Written evidence submitted by Lloyds Banking Group plc (OSB0135)

About Lloyds Banking Group plc

We are a financial services group focused on retail and commercial customers – with millions of customers in the UK, and a presence in nearly every community. It is our role to help businesses and individuals, while making a positive contribution to the communities in which we operate. Lloyds Banking Group incorporates a number of household names like Lloyds Bank, Halifax, Bank of Scotland and Scottish Widows.

Tackling online financial scams

1. Our primary interest in this draft legislation concerns its potential contribution towards efforts to tackle online financial scams. In short, it is critical that urgent action is taken to prevent fraud and in so doing reduce the impact of online financial scams on households and businesses in the UK. A significant part of the solution lies in strengthening the provisions of the Bill to ensure there is a comprehensive legal framework in place to prevent multiple sources of online financial scams – not just user-generated content as currently proposed.

2. The Government's decision earlier this year to include measures in the Bill to tackle online financial scams originating from user-generated content was a welcome development in the joint public/private effort to tackle fraud. We see this as a highly significant step, as it will for the first time place requirements on online platforms, including social media companies, to take appropriate action to prevent the abuse of their services by criminals seeking to perpetrate fraudulent activity.

3. This should lead to a reduction in the use of online platforms by criminals to steal money from users, but also to reduce their use in recruiting users to participate in criminal activity (e.g. as money 'mules'). It would serve to incentivise further efforts to vet, remove and block fraudulent online accounts and content, as well as greater investment in human and automatic review systems.

4. It should lead to the creation of better channels for users and other parties to report scams, for example by cooperating with the payment providers that discover them. There is also scope for platforms to improve awareness among their users on how to recognise scams, to encourage users to report fraudulent content and to take more action to report cases to law enforcement.

Scale of the challenge

5. Online financial scams can have a profound impact on victims, either financially or emotionally. Even if the individual is compensated in full by their bank, the organised criminal gangs that perpetrate this fraudulent activity still profit from the proceeds. Such monies can go on to fund illicit acts – terrorism, drug trafficking and people smuggling – that damage the fabric of our society.

6. The banking industry worked to prevent over £1.6bn of fraud last year. As a result of the significant industry investment to date in fraud prevention measures, approximately two-thirds of attempted fraud is successfully intercepted. This investment includes initiatives such as enhanced customer awareness, fraud detection systems, the introduction of Confirmation of Payee technology, and real-time detection of 'mule' accounts. We recognise that there is more we can do as a bank and as an industry, and we are committed to working collaboratively to this end, but equally there is more that could be done to raise standards across the broader economy and protect the public from fraud.

7. Despite these efforts, the fraud threat continues to flourish. There has been particular growth in fraud perpetrated through social media content and online adverts in recent years. For example, there has been a 38% increase in the volume of so-called 'romance' scams involving social media and dating platforms since 2019.

8. Fake social media accounts are often used to recruit young people as money mules or used to trade stolen card details. Criminals use online platforms to engage their victims, offering goods and investments which never materialise once the payment has been made. In the case of purchase scams for example, our data shows that 93% of victims made the first contact with the fraudulent seller, who were simply waiting to be contacted.

9. Based on our analysis of reported fraud affecting our customers, user-generated online content accounts for a quarter of all fraud by volume (and <10% by value), compared to 40% (a quarter by value) for advertising via online platforms and e-mail. The remainder of fraudulent activity (two thirds by value) is derived from offline sources, including telephone and SMS messaging. As such, the Bill as drafted only seeks to address a small proportion of fraudulent activity and leaves households and businesses exposed to multiple ongoing fraud threats.

Improving the Bill

10. It is notable that, despite the Government's commitment to tackle "ruthless criminals who defraud millions of people and sick individuals who exploit the most vulnerable in our society" and be "unapologetic in going after them"[1], there is nevertheless no mention of fraud or financial scams in the Bill itself. In the absence of any specific financial scam prevention measures, this suggests that measures to tackle online financial scams originating from user-generated content will fall within the general measures in the Bill relating to illegal content posted online.

11. A more robust approach would include the provision of an explicit definition of online financial scams, for example specifying the types of fraud offences that will be captured by the Bill. Critically, this should also include financial scams that are promoted through both paid-for online advertisements and cloned websites. Online platforms would then have greater clarity about the new requirements applicable to them, as would the

[1] DCMS / Home Office press release, 12 May 2021: https://www.gov.uk/government/news/landmark-laws-to-keep-children-safe-stop-racial-hate-and-protect-democracy-online-published

nominated regulatory body responsible for overseeing compliance with the new regime.

