.

Barclays welcomes the opportunity to engage with DCMS and the Home Office's Online Harms White Paper. In this response, we begin by providing some thematic perspectives on this hugely important topic, before responding to the specific consultation questions as posed in the consultation. We hope you find our views useful and we would of course be happy to discuss them further if helpful.

Barclays Perspective

Online Consumer Fraud Should be an Online Harm Under the New Regulatory Framework

The proliferation of the internet into all aspects of modern life has undoubtedly created enormous benefit for society. With the internet we have almost limitless access to information; we can purchase all kinds of goods and services without ever leaving our home or whilst on the go; and we can communicate with friends and family all over the world. But it is important to acknowledge that the internet also has a darker, more harmful side: the facilitation of child exploitation, terrorist extremism, and online cyber bullying are all undertaken on mainstream digital platforms. It is for this reason that we consider the Government's plans to tackle such online harms through a new system of accountability and oversight for technology companies, as a positive step forward.

However, we believe that the Government should widen their proposed definition of 'online harms' to encompass the clear and present threat of online platform-originated consumer fraud; a harm that is rapidly increasing in scale, having enormous negative impacts on consumers, and is increasingly being used to fund criminal activity, for example, county lines and terrorism. The Government's clear direction that this harm requires concerted action from the online platforms that enable it would represent a welcome and much needed step in helping protect customers and hamper the criminal elements who undertake this criminal activity.

Fraudsters and scammers are increasingly using sophisticated techniques, leveraging legitimate, online platforms and digital technologies to deceive and defraud consumers; for example, romance scams on dating websites, and scams using fake mirror profiles on social media platforms are now common methods of defrauding consumers. If these platforms and technology companies were subject to a duty of care and were required to have greater controls and protections in place, fewer scams would succeed, and fewer customers would lose out financially as a result, and funding to criminals would be reduced. Irrespective of whether customers ultimately have their stolen funds refunded, financial scams create great emotional distress to consumers who fall victim. It is therefore

imperative to maximise efforts to stop fraud and scams at their source – preventing them from taking place in the first place, rather than just remediating any financial impact to consumers.

Regrettably, the Government's proposed approach excludes online fraud from the scope of the new proposed regulatory framework, on the basis that there are separate Government initiatives seeking to tackle this issue. However, these initiatives focus predominantly on the financial services sector, placing responsibility and accountability for preventing fraud on financial institutions. While these initiatives are positive, they can only go so far. A more holistic approach, encompassing technology and social media platforms, would be much more effective in disrupting the fraud ecosystem, preventing fraud at its source, and reducing the flow of funds to criminals.

Given fraud and financial scams are one of the fastest growing crimes in Britain, and online platforms are playing an increasingly central role in online fraud, we therefore urge Government to reconsider the proposed scope of the new regulatory framework and include online fraud as an online harm.

The New Regulator Should be Empowered to Require Firms to Take Action to Reduce Fraud

Barclays believes including online fraud in scope of the new regulatory framework would provide a significant opportunity for the new regulator to take action against this increasing online harm.

Consumers, rightly, expect the organisations with which they engage to protect them from criminal activity. If a consumer trusts a dating site to find them a partner, or a social media site to engage in an online community, then those organisations should have a responsibility to take reasonable action to prevent that customer being targeted by fraudsters misusing their product, platform or service. Unfortunately, there are currently various barriers that may discourage these firms from taking action: the scale of online activity may make monitoring and policing content for online fraud seem a difficult task to tackle; and there may be little commercial incentive for these firms to take action to reduce the prevalence of online harms on their platform. However, these perceived barriers should not excuse these firms from their responsibilities to protect consumers. Rather, digital platforms and social media firms should face minimum requirements to protect their users, regardless of their complexity.

Positively, the introduction of this new regulatory framework, would require firms that currently inadvertently facilitate significant volumes of online fraud to take action, and would enable the proposed regulator to enforce changes and controls that could help prevent fraud taking place. And if firms fail to meet their new obligations and responsibilities, the new regulator should be empowered to hold them responsible for any negative social impact or consumer detriment that results – reflecting the 'polluter pays principle'.

Barclays therefore believes the proposed 'duty of care' for social media and digital platforms should include a responsibility to protect consumers from online fraud. As with any other utility, those who operate the systems should have responsibility for ensuring they are safe to use, fit for purpose, and not abused. At a very high level, this could be achieved by requiring social media firms and digital platforms to undertake adequate 'Know Your Customer' (KYC) checks on their users, so only legitimate

consumers are able to use their services, and by requiring them to deploy minimum standards of fraud prevention and detection measures across their platforms.

