Written evidence submitted by Revolut

Revolut's response to the DCMS Sub-Committee on Online Harms and Disinformation's Call for Evidence

Introduction

1. Revolut welcomes the opportunity to respond to the DCMS Sub-Committee's Call for Evidence, and looks forward to working with the Committee as its inquiry progresses.

2. Revolut supports the Government's goal of making the UK the safest place in the world to be online, as well as the specific policy objectives for the Bill. Revolut welcomes the recent confirmation from the Prime Minister that "one of the key objectives of the Online Safety Bill is to tackle online fraud"[1].

3. Our response focuses on question 4 (omissions from the Bill), and sets out a proposal to strengthen the Bill in relation to online fraud perpetrated through paid-for advertising.

About Revolut

4. Revolut is a British financial technology company offering retail and business financial services to 16 million customers in the UK and around the world. Revolut is the UK's fastest growing and most valuable private technology company.

5. Revolut is building the world's first global financial superapp, to help people get more from their money – from everyday spending to planning for the future. In 2015 Revolut launched in the UK offering money transfer and exchange. Today, our customers around the world use dozens of Revolut's innovative products to make more than 150 million transactions a month.

6. Across our personal and business accounts, we help customers improve their financial health, give them more control, and connect people seamlessly across the world.

Executive summary

7. The Prime Minister recently confirmed that "one of the key objectives of the Online Safety Bill is to tackle online fraud".

8. A significant and growing proportion of frauds perpetrated against our customers originate from paid-for advertising, and industry wide data show that 70% of fraud in 2020 originated from online platforms.

9. However, the Bill as drafted explicitly **excludes** paid-for adverts from the scope of the new regulatory regime (Section 39 Clause 2(f)). We do not believe that the Government's objective for the Bill to tackle online fraud can be met if this carve out remains.

---

[1] https://committees.parliament.uk/oralevidence/2308/default/#page=19

10. Therefore, **Revolut recommends that S.39 2(f) is removed from the Bill** prior to its introduction to Parliament.

The scale of the problem

11. Fraud poses a significant and growing threat to the UK public and economy. According to the most recent data from the Office for National Statistics, there were 4.3 million incidents of fraud last year, making fraud the most likely crime that adults can fall victim to in the UK[2]. Action Fraud data estimate that the cost of this fraud was £1.7 billion[3].

12. The true cost and incidence of fraud is likely to be significantly higher than these official statistics as fraud is typically unreported - for example the National Crime Agency estimate that 80% of fraud cases are not reported[4].

13. One of the most common types of fraud in recent years has been Authorised Push Payment (APP) fraud. In an APP fraudulent transaction, a customer is duped into making a payment to another account which is controlled by a criminal.

14. Data from UK Finance show that the number of APP frauds are increasing significantly - fueled by the consequences of the Covid-19 pandemic[5].

The impact of fraud

15. Online fraud does not just create significant financial losses for industry and the public - it has a devastating emotional impact on victims and facilitates serious organised crime.

16. As APP fraud involves victims being directly manipulated into making a fraudulent payment themselves, it can have a more damaging psychological impact than more traditional types of fraud. Data from the Money and Mental Health Policy Institute show that a significant proportion of victims of fraud subsequently face mental health issues[6].

17. Research from bodies including the Royal United Services Institute has shown that the proceeds of fraud can be used to fund serious organised crime including terrorism, drug trafficking and child sexual exploitation - undermining the UK's standing as a safe place to live and to do business[7].

How fraud via advertising takes place

18. One of the most common ways of committing fraud is via paid-for advertising on search engines and social media platforms.

---

[2]https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2020/pdf

[3]https://press.which.co.uk/whichpressreleases/fraudsters-run-riot-as-search-engines-fail-to-adequately-protect-users-from-scams-which-reveals/

[4] https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime

[5]https://www.ukfinance.org.uk/press/press-releases/criminals-exploit-covid-19-pandemic-rise-scams-targeting-victims-online

[6] https://www.moneyandmentalhealth.org/wp-content/uploads/2020/12/Caught-in-the-web-full-report.pdf

[7] https://static.rusi.org/the_silent_threat_web_version.pdf

19. Criminals will clone a legitimate firm's website and run adverts in the name of that company purporting to offer customer support channels. The criminals will then pay the search engines significant sums of money to appear at the top of search results for the legitimate company. In this way, **platforms are not only facilitating fraud, they are profiting from it.**

20. When a customer clicks on one of the fake adverts they are taken to a highly sophisticated cloned version of the targeted company's website, which is identical in nearly every way apart from certain key details such as a customer support phone number being changed.

21. A customer will then call that number and be tricked by a criminal, employing sophisticated methods of social engineering, into transferring funds to a criminal's account.

22. Another common method of fraud facilitated by paid-for advertising is Account Takeover fraud. Similar to the customer support modus operandi, criminals will clone a legitimate firm's internet banking login page and run adverts in the name of that company.

23. Customers will then click on the advert and enter their login details. The criminals can then use these stolen details to access a customer's account directly and steal funds.

24. Alternatively, criminals will sell the login details to other criminals. Many of these stolen details, often referred to as 'fullz', are openly advertised for sale on the same online platforms[8].

