Written evidence submitted by Barclays (OSB0106)

About Barclays

Barclays is a British universal bank. We are diversified by business, by different types of customer and client, and geography. Our businesses include consumer banking and payments operations around the world, as well as a top-tier, full service, global corporate and investment bank, all of which are supported by our service company which provides technology, operations and functional services across the Group. For further information about Barclays, please visit our website home.barclays.

Barclays' Headline Recommendations on the Draft Bill

Barclays' Recommendations

A. The duty of care should be extended to require regulated service providers to also protect users from scam content that is not user-generated: in particular, paid-for fraudulent adverts and links to fraudulent cloned websites.

B. The draft Bill should include provisions allocating liability on regulated services providers for losses incurred by victims of scams undertaken on their platform.

C. The Bill should make clear that fraud and scam content is to be treated as severe illegal content with content minimisation requirements similar to terrorism and CSEA offences, or at the very least, it should be designated in the primary text as 'priority illegal content'.

D. Building on the framework designed for regulated service providers, an additional pillar should be added to the Bill with provisions applying to web hosting service providers and Internet Service Providers (ISPs), designed to tackle fraudulent cloned websites.

Barclays Perspective

The Rapidly Growing Problem of Scams in the UK

1. An Authorised Push Payment scam, or 'APP scam', occurs when a consumer or business is deceived into voluntarily authorising a payment to a fraudster, believing the payment is for a legitimate purpose. Scams differ to other types of fraud, which involve criminals gaining unauthorised access to accounts and making payments that are unauthorised by the account holder.

2. The number of scams is increasing rapidly in the UK (a 77% increase from 2018 to 2020), resulting in devastating consequences for consumers and businesses, as well as undermining the broader economy. In 2020, UK customers lost £479 million as a result

of scams, an increase of 35% from 2018. Alongside the financial cost, scams result in emotional trauma for victims, even where they are reimbursed; according to the Money and Mental Health Institute, 40% of online scam victims report significant emotional trauma and lasting impacts on their mental health. It is important to recognise that APP scams can impact all corners of society; consumers of any age or background, and businesses of all types and size. While many may believe that older people may be most at risk of scams, Barclays' research has revealed that the 21-30 age group is actually the age bracket that fell victim to the highest number of scams in the past three months (29 per cent of total scams), followed closely by those aged 31-40[1].

3. The public policy objective must be, therefore, to reduce the incidence of scams prevent them occurring at their source. This will not only reduce the emotional stress suffered by victims but will also deprive criminals of fraudulently obtained income.

Scams Have Evolved to Leverage Online Platforms

4. The retail banking sector has a critical role to play in detecting and preventing scams, and educating consumers on how they can protect themselves. However, the nature of scams has changed markedly in recent years, with the majority (our data suggests 60%) now enabled by criminals' exploitation of online platforms (e.g. online commerce/auction websites, social media platforms, dating websites etc) as part of the 'scams ecosystem'.

5. As a result, the 'capture' (social engineering and manipulation of victims) takes place away from banks' infrastructure, on these online platforms over which banks have no control or oversight. The attempted payment to the criminal at the final stage of the scam is the first that a bank will see of what is a complex 'scam journey', meaning there is a limit to banks' ability to identify and prevent the scam. It is critical, therefore, that these online platforms are required to take greater action at the source to prevent scams occurring in the first place. Without this, there is a limit to what can be done to reduce the prevalence of scams, and to protect customers from their devastating impacts.

The Online Safety Bill is the Solution

6. At present there is little, or no, specific legislation or regulation that requires online firms to act to minimise and prevent the occurrence of scams on their systems, or provides any consequences if they fail to do so. It is imperative, therefore, that we seize the opportunity presented by the Online Safety Bill to address this critical gap.

7. The draft Bill makes some positive and welcome progress in the battle to combat online platform enabled scams. However, Barclays has a number of recommendations to improve the Bill and strengthen the UK's capabilities to prevent scams.

8. Barclays' recommendations:

[1] Mortar Research study of 2,000 participants, July 2021

A. The duty of care should be extended to require regulated service providers to also protect users from scam content that is not user-generated: in particular, paid-for fraudulent adverts and links to fraudulent cloned websites.