In the financial services sector, a group of Payment Service Providers have signed up to the Contingent Reimbursement Model (CRM) voluntary code. The code aims to reduce the prevalence of Authorised Push Payment (APP) scams, and reimburse customers where they have met a reasonable level of care. This is a major step forward, and demonstrates how an ecosystem wide framework can be implemented to ensure consumers are protected against online fraud. Given the central role major online firms play in facilitating fraud in the broader fraud and scams ecosystem, Barclays believes the CRM should be extended to include digital platforms and social media firms, requiring them to reimburse consumers for fraud undertaken on their platforms. Bringing these firms in scope of the CRM reimbursement principles would likely provide strong commercial incentives for them to take action to prevent fraud at its source, reduce the flow of funds to criminals, and reduce the harm caused by fraud and scams across the wider ecosystem.

In summary, to reduce the rapidly increasing levels of online fraud, Barclays believes:

1. Government should bring online fraud into scope of the online harms framework.
2. The proposed online harms regulator should be empowered to require social media and digital platforms to implement certain controls and requirements in order to reduce fraud.
3. The CRM voluntary Code should be extended to include social media firms and digital platforms, to reduce the incidence of fraud, and the harm it causes across the wider ecosystem.

Consultation Questions

1. This government has committed to annual transparency reporting. Beyond the measures set out in this White Paper, should the government do more to build a culture of transparency, trust and accountability across industry and, if so, what?

Barclays supports the Government's intention to require annual transparency reports from companies, outlining the prevalence of harmful content on their platforms and the measures they are taking to address the problem.

As set out in the section above, Barclays strongly believes that online fraud should be brought into scope of the new regulator as an online harm. Indeed, Barclays sees particular value in the reporting of economic crime and online fraud and scams by online firms, for example: the number of fake account accounts identified; the number of fraud / scam cases reported; the action taken in response to those reports. Transparent reporting of economic crime, and fraud and scams undertaken across the major online platforms would provide a much clearer sense of scale of the issue, which would subsequently help drive greater action to solve the problem. To ensure data published would be of maximum value, all firms should follow a standardised methodology to measure their online harms.

2. Should designated bodies be able to bring 'super complaints' to the regulator in specific and clearly evidenced circumstances?

Yes, Barclays supports the Government's proposed approach, enabling designated bodies to bring super complaints regarding online harms to a designated regulator.

– 2a. If your answer to question 2 is 'yes', in what circumstances should this happen?

Designated bodies should be allowed to bring forward super-complaints in circumstances similar to those prescribed in legislation covering the role of designated bodies in other markets (e.g. The Enterprise Act 2002 or the Financial Services (Banking Reform) Act 2012). Namely, designated bodies should be able to raise super-complaints where they see evidence that any feature, or combination of features is, or appears to be, significantly harming the interests of consumers.

3. What, if any, other measures should the government consider for users who wish to raise concerns about specific pieces of harmful content or activity, and/or breaches of the duty of care?

Barclays believes consumers should have the right to complain or raise concerns about specific pieces of online harm to the new regulator, as is the case with existing regulators, such as the Financial Conduct Authority (FCA), the Financial Ombudsman Service (FOS) and the Information Commissioner's Office (ICO). With respect to the FOS, if a consumer feels aggrieved by a financial service they have received, they can lodge a complaint with the FOS who will raise it with the firm in question. The establishment of an equivalent 'Digital Ombudsman' with oversight of social media platforms and responsibility to mitigate the risks as described in the White Paper and online fraud, may provide an effective model for consumers to raise concerns and seek redress arising from failure to prevent online harms or fraud on social media or digital platforms.

4. What role should Parliament play in scrutinising the work of the regulator, including the development of codes of practice?

Parliament should scrutinise the work of the new regulator for online harms in the same manner as they do for other existing regulators, policy and legislation, i.e. formal inquiries and ad hoc evidence sessions with the regulator. It is important to ensure consistent standards of scrutiny across the board.

5. Are proposals for the online platforms and services in scope of the regulatory framework a suitable basis for an effective and proportionate approach?

Barclays believes that the proposals are appropriate for the online harms identified as being in scope of the regulatory framework. However, as we have set out, Barclays strongly believes that economic crime and online fraud should also be brought into scope of the new regulator as an online harm. This would enable the new regulator to take effective action against online firms if they facilitate this rapidly growing crime.