Action taken by financial services companies to prevent fraud

25. Revolut recognises its responsibility to tackle fraud and protect our customers. We have invested significantly in technology, people and customer education in order to protect our customers from harm.

26. We would be happy to provide the Committee with more information on the specific measures we have taken to combat fraud, including our advanced machine learning models, pre-transfer warnings and customer communications strategies, on a confidential basis.

27. As the Committee will understand, Revolut does not want to put this detailed information in the public domain as it could help criminals to commit fraud.

Why legislation is necessary and urgent

28. Legislation is required to tackle fraud perpetrated through online advertising because non-legislative solutions have failed to address this significant, and growing, problem.

29. On top of our efforts to prevent fraud directly, Revolut and other financial services companies dedicate significant resources to reporting fake adverts to online platforms to have them removed. Unfortunately, platforms are generally slow to respond to these

[8] https://www.bbc.co.uk/news/uk-58223499

takedown requests and there are examples of **fake adverts remaining online for several days following takedown requests**.

30. Even if a platform responds to a specific takedown request, they do not normally take measures to tackle the root cause and prevent criminals from running the adverts in the first place. For example, after an advert is taken down the criminals can make a minor change to the text or targeting criteria of the advert and run it again.

31. If a criminal's advertising account is closed down then they can open a new one, design another fraudulent advert and launch it on the same major search engine targeting the same search terms in **under 150 seconds.**

Widespread support

32. There is considerable support for bringing paid-for advertising within scope of the Bill from the public and a diverse range of stakeholders including regulators, consumer groups, charities and industry.

33. Recent polling conducted by Censuswide found that 87% of people think the Government should legislate to ensure search engines and social media sites do not mislead consumers or promote financial scams. Additionally, 85% of people think search engines should be responsible for ensuring that advertising content on their platforms is not misleading[9].

34. Governor of the Bank of England Andrew Bailey wrote to the Treasury Committee earlier this year saying that "*[The] issue concerns online advertising of financial products and the scope for fraud... The online world is not subject to the same legal duties as the more traditional media. There is consequently no adequate shared responsibility with online service providers and consumers are at much greater risk. This could be tackled through the Online Harms Legislation, but the experience so far… is that there is strong resistance... to extending the legislation... This is a serious problem*"[10].

35. The Financial Conduct Authority's Chief Executive Nikhil Rathi told the Financial Times last month that "*We're very keen for… fraud ... to be included in that bill, in particular as it relates to online advertising. It will now be a matter for parliament and government to decide whether to pass the amendment that would enable this to happen. We think it would play a decisive role in helping us to protect consumers from online harm, and particularly those scams that target vulnerable consumers*"[11].

36. Which? Chief Executive Anabel Hoult has written that "*the tech giants are not doing enough to stop lives being devastated by fraud. We're demanding the government includes scams in the Online Safety Bill*"[12], while the founder of MoneySavingExpert.com

---

[9]https://www.aviva.com/newsroom/news-releases/2021/08/latest-aviva-fraud-report-calls-for-online-safety-bill-to-include-financial-scams/

[10]https://committees.parliament.uk/publications/5304/documents/52929/default/

[11]https://www.ftadviser.com/regulation/2021/08/04/fca-urges-govt-to-change-online-ads-position-over-scam-fears/

[12] https://conversation.which.co.uk/scams/online-safety-bill-open-letter-anabel-hoult/

Martin Lewis has said that "*the UK is facing an epidemic of scam adverts. Unless the [government] change their approach… millions of consumers will still be at risk of losing money and personal information through fake ads. We need to cut off scammers' ability to reach the public, and stop big-tech profiting from scams. We must put scam ads in the Online Safety Bill.*"[13]

37. Finally, in a letter to the DCMS and Home Secretaries, a coalition of 17 charities and law enforcement organisations said that "*We urge the Government to expand the scope of this vital legislation to include fake and fraudulent content that leads to scams. This would better protect people against the devastating financial and emotional harm caused by these crimes.*"[14]

Proposed amendment

38. Revolut recommends that Section 39 Clause 2 (f) is removed from the Bill, as set out below.

CHAPTER 6
INTERPRETATION OF PART 2

39 Meaning of "regulated content", "user-generated content" and "news publisher content"

(1) This section applies for the purposes of this Part.

(2) "Regulated content", in relation to a regulated user-to-user service, means user-generated content, except—

(a) emails,
(b) SMS messages,
(c) MMS messages,
(d) comments and reviews on provider content (see subsection (5)),
(e) one-to-one live aural communications (see subsection (6)),
~~(f) paid-for advertisements (see subsection (7)), and~~
(g) news publisher content (see subsection (8)).

Conclusion

39. Revolut thanks the Committee for considering this written submission and we would welcome the opportunity to provide further evidence to the Committee in due course.

40. The Online Safety Bill presents the UK with a unique opportunity to tackle fraud that is perpetuated through paid-for advertisements and significantly reduce the economic and social harm caused by this devastating crime.

41. Revolut looks forward to the successful passage of the legislation and continuing to work with the entire sector to protect our customers and provide them with the safest and most secure financial superapp.

---

[13] https://www.moneysavingexpert.com/news/2021/07/government-s-online-safety-bill-doomed-to-fail/
[14]https://conversation.which.co.uk/wp-content/uploads/2021/05/Open-Letter-Scams-and-the-Online-Safety-Bill.pdf