TSB – Written evidence (FDF0066)

Introduction to TSB and the Fraud Refund Guarantee

TSB offers the highest level of protection to victims of scams of any UK bank, through our Fraud Refund Guarantee (FRG). Since the FRG launched in April 2019 we have refunded 97% of fraud claims compared to an industry average of 42%.[1]

We believe that banks are best placed to directly protect their customers from the impact of fraud and that obligations to refund victims should be mandated across the financial services industry. We support the ongoing work of the Payment Systems Regulatory to implement such obligations but are mindful that final proposals have not yet been tabled.

Banks have a duty to protect their customers from fraud, however it is not a sole responsibility, and we need to recognise that the fraud landscape is comprised of a huge range of actors and industry and public bodies.

The UK's approach to fraud requires significant reform. The current landscape is fractured and is comprised of actors with competing interests. Few organisations accept responsibility for their role in allowing fraud to be perpetrated and there is no holistic view of fraud and its impact on society and the economy.

Fraud costs the UK £137 billion each year[2]. However, much of this cost ends up falling to the victims of fraud (consumers and businesses) and as such there is little incentive for these organisations to act.

TSB is calling for a new approach that prioritises prevention. The Crime Survey for England and Wales (CSEW) shows that there were an estimated 5.1 million incidents of fraud in the year ending September 2021, which represents a 36% increase compared with the year ending September 2019.[3] This level of fraud cannot be investigated or prosecuted. We must focus on ways to limit fraud occurring in the first place.

To do this we are arguing for a principles-based approach based on transparency, accountability, and responsibility.

Fraud Landscape

1. What fraud risks are UK a) individuals, b) the Government and c) businesses particularly vulnerable to today, and what are the reasons for this?

I. The Crime Survey for England and Wales (CSEW) shows that there were an estimated 5.1 million incidents of fraud in the year ending September 2021, which represents a 36% increase compared with the year ending September 2019.[1] It is not possible to precisely quantify the fraud risks facing these groups given how fraud is highly targeted. The individuals that are affected by a crypto scam are not the same group affected by a romance scam or impersonation scam.

---

1 https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2021#fraud

II. We urge caution, as a focus on specific types of fraud is unhelpful – fraudsters are always adapting and responding and any outline of the specific types of fraud affecting the UK will not have a long shelf life. Instead, it is more helpful to consider the commonalities that these types of fraud share in order to better understand the factors that enable fraud.

III. Most of the fraud affecting people and businesses today typically share the following things in common:

a. They are technologically enabled.

b. They are designed to use social engineering tactics to mitigate prevention.

c. They are tailored to specific groups.

d. They prey on a range of human characteristics: a trusting nature; being overconfident; fear; politeness; hope; and many others

e. They exploit wider societal norms (good and bad): online shopping; loneliness; poverty; deference to authority; fear of being the victim of fraud; a trust in technology; vulnerability; and the list goes on.

f. They involve multiple platforms across different sectors (technology, social media, telecommunications, banking etc).

g. The victim likely assumed it wouldn't happen to them.

h. Rather than be supported as a victim of crime, the victim will likely be blamed and judged.

i. The victim is unlikely to report the crime.

j. The perpetrator is unlikely to ever be caught.

2. What future economic and technological developments are likely to impact how fraudsters seek to commit crime over the next five to ten years, and how might these be prepared for and mitigated? What role can technology and tech companies play in combatting fraud across this timescale?

I. Our approach to fraud should not be predicated on having correctly guessed the direction of travel of technology and innovation. It is not possible to predict this given the scale of change and the creativity of fraudsters. Any attempt to legislate based on predictions for the future will invariably miss the mark.

II. Crypto is clearly an emerging challenge and regulators are having to move quickly to catch up with the changes seen over the last few years. TSB has a number of recommendations regarding crypto in the annex of this submission.

III. Even if we were to correctly guess and regulate future threats the reality would be that fraudsters would identify loopholes to exploit.

IV. Instead, we must have in place an approach that is principles based and that focuses on outcomes and behaviours rather than technologies and use cases.

V. Recent years have seen a huge rise in the incidence of "authorised" fraud where the victim themselves sends the funds to the criminal. This differs from other fraud types ("unauthorised") where the criminals gains access to a victim account (usually as a result of compromised security credentials) and moves funds without the consent of the victim. A hybrid type of fraud has also developed where the fraudster initiates a payment and then socially engineers the victim to inadvertently authorise it on a false pretence.