6. In developing a definition for private communications, what criteria should be considered?

Barclays believes any new regulatory framework introduced to protect the public online should not apply to companies' internal private communications networks or platforms.

7. Which channels or forums that can be considered private should be in scope of the regulatory framework?

As set out previously, Barclays strongly believes that online fraud should be brought into scope of the new regulator as an online harm.

Online private channels and forums are often used by criminals to undertake online fraud. Barclays believes that where there is suspicion of abuse by particular individuals or organisations based on a complaint or other information, private channels and forums provided by online platforms should be in scope of the regulatory framework. Of course, as acknowledged in the consultation document, any action taken by the regulator should be proportionate and consistent with Article 8 of the European Convention on Human Rights. Without access to private channels, large swathes of the internet would be out of reach of the regulator and its potential effectiveness as a regulator would be reduced.

– **7a. What specific requirements might be appropriate to apply to private channels and forums in order to tackle online harms?**

Any specific requirements applied to private channels would need to be proportionate and aligned with all applicable data privacy requirements.

8. What further steps could be taken to ensure the regulator will act in a targeted and proportionate manner?

When this new regulator is established, it is important to ensure it is aligned with other regulators, for example, the FCA, ICO, OfCom, to ensure there is close cooperation and

interaction, and no duplication in remit exists. It is also important to ensure the role of this new regulator is clear, vis-à-vis the broader consumer and competition law responsibilities of Competition and Markets Authority, the sectoral regulators and any new regulatory function introduced following the Furman Review of Competition in Digital Markets.

As mentioned previously, Barclays strongly believes that online fraud should be brought into scope of the new regulator as an online harm. If this were to occur, Barclays believes the regulator should:

- commit to a Service Level Agreement to respond to urgent concerns raised by industry, for example, e.g. taking action to ensure third parties remove adverts identified as being fraudulent within a reasonable period of time.
- introduce Know Your Customer (KYC) and due diligence requirements for social media, digital platforms and online advertisers. Currently, these requirements do not exist, allowing online criminals to misrepresent themselves online, and scam both vulnerable and tech savvy consumers. Having such identity verification procedures in place would deter and likely reduce the number of parties looking to engage in fraudulent activity. Similar requirements have existed in financial services for many years. With the transformation of the internet, these protections should be replicated for online firms to reflect modern times, and ensure consumers are best protected.
- undertake periodic assessments of the online-harm threat landscape, with wider input and support from industry, to remain up to date with the nature and volume of the most harmful activities. This will help target enforcement and so ensure regulation remains proportionate.
- introduce a kitemark standard for firms to demonstrate they comply with the regulatory framework, which would encourage a voluntary increase in standards.
- introduce a framework of principles to guide the behaviour of firms, similar to the FCA's Conduct of Business rules.

Furthermore, to ensure the regulator acts in an appropriate and proportionate manner, the enabling regulation could include a regulatory steer, setting out the relevant principles to be followed by the regulator in the exercise of its duties.

9. What, if any, advice or support could the regulator provide to businesses, particularly start-ups and SMEs, comply with the regulatory framework?

It may not be clear to some firms whether they are in scope of the new regulatory framework and whether they are subject to any new requirements. The regulator should develop clear, easily understood guidelines to help firms understand their responsibilities and best practice guidance on how they can comply with any new framework. The new regulator should also seek to raise awareness and educate firms how their business model could be exploited by criminals for fraudulent purposes. For example, a start-up establishing a new social network platform may not fully appreciate how its platform could be abused by fraudsters.

Barclays would suggest that the larger social media firms and digital platforms would be relatively well equipped to implement and comply with the new framework, given the resources available to them.

10. Should an online harms regulator be: (i) a new public body, or (ii) an existing public body?

Regardless of whether the new regulator is established as a new public body, or within an existing public body, Barclays believes it should be equipped with expertise in all relevant areas required to fulfil its responsibilities.

As mentioned previously, Barclays strongly believes that online fraud should be brought into scope of the new regulator as an online harm. It is for this reason that Barclays believes the new regulator should work in close cooperation with the existing financial services regulator, the FCA, and the FOS to ensure it is best positioned to take action against online fraud. Indeed, as mentioned previously (see response to questions 3 and 8), it is vital that the new regulator works closely with all other interested regulators to ensure all stay aligned and they are not driving towards competing objectives.