B. The draft Bill should include provisions allocating liability on regulated services providers for losses incurred by victims of scams undertaken on their platform.

C. The Bill should make clear that fraud and scam content is to be treated as severe illegal content with content minimisation requirements similar to terrorism and CSEA offences, or at the very least, it should be designated in the primary text as 'priority illegal content'.

D. Building on the framework designed for regulated service providers, an additional pillar should be added to the Bill with provisions applying to web hosting service providers and Internet Service Providers (ISPs), designed to tackle fraudulent cloned websites.

Problems with the Draft Bill, and Recommendations to Improve

Problem 1 - The focus only on user-generated illegal content leaves significant gaps in the framework

9. The draft Bill imposes a duty of care on providers of user-to-user services, to protect their users from illegal content generated and shared by other users. Government is clear in its press release that illegal content in this context covers fraudulent and scam material that is user-generated. This represents a welcome step forward, considering that government had previously stated this Online Safety framework would not cover any economic crime or harms.

10. However, while the inclusion of user-generated scams in scope of the Bill is a positive step, we do not believe it is sufficient to comprehensively tackle the problem of online platform enabled scams. We estimate that user-generated scams only represent c.30% of all online platform-enabled scams, and tend to be relatively low value and small scale scams, for example, a purchase scam in which a fraudster deceives a user on an online commerce website into purchasing an item that does not exist.

11. Crucially, the duty of care does not require regulated services providers to protect their users from illegal content that is not generated and shared by other users. As a result, fraudulent and scam material that appears on regulated service provider, but is not posted by users, would not be covered by the duty.

    a. As an example, a fraudulent advertisement (e.g. for fake high-return, zero-risk investment opportunities) that is sponsored or paid-for by a criminal to appear as a legitimate advert on a regulated service provider, would not be covered by the duty of care. As a case study, a Barclays customer lost over £251k after

engaging with an advert on a social media platform for a fraudulent 'investment opportunity' involving cryptocurrency. This type of fraudulent scam content tends to have a much greater scale in that it can reach a very large number of users at the same time, and therefore has a much greater value of impact. The duty of care not covering this type of scam content represents a significant gap in the Online Safety Bill framework, as there is no requirement on the provider to protect their consumers from the risks posed.

b. Similarly, the paid-for promotion of links to fraudulent cloned websites on platforms and search engines is not covered by the duty of care. As explained in 'Problem 3' below, criminals are increasingly using fraudulent cloned websites to deceive and scam consumers. While we believe the Bill should include specific measures to tackle these cloned websites at their source (see Recommendation C), it is critical that the Bill's duty of care also requires the regulated service providers to protect their users against inadvertently accessing any cloned websites promoted on their platform. For example, user-to-user services should be required to identify, minimize and prevent the promotion of fraudulent cloned websites on their platform as part of their duty of care. Likewise, search service providers should be required to ensure the paid-for links they are promoting at the top of their search results are not directing their users to fraudulent cloned websites.

12. Therefore, to really make a difference in tackling online scams, the duty of care should be extended to require regulated services providers to also protect users from scam content that is not user-generated, in particular, paid-for fraudulent adverts and links to cloned websites.

13. We would note that this position is shared by a number of relevant stakeholders, including but not limited to: Andrew Bailey; Nikhil Rathi; Martin Lewis; Which?; the Work and Pensions and Treasury Select Committees; as well as UK Finance and the broader retail banking sector.

Recommendation A - The duty of care should be extended to require regulated service providers to also protect users from scam content that is <u>not</u> user-generated: in particular, paid-for fraudulent adverts and links to fraudulent cloned websites.

Problem 2 – The Bill does not introduce any liability on regulated services providers for losses incurred by victims of scams undertaken on their platform

14. As set out above, the majority of APP scams now involve criminals exploiting online platforms to engage and scam their users. At the very final stage of the scam, the victim will make a payment to the criminal through their bank.