VI. The major driver for this growth in authorised fraud has been investment by banks and other firms to reduce the incidence of unauthorised fraud through ever more robust controls. Fraudsters have responded to this by targeting the new weak link in the chain which is often the customer themselves. It is reasonable to believe that this trend will continue as banks invest further in security controls to reduce unauthorised fraud.

VII. It is noted that victims of authorised fraud currently have no statutory right to any reimbursement and therefore this trend is likely to, over time, only worsen the level of protection offered to consumers.

VIII. That is why TSB is arguing for a system build on: transparency; accountability; responsibility. The technology firms, social media companies, telecoms and any other sectors which emerge in the future must be transparent with their users about the risks on their platforms/technology. They must be held responsible for taking proactive steps to limit fraud and make it harder for fraudsters to use their platforms. And they must be held accountable when fraud occurs.

IX. A principles-based approach, with strong oversight and robust enforcement and penalties, is highly effective and is commonplace for financial services firms. The FCA is currently developing "the new consumer duty" and has the aim of ensuring firms "ensure that their products and services are fit for purpose and offer fair value, and that their communications and customer service enable consumers to make and act on well-informed decisions." Forcing fraud-enabling companies to be proactive and work to a set of principles to combat fraud will ensure that future threats can be mitigated quickly and effectively and at limited cost to the taxpayer.

X. The Online Safety Bill is evidence of how difficult and time-consuming it is to update legislation to mitigate new risks.

XI. TSB jointly funds, with industry, a specialist police unit - the Dedicated Card and Payment Crime Unit (DCPCU). We are also members of Stop Scams UK - a collaboration between banks, telcos and a small subset of technology firms. There is no legislation requiring us to do this, however the financial services sector has the right commercial and regulatory incentives to drive this kind of voluntary action.

3. Is fraud and its victims treated as a priority? If not, what are the reasons for this. The Committee is particularly interested in responses that can explain any barriers preventing effective counter-fraud cooperation within Government, law enforcement, the public sector and the private sector.

I. Fraud is complex and the current fraud policy and regulatory landscape has evolved over time. It is complex and disparate. Consider that fraud reimbursement is covered by banks, a voluntary code and the Payment Systems Regulator, while a lot of fraud is driven by social media and tech firms which are being regulated by DCMS and Ofcom. Fake investment adverts are also covered by the FCA. Law enforcement, on the other hand, sits with the Home Office, the City of London Police, Police and Crime Commissioners and local police as well as the National Crime Agency and other bodies. This is understandable but it is complex and makes cooperation very difficult. Different departments have different objectives, priorities and stakeholders and there is no single organisation that has a holistic view of the whole landscape.

II. As such, TSB believes we need a single point of accountability: a Minister for Fraud. This Minister should have oversight across departments to join-up the different and competing elements that are the current fraud landscape.

III. Currently it is difficult to see any organisation or individual who can adequately consider the costs and benefits of a given response to fraud. To take social media as an example – the costs of the fraud social media firms enable falls to Banks and fraud victims but the costs of reducing fraudulent activity on social media would fall to social media firms.

IV. Another crucial element that creates barriers to cooperation is that there is little incentive to do so. Because the current framework for refunding fraud victims means that banks can reject claims when they deem a customer to have been to blame for the fraud, they have an incentive to investigate their customer.

V. This creates little incentive to tackle the causes of fraud and instead incentivises the avoidance of fraud costs. TSB, through its FRG, does not have this problem. While we feel it is ultimately the responsibility of banks to refund their customers, we do not feel it is banks who should bear the sole cost of fraud – given that banks are doing more than any other sector and that many other sectors enable fraud.

VI. Banks currently have no obligation to refund victims of authorised payment fraud. Most major banks have signed up to the Contingent Reimbursement Model which covers victim refunds, but this remains voluntary, and many financial firms (often new entrants and "fintechs") have not adopted this code. That said, this will not likely remain the case due to plans by the PSR to mandate reimbursement in most instances. Social media firms, tech firms and telcos have almost no financial or regulatory incentive to prevent fraud. While this remains the case these firms will have no reason to cooperate or to take the issue seriously. Even the Online Safety Bill, whilst creating new offences relating to harmful content, will not currently require any steps to be taken for in-scope platforms to refund any fraud victims. Our current understanding is that any fines levied under this act (as and when they are issued) will be absorbed by HM Treasury.

VII. A quick search of Instagram for the term "cash flip" will return hundreds of accounts targeting people with this scam. Action Fraud highlighted this issue in 2020[2] yet hundreds of accounts remain.