– **10a. If your answer to question 10 is (ii), which body or bodies should it be?**

Barclays has not responded to this question.

11. A new or existing regulator is intended to be cost neutral: on what basis should any funding contributions from industry be determined?

Any funding contributions from industry should be provided by the online platforms and social media firms the new regulatory framework is intended to cover. Funding could also be part-generated through a model equivalent to the FOS, where a fee is levied on a firm by the regulator, if a complaint is made against that firm.

12. Should the regulator be empowered to i) disrupt business activities, or ii) undertake ISP blocking, or iii) implement a regime for senior management liability? What, if any, further powers should be available to the regulator?

Barclays strongly believes that the new regulator for online harms should be provided with strong powers of intervention to achieve its objectives. We would support the regulator having all the powers referenced in the question.

Barclays believes the regulator should have the power to check whether human intervention is included in any process resulting in 'decisions' stemming from automated decision making (under the GDPR and in conjunction with the Information Commissioner) in the context of profiling using personal data, where an outcome has resulted in, or has the potential to result in, online harm.

If the CRM voluntary code is not extended to cover social media and digital platforms directly, Barclays believes the regulator should be empowered to require these firms to refund consumers who fall victim to a scam on their platform, if the firm is deemed to be at fault.

When seeking to create a protective environment for consumers online, use of 'soft powers' to encourage outcomes on a best efforts basis will be insufficient to resolve the problems that currently exist. The regulator should be appropriately empowered to take action or enforce new mandatory rules or requirements on entities within its remit. Financial services and medicine are good examples of strong regulatory frameworks resulting in positive consumer outcomes.

The new regulator will require wide information gateways to share information with relevant organisations and law enforcement both within the UK and overseas.

13. Should the regulator have the power to require a company based outside the UK and EEA to appoint a nominated representative in the UK or EEA in certain circumstances?

Yes, the regulator should have the power to require a company based outside the UK and EEA to appoint a nominated representative in the UK, if doing so would help it achieve its objective of reducing online harms. It is important to recognise the difficulties in seeking to regulate a global online network that does not operate with national borders, within the boundaries of only one jurisdiction. There is a risk that the online harms regulator may be unable to take action if a firm is based, or harm is committed, outside of the UK or EEA. The online harms regulator should therefore take bold action to ensure it has the necessary powers or authority to effectively regulate the ecosystem within the UK, and is able to work closely with regulators and law enforcement overseas to achieve its objectives.

14. In addition to judicial review should there be a statutory mechanism for companies to appeal against a decision of the regulator, as exists in relation to Ofcom under sections 192-196 of the Communications Act 2003?

Barclays believes there should be a statutory mechanism providing the opportunity for firms to appeal against a decision of the regulator.

- **14a. If your answer to question 14 is ‘yes’, in what circumstances should companies be able to use this statutory mechanism?**

Barclays has not responded to this question.

- **14b. If your answer to question 14 is ‘yes’, should the appeal be decided on the basis of the principles that would be applied on an application for judicial review or on the merits of the case?**

Barclays has not responded to this question.

15. What are the greatest opportunities and barriers for (i) innovation and (ii) adoption of safety technologies by UK organisations, and what role should government play in addressing these?

Unfortunately, there are currently various barriers that may discourage digital platforms and social media firms from taking action to address online harms: the scale of online activity may make monitoring and policing content for online fraud seem a difficult task to tackle; and there may be little commercial incentive for these firms to take action to reduce the prevalence of online harms on their platform. However, these perceived barriers should not excuse these firms from their responsibilities to protect consumers. Rather, digital platforms and social media firms should face minimum requirements to protect their users, regardless of their complexity. The establishment of a new regulator and regulatory framework may be required to force firms to take action.

16. What, if any, are the most significant areas in which organisations need practical guidance to build products that are safe by design?

Greater information sharing by digital platforms and social media firms and the new regulator, on evolving online harms and how they are perpetrated, would be helpful for other firms looking to take action.

17. Should the government be doing more to help people manage their own and their children's online safety and, if so, what?

Yes, Government should do more to help all demographics, not just vulnerable people and children, manage their online safety. Barclays believes government should specifically do more to raise awareness of the risks of online fraud, and educate on best practice to stay safe online.

18. What, if any, role should the regulator have in relation to education and awareness activity?

As per question 17, regulators should do more to raise awareness of the risks of online fraud, and educate on best practice to stay safe online.