Written evidence submitted by TSB Bank

***TSB is a member of UK Finance and this submission is in addition to the submission made by UK Finance

Dear Mr Knight,

TSB Bank submission to DCMS Sub-committee Call for Evidence on Online Harms and Disinformation

I am writing on behalf of TSB Bank to highlight a key omission in the draft Online Safety Bill - action to tackle the harms caused by financial fraud and economic crime online.

As I have set out in detail below, online fraud is growing exponentially. It is causing significant harm to personal finances and mental health, with devastating consequences to people of all ages and backgrounds.

Fraud is the fastest growing crime in the UK and TSB remains the only bank to protect our customers with a refund guarantee for fraud and publish our reimbursement rates in full. However, more needs to be done not just in banking, but across telecoms, technology, and retail sectors to better protect customers and do more to catch criminals.

Since the onset of Covid, as more people shop and bank online, we see fraudsters increasingly using social media and the internet to commit fraud – making regulation of social media platforms essential to protecting people from becoming a victim of fraud.

The Government's decision to expand the scope of the Bill to include fraudulent user-generated content is welcome. However, it does not bring adverts or cloned websites within its scope. It also remains unclear exactly what types of user-generated fraud will be covered in practice. And specifically, for the victims of fraud, the Bill's provisions for harmful content should be expanded to include financial, as well as psychological and physical impacts.

We understand the Government is planning to tackle fraud facilitated by paid-for advertising through a separate Online Advertising Programme, led by DCMS. However, this work is yet to begin and will take a significant amount of time to complete. This approach creates unnecessary complexity and risks slowing down action to tackle crime. Including these measures in the Online Safety Bill represents a simpler and quicker route to addressing online-enabled fraud.

Yours sincerely,

George Gordon
TSB Bank

.

1. TSB's unique view of fraud

I. TSB is the only bank in the UK to offer its customers a Fraud Refund Guarantee (FRG) – which guarantees a full refund to all our customers if they fall victim to fraud. Introduced in April 2019, our FRG remains a revolutionary approach to supporting the victims of fraud. This means that TSB refunds 98% of fraud claims compared to the industry average of around 50%, according to the Payment Systems Regulator.[1] Indeed, the Payment Systems Regulator is now considering introducing a mandatory code with much higher consumer protections, similar to TSB's FRG.

II. When TSB introduced the FRG many opposed it, arguing that it would result in customers being more careless and that TSB customers would be more likely to be targeted by fraudsters. Neither of these predictions have proven true and many have changed their position and now support an industry-wide FRG.

III. While these predictions were proven to be inaccurate, TSB was surprised by one effect the FRG did have: because our customers know that we will not refuse a claim based on the information they share with us about how a fraud occurred, they are far more willing to be open and honest about the tactics and techniques used by fraudsters.

IV. This approach has led to a 1338% increase in intelligence disseminations to law enforcement. Since launching the FRG, TSB has received c.15,000 intelligence reports, including screenshots, from our customers – an exponential rise on pre-FRG levels.

V. Working with our customers means we can work with them to avoid them being targeted in the first place and to also use their experience to educate other customers who might be targeted.

VI. We share this with law enforcement, but we also analyse this information and use it to inform and educate our customers about specific types of scams and how they operate. Our customer intelligence reports have provided vital input into over 12,000 targeted fraud education emails which we tailor to a customer's risk type and send to them directly.

VII. Because TSB does not penalise customers for telling the truth about being the victim of fraud, we can confidently say we have a virtually unparalleled view of the methods and tactics used by fraudsters.

2. The harm caused by fraud

I. By virtue of this insight, we can also confidently say that the scale of online fraud, and the harm that it causes consumers and businesses, has reached a point where it cannot be ignored. The Crime Survey for England and Wales (CSEW) shows that there were an estimated 3.8 million incidents of fraud in the year ending March 2019, with evidence of a rising trend that is also seen in other data sources.[2] In the year to June 2020, Action Fraud received 822,276 reports of fraud. Action Fraud estimates 85% of these scams relied on the use of the internet in some way.

II. According to ONS data, there were 4.3 million incidents of fraud in the year ending June 2020, making fraud the most likely crime that adults can fall victim to in the UK. Action Fraud data shows that there was an increase of 413,000 reports of fraud over the past year, estimated to cost £1.7 billion: equivalent to every person in the UK losing £25 last year. Given cases of fraud often go unreported – with the National Crime Agency estimating that fewer than 20%of incidents of fraud are actually reported – this is likely to substantially underestimate the true scale of fraud that takes place in the UK.

III. However, quoting large figures about the impact on the overall economy misses a much more important point. Even losing relatively small sums can have a devastating impact on people's finances and wellbeing and the effects are felt unevenly.