15. Nine banks have voluntarily developed and agreed an industry Code, known as the Contingent Reimbursement Model Code (CRM Code, or 'the Code'), setting out a framework to guide when and how scam victims should be reimbursed. This Code

dictates that where the bank is deemed to be at fault, e.g. it fails to detect unusual activity, or to effectively warn the customer against the risk of a scam, it should be responsible for reimbursing the victim. It dictates that where the customer is deemed to be at fault, e.g. they have not undertaken any level of check or due diligence to ensure the situation is legitimate, or have ignored bank warnings, they are to bear some if not all of the loss from the scam. However, for scenarios where neither the bank nor the customer are deemed to be at fault, so called 'no blame' scenarios, banks are currently required to reimburse the victim, despite it being clear and accepted that they were not at fault and took reasonable action to prevent the scam.

16. Currently, there are no requirements on the online platforms to minimise and prevent the occurrence of scams on their systems, nor are there any requirements on them to reimburse or contribute to the reimbursement of victims of scams undertaken on their platform.

17. While the draft Bill includes enforcement provisions, including significant fines, these will not be used to reimburse victims of scams. The draft Bill should therefore be amended to require the online platforms in scope to contribute to an economy-wide scam victim reimbursement fund, commensurate with their role in enabling scams. This liability for losses incurred by scam victims would provide a major incentive for them to take significant action to prevent scams taking place in the first instance.

Recommendation B – The draft Bill should include provisions allocating liability on regulated services providers for losses incurred by victims of scams undertaken on their platform.

Problem 3 - Fraud and scams content is not treated as high severity or 'priority' illegal content in the draft Bill.

18. The draft Bill sets out three categories of illegal content, with a scale of severity:
    i. The most severe illegal content is any offence relating to terrorism or child sexual exploitation and abuse (CSEA).
    ii. The next level is 'priority illegal content', which includes offences that will be specified in secondary regulations by the Secretary of States. While this is still to be specified, the government's response to the Online Harms White Paper suggested this category could include hate speech and the sale of illegal drugs and weapons.
    iii. The last tier of illegal content is a catch all tier covering any offence, where the victim is an individual.

19. The duty of care to protect users from illegal content imposes certain base level requirements on user-to-user service providers that apply for all three categories. For example, providers must undertake an 'illegal content risk assessment' and take proportionate steps to mitigate and effectively manage risks of harm to individuals identified in their risk assessment.

20. However, the duty of care also imposes certain additional requirements on the provider, depending on the severity/category of the illegal content in question.
    - For example, for the most severe terrorism and CSEA illegal content, providers must also follow specific requirements on content minimisation set out in codes of practice to be developed by OFCOM, and be subject to new powers conferred to OFCOM enabling it to order firms to efficiently identify and take down content.
    - For 'priority illegal content', providers must also use proportionate systems and processes designed to minimise the presence of such content, the length of time it is present, and its dissemination.

21. It is not clear from the draft Bill into which category of illegal content fraudulent and scam content will fall. The Bill does not specifically list fraud and scam content as being the most severe illegal content on a level with terrorism and CSEA, and there is currently no indication from government or the draft Bill that it will be deemed 'priority illegal content'. This would, by default, leave fraud and scam material being caught in the third tier of illegal content, with service providers only required to undertake the base requirements described above in para 20 – i.e. mitigating and managing risks identified in providers' own risk assessments. With fraud and scam content only caught in the bottom catch-all tier of illegal content, there would be no specific requirements or duty on providers to minimise the presence and dissemination of the content.

22. With online fraud and scams content growing so rapidly in the UK, and UK citizens becoming increasing exposed and vulnerable to skilled and experienced criminals on online platforms, it is not sufficient for fraud and scam content to be caught only in the third tier of illegal content under the draft Bill, with providers only subject to the base level requirements. More broadly, this low-level intervention would be unlikely to result in a substantial reduction in the volume and value of scams – continuing to expose potential victims and missing this once in a generation opportunity to stop scams at source.

23. While we recognise the extreme severity of terrorism and CSEA offences, we firmly believe that fraudulent and scam content (the largest by volume crime in the UK) should be recognised as sufficiently severe so as to require specific treatment under the Bill. This could be in a similar manner to terrorism and CSEA, with similar content minimisation obligations applying to providers, or at the very least, the Bill should be clear in in its primary legislation text that fraud and scams (amongst others) are to be designated as 'priority illegal content'. That is to say the list of offences to be deemed 'priority illegal content' should not all be left to secondary regulations by the SoS.