VIII. We reviewed our data on investment fraud claims and found that Instagram is by far the worst platform. 70% of cases of investment fraud reported to TSB (where a platform was recorded) between January and March 2022 started on Facebook or Instagram, either through adverts or victims being directly messaged on the platforms. In July 2021 Google made up 20% of investment fraud cases. However, Google took proactive steps to tackle the problem (driven by FCA intervention) and since then, TSB has not seen any investment fraud cases originating from this platform, while other platforms have maintained their fraud rates.

Action to Tackle Fraud

5. How effective is the current structure for policing fraud? How successful are the City of London Police, including Action Fraud and the National Fraud Intelligence Bureau, at executing their role as the lead police force for fraud?

I. Victims of fraud frequently express frustration with the response from Action Fraud, although we believe that this is largely down to the service being badly named. Not unreasonably, after reporting a case to Action Fraud, victims expect some action to be taken. However, it is a fraud reporting service and responsibility for responding to each report sits elsewhere. We would recommend that the service would benefit from reform including a new name and a clearer articulation to victims of the service they can expect to receive.

II. More generally, the response of law enforcement to cases of fraud in the UK barely scratches the surface of the problem. Individual police forces are working hard to tackle fraud but lack the resources to properly investigate the crime given its scale. This is not helped by the fact that the crime tends to occur across regional and national borders. The national response is then spread across multiple bodies including the Metropolitan Police, City of London Police, the National Crime Agency and others. Notwithstanding the efforts of all of these bodies, their success rate in disrupting criminals is evidenced by the very low rate of convictions vs the incidence of the crime. This is only likely to improve with much greater resources being allocated to tackling the problem as opposed to simply reallocating responsibilities.

6. Are sufficient resources available to Government organisations (such as the Serious Fraud Office and Crown Prosecution Service) and wider police forces to tackle fraud and support victims, and how should this be addressed if not? Answers need not be limited to financial resources.

I. Given the scale of fraud, and that many fraudsters operate abroad, the ability of the problem to be addressed by law-enforcement is limited. That said more resources are needed to ensure that fraud victims are more likely to see justice.

II. Due to the scale of fraud and limited resources many low-value frauds are rarely investigated. Fraudsters know this and many operate with virtual

[2] 164 Instagram users report losing over £350,000 to investment scams | Action Fraud

impunity by exploiting this approach. 51% of the claims we see at TSB are for sums below £500. However, while £500 may be a relatively small sum to some people it can have devastating consequences for others. TSB's research found that around one-third of the UK public would be unable to pay their rent or mortgage or afford food if they lost just £500. A similar amount reported that it would have negative mental health effects. With the current cost-of-living crisis affecting the UK, the impact of being a victim of fraud will only worsen.

III. There is no conceivable way the UK could investigate and prosecute every fraud in the UK, and this is why it is important to make it much harder for fraudsters to operate.

IV. The support for fraud victims is patchy. It is also important to recognise that due to the culture of blaming victims many fraud victims do not report the crime meaning they receive no formal support.

V. As well as investing in our own systems to prevent fraud occurring in the first place, we joint fund, with industry, a specialist police unit - the Dedicated Card and Payment Crime Unit (DCPCU). We are also members of Stop Scams UK - a collaboration between banks, telcos and a small subset of technology firms.

7. What are the responsibilities of the private sector in protecting the public against digital fraud? How can a balance be achieved between the need to tackle digital fraud whilst supporting the growth of these sectors? To what extent is work done to combat fraud across the private sectors undermined by siloed or independent working practices?

I. The private sector has a responsibility to protect its customers against the threat of fraud. Banking customers especially should be confident in the knowledge that their earnings and investments are safe from being lost to fraudulent activity.

II. Most importantly, it is the responsibility of the private sector to view victims of fraud as victims of a crime, and not hold them responsible for the actions of criminals. A key reason why TSB has declined to join the Contingent Reimbursement Model (CRM) Code to date is that it is built on the principle that fraud victims are sometimes to blame. Such an approach creates a sense of shame and means many victims of fraud do not come forward to friends or family, let alone the authorities or their bank. That said, many banks have made no public commitments at all about victim reimbursement.

III. However, the private sector – in its broadest sense - is not working to these ends. Banks invest large sums into protecting their customers from fraud. TSB goes further in offering a Fraud Refund Guarantee which provides our customers with much better protection from financial harm if they are the victim of fraud. However, a huge amount of the fraud that we see is driven by sectors outside of banking. These firms have little commercial incentive to address the fraud they enable. Some actually have a financial incentive to overlook fraud as they profit from fraud – e.g. paid for scam adverts.