---

[1] CP21/3 Authorised push payment scams – call for views | Payment Systems Regulator (psr.org.uk)
[2] Nature of fraud and computer misuse in England and Wales - Office for National Statistics (ons.gov.uk)

IV. ***Case study:*** In December 2020 TSB refunded a customer £530 after he was scammed when purchasing a PS5 console on Twitter, intended to be a Christmas present for his son. The customer said the Twitter user "had 70,000 followers – including verified Twitter users – 35,000 YouTube subscribers, and I saw him sell a couple of PlayStations the day before, so I thought – legit." However, the seller was a fraudster and the customer lost his money. Because the customer banked with TSB he received a full refund - but for many, a momentary lapse in judgement can cause significant financial hardship.

V. We believe new measures are essential to tackle the rising tide of fraud sweeping across the internet. In 2020 UK Finance members saw the value of scams reported to them by UK customers rise to over £1.26 billion, whilst banks and card companies prevented another £1.6 billion being lost through unauthorised fraud.[3]

VI. During the pandemic, we have seen opportunistic fraudsters taking advantage and using a number of new scams to target people at this already difficult time. In particular, fraudsters have capitalised on people spending more time online, using social engineering to prey on fears and uncertainties about the pandemic. The National Fraud Intelligence Bureau reported a 400% national increase in incidents of fraud at the start of the pandemic. Action Fraud has already received 11,500 reports of Covid-19 themed phishing scams, including scammers offering fake access to a Covid vaccine.

VII. At TSB the most common type of fraud our customers have been targeted by has been impersonation fraud. 43% of those who were scammed during the pandemic were targeted by criminals impersonating trusted organisations such as utility providers or preying on people's isolation with targeted romance scams.[4] We have also seen a rise in purchase scams and TSB has reported thousands of fake online profiles, scam adverts and links to online platforms as fraudsters set traps on popular social media platforms trying to trick customers into scam purchases.

VIII. The abuse of social media platforms by organised criminals for the purposes of financial crime has increased significantly over recent years. In 2019 almost half the scams we saw originated from social media. Our ongoing work with the Cifas, Action Fraud and the police has identified thousands of online accounts in operation by criminals at any one time and the majority are openly advertised and visible to users. These facilitate advertising for money mules (for the purposes of money laundering), selling stolen identity and credit-card data, phishing, impersonating legitimate companies (e.g. banks) to steal customer banking details and finance terrorism.

IX. Across the banking industry we are increasingly seeing criminals preying on people's financial insecurities during the pandemic with scams based on investments promising high returns. Criminals are now using sophisticated techniques to commit this form of fraud, primarily online. The City of London Police and Action Fraud have found that over £63m was lost nationally by victims of investment fraud targeted by criminals on social media. Investment scams, which are often promoted through paid-for adverts on search engines or social media, increased by 32 per cent in 2020 and while investment scams accounted for only six per cent of the total number of APP fraud, they accounted for 28 per cent of the total value of all APP fraud.[5]

X. Online fraud is increasingly common, and whilst it is welcome to see some action from platforms, such as Google's recent commitment to verify all financial services adverts with the FCA before they are published, all platforms still need to take greater responsibility for keeping their users safe.

3. Recommendations:

I. As set out by UK Finance, the Online Safety Bill should explicitly define fraudulent content as illegal content and amend the Bill to include a new schedule on fraud that specifies the types of fraud offences that will be captured by the Bill and this must include fraud committed through paid-for advertisements and cloned websites.

---

[3] https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2021

[4] https://www.tsb.co.uk/news-releases/tsb-reveals-insights-in-protecting-its-customers-through-a-year-of-pandemic-fraud/

[5] Criminals exploit Covid-19 pandemic with rise in scams targeting victims online | UK Finance

II. Harmful content provisions should be expanded to include financial impacts on individuals in any assessment of harmful content, alongside psychological and physical impacts on individuals which are already included in the draft Bill's harmful content provisions.

In addition, TSB is calling for more action from firms to:

I. **Vet advertisers to identify scams before they are able to advertise.** Many platforms are slow to remove the most objectionable content and there are currently too few checks before adverts go up. Many scams use very convincing fake websites, and it is not reasonable to expect the average person to maintain constant vigilance. More robust checks will help reduce the overall number of scams getting onto platforms in the first instance.

II. **Remove any online scam adverts and influencer scam endorsements before consumers are exposed to them.** Once scams are identified it is vital that action is taken quickly to minimise further consumer losses. Clear and well-defined minimum standards for responsiveness when removing scams will drive the right behaviours from organisations that currently operate on timescales that work for them - and not for consumers.

III. **Publish the data showing the time taken between a scam being reported and action being taken.** The overall lack of transparency currently makes it very hard to identify who is acting responsibly and who is not. Publishing of basic service and performance metrics is common within the banking sector and gives consumers the information on which to make informed choices. Knowing that a social media platform does not move to quickly remove scams would give consumers an additional way to identify whether something appearing on a given platform is trustworthy.

IV. **Social media and other internet advertising companies to share data with the banking sector.** These firms should share with banks the data on identified scams on their platforms in order that banks can better safeguard their customers and understand the scale of the issue.

Ends.