12. As it stands, Section 39 (2) (f) of the Bill explicitly carves out paid-for advertising from the definition of what constitutes regulated content for the purposes of the legislation. This is a missed opportunity to deal with a significant source of online scams, by placing obligations on online advertising platforms as the publishers of this advertising content. The Government has so far stated that it aims to address online scams originating from paid-for advertising via its forthcoming Online Advertising Programme – however, little is known of this initiative and its timeline is uncertain, suggesting there will be a considerable delay before any of its measures take effect in helping to prevent scams and fraudulent activity.

13. Similarly, online financial scams originating from cloned websites risk being excluded from the legislation because Section 41 (6) (a) of the Bill excludes infringements of intellectual property rights from the definition of a "relevant offence". This contrasts with the approach being taken by other jurisdictions also adopting new legislation designed to combat online scams, for example by placing obligations on online platforms to remove a broader array of illegal content, including where there is an infringement of intellectual property rights.

14. The likely consequence of these exceptions in the UK's approach is that the overall effectiveness of this important legislation in tackling online financial scams will be much reduced. We therefore strongly encourage the Government and Parliament to consider the best way to address these shortcomings in the Bill so as to accelerate efforts to prevent fraud and make the UK's financial system safer for households and businesses.

Concluding remarks

15. The Online Safety Bill provides a golden opportunity to halt a significant source of illegal and harmful content that facilitates online financial scams. However, as drafted, the Bill only seeks to address one source of online financial scams: user-generated content, which accounts for a small proportion of overall financial scam activity. Extending the scope of the Bill to include paid-for advertising and cloned websites would hold out the prospect of making a lasting impact on the scourge of fraud in the UK.

16. Improving the Bill in this way should be combined with further concerted efforts to combat fraud. Among these efforts should be broadening the burden of financial liability when reimbursing the victims of fraud deemed to have acted appropriately in protecting themselves. At present this liability rests solely with financial institutions, but there is a case for other actors including online platforms and telecommunications companies to share the liability where their services have been abused to perpetrate fraudulent activity. This will provide an incentive for these sectors to take steps to prevent the use of their services by fraudsters.

17. Further steps could include requirements on online platforms to share data on scam advertising and cloned websites with telecommunications companies, so that they may

take steps to ensure that advertised phone numbers and websites / IP addresses are blocked. Finally, online platforms could be required to identify ‘at risk’ users of its platforms, allowing them to display tailored warning messages (or service blocks) so as to help prevent online scams from occurring in the first place.

Case study – example of a financial scam involving a cloned website

David [J] is an 81-year-old retired businessman and has been a Halifax customer since 1992. In January this year, Mr J completed an online questionnaire expressing interest in taking out a two-year fixed bond investment. The next morning, he received a call from a man claiming to be a representative of a well-known investment company saying he believed Mr J was interested in investing and suggesting he send a prospectus.

This initial interaction prompted a series of convincing activities including e-mails, a cloned website and even calls from someone claiming to be a compliance manager checking Mr J's eligibility to invest and using terminology you might reasonably expect to hear when investing, such as: "are you sure this is the right investment for you?"; "you're not investing all your money – are you leaving yourself a nest egg?"

There was nothing in this professional approach that screamed 'fraud' and he was keen to invest £80,000 that he had set aside for his children. By this point Mr J had provided his ID and signature to progress the application. When he went into the local Halifax branch to make an electronic transfer to the 'investment company', the Halifax bank staff asked for more details about the payment. Looking at the paperwork provided from the 'investment company', the staff expressed concerns specifically around the receiving bank account details, the requested 'reason for payment' that didn't mention an investment, and also assurances that should any alerts be received during the transfer, not to be alarmed.

They spoke to Mr J about these at length and through their conversation it transpired that Mr J's brother-in-law had held an investment with the (legitimate) investment company in question for a number of years. The staff suggested he check the details provided with his brother-in-law before any transfer was made, and on contacting the legitimate business it became clear that fraudsters had been at work and it was all an elaborate scam. The staff have since helped point out a number of resources to help Mr J stay safe following the details he unwittingly provided to the fraudster including:

- registering with credit reference agencies so he will be alerted if anyone uses his details to apply for bank accounts, credit cards or other loans
- changing any PIN numbers and passwords
- contacting Action Fraud
- getting his computer checked for any viruses

Mr J has reported the scam to the FCA which is aware of activities of people claiming to be from this company, and he has also contacted Cifas [the cross-sector fraud prevention organisation], keen to do whatever he can to prevent this from happening to other people. Mr J is tech-savvy and has since installed a VPN connection to provide additional protection for his e-mail.

27 September 2021