Recommendation C – The Bill should make clear that fraud and scam content is to be treated as severe illegal content with content minimisation requirements similar to terrorism and CSEA offences, or at the very least, it should be designated in the primary text as 'priority illegal content'.

Problem 4 - The draft bill does nothing to tackle fraudulent cloned websites

24. The government's stated objective for the Online Safety Bill is to protect consumers in the UK from illegal and harmful content online.

25. To achieve this objective, the draft Bill is designed in a way to impose a duty of care on regulated service providers to protect their users from illegal and harmful content. However, there are other ways that consumers can encounter and suffer illegal and harmful content online that do not involve the regulated service providers covered by the Bill. The most significant example is consumers inadvertently visiting fraudulent cloned websites imitating the legitimate websites of well-known firms. Criminals will develop a cloned website almost perfectly identical to a legitimate website, in order to deceive a victim into entering critical information or sending funds as part of a scam or other fraud. As an example, a Barclays customer lost over £175k after visiting a cloned website imitating a major investment firm as part of an investment scam. This is an increasingly significant problem and may see criminals driving traffic to their cloned website through fraudulent adverts on popular platforms, phishing scams (sending fake emails to direct the recipient to a fake website) and smishing scams (sending fake text messages to direct the recipient to a fake website).

26. Despite being a major type of illegal and harmful content online, the draft Bill does not include any provisions intended to tackle this growing problem. Barclays firmly believes that, building on the framework designed for regulated service providers, an additional pillar should be incorporated into the Bill with provisions designed to tackle fraudulent or cloned websites. These provisions should be targeted at the organisations which 'host' and support these websites (web hosting service providers) and should require them to undertake due diligence on the websites and those developing them, and ultimately take down any fraudulent or cloned pages. The Bill should also apply to Internet Service Providers (ISPs) so that, in the event that the website is hosted by an organisation outside the UK and not subject to the Bill, the ISPs can be required to block access to the page where it is flagged to them.

27. This additional focus of the Bill would provide additional powers and leverage to help combat online fraud enabled by fraudulent websites.

Recommendation D – Building on the framework designed for regulated service providers, an additional pillar should be added to the Bill with provisions applying to web hosting service providers and Interest Service Providers (ISPs), designed to tackle fraudulent cloned websites.

Annex – Barclays Understanding of the Draft Bill

Objective - the draft Online Safety Bill is intended to establish a new regulatory regime to address illegal and harmful content online, with the aim of preventing harm to individuals in the UK.

Key Elements

- The Bill imposes various duties on providers of 'regulated services' i.e. user-to-user services, and search services, including.
    - A duty to protect users from illegal content, generated and shared by other users. Providers must take proportionate steps to mitigate and effectively manage the risk of harm caused by illegal content, and use proportionate systems and processes to minimise the presence of certain priority illegal content (to be defined in future regulation) and swiftly remove such content on notice.
    - A further duty relates to harmful content. There are safeguarding obligations for services "likely to be accessed" by children, and providers of user-to-user services which meet specified thresholds (defined as 'Category 1 services') are subject to additional duties in relation to content that is harmful to adults. Harmful content includes content with a 'material risk' of causing a 'significant adverse physical or psychological impact'.
- In addition to the duties to safeguard against illegal and harmful content, the Bill also imposes duties on regulated service providers in relation to the protection of users' freedom of expression and privacy rights. Category 1 service provider are also subject to duties in relation to journalistic content and content of democratic importance.
- The Bill confers powers on OFCOM to oversee and enforce the new regulatory regime (including dedicated powers in relation to terrorism content and child sexual exploitation and abuse (CSEA) content), and requires OFCOM to prepare codes of practice to assist providers in complying with their duties of care.
- **Enforcement** - Providers that fail to meet their duties under the new Bill would be subject to potential enforcement action. Ofcom would have the power to impose fines of up to £18 million, or 10% of a providers' annual global revenue, whichever is highest. It would also be able to seek court orders to disrupt the activities of non-compliant providers or prevent access to their services altogether where it is deemed there is a risk of significant harm to individuals in the UK.

21 September 2021