IV. TSB wants to see social media firms, telcos and other tech firms share data on fraud with banks and work to proactively identify and remove fraudsters from their platforms and services. We believe that the simplest way to do this is to allow banks to claim back the costs of refunding fraud victims from the platforms and services that enabled the fraud to happen. The polluter pays principle is well established and an effective policy tool to drive accountability and we believe if fraud becomes a cost for businesses, then they will be incentivised to act.

8. What are the legislative or regulatory impediments to sharing fraud risk data across and between the private and public sectors? For example, to what extent does General Data Protection Regulation (GDPR) limit data sharing?

I. There are several sectors where payments are being made at large by the population to a limited number of accounts, for example to pay taxes to HMRC or to registered conveyancers for house moves, or to regulated investment companies. If these account details were shared with banks by the receivers, it would enable banks at a simple glance to be able to rule out many payments being made to fraudulent accounts. This is a simple idea with the potential to be highly effective. Yet despite it being under discussion for a long time, these examples have yet to agree to share a complete set of such 'safe lists'.

II. Sharing additional data relating to consumer payments could also enhance the ability of banks to prevent fraud. Some progress is being made here, with payment technology companies now offering services which can risk assess receiving bank accounts and share data on this risk assessment with the bank making the payment, in real time. It is expected that this technology will be deployed across the banking industry in 2022. However, there remains no simple way for banks to share greater information on the remitter of a payment and GDPR considerations remain a key barrier for this type of approach to be adopted.

9. What is the role of the individual in relation to fraud? Are consumers well informed about the risks of fraud and how to prevent them? If not, which bodies or organisations should do more to ensure this? What are the most effective methods of educating the public about fraud crime and prevention?

I. Personal responsibility is important and there are instances where an individual's actions must be taken into account. For example, if someone wishes to transfer their money to an unregulated crypto exchange. But the instances where an individual's responsibility is greater than the companies, regulators, and platforms that they trust is rare.

II. Banks do a significant amount to inform customers of the risks of fraud and to educate them on the ways fraudsters target people.

III. This is important work and TSB does a huge amount to inform and educate its customers. Our Fraud Refund Guarantee means we reimburse our customers when they are the victim of fraud and that means we bear much of the cost of the fraud losses of our customers. This means that

TSB has more incentive than any other bank to educate its customers about fraud.

IV. However, we also recognise that given the scale of fraud in the UK and the sophistication of many scams, the technologies that are used, and the complex social engineering tactics used it is not credible to suggest that educating people about fraud is particularly effective.

V. We must also recognise that fraud is always evolving. Fraudsters will always find ways to explain away a customer's concern. It is also important to recognise it is not possible, or reasonable to expect, people to maintain an advanced level of knowledge about the current *modus operandi* of every type of fraud that they may fall victim to.

VI. Fraud is one of the only crimes in the UK where it is acceptable to immediately question the degree to which the victim is responsible for having been the victim. This means fraud victims are often met with less sympathy, support and understanding than the victims of other crimes. It also creates a false distinction in the minds of the public. People hear stories of fraud and, with the benefit of hindsight, immediately think that the victim was stupid or carless. This drives a view that fraud happens to other people and leads to people having a false sense of their own competence. The focus on personal culpability also means people feel ashamed and embarrassed when they are the victim of fraud. Some people do not tell their friends or family and instead suffer alone.

VII. The idea of personal responsibility is important, but it should not be used as an excuse for public and private bodies to ignore their responsibilities.

VIII. A simple question is helpful to crystalise the issue and the absurdity of our current view of fraud and personal responsibility:

> *Is it simpler to educate and inform every person in the UK about every type of scam happening on social media platforms and expect them to maintain constant vigilance against these scams, and then re-educate and inform them of new scams as they emerge; Or would it be simpler for social media firms, some of the largest and most technologically advanced companies in the world, to prevent fraudsters operating on their platforms?*

Legislative Remedies

10. What is your assessment of the Fraud Act 2006? What has been the impact of the Act and is it having any unintended consequences; if so, what are these?

I. The Fraud Act 2006 focuses on the fraudsters themselves. This is problematic as for it to be a deterrent the fraudster would need to be in the UK and would also need to believe there was a realistic chance of getting caught.

II. A better approach both in terms of ease of enforcement and effectiveness would be to consider ways to regulate the companies on which fraudsters rely on to carry out their fraud.

III. For example, while the Fraud Act 2006 covers participation in a fraudulent business it does not cover a business ignoring, enabling or facilitating the use of its technology or platform to systematically target people for the purposes of fraud.

11. Is existing legislation effective in tackling the increase in modern forms of fraud? If not, is there a legislative remedy, or should fraud be addressed primarily through implementation of existing provisions? Answers may refer to existing mechanisms such as increasing the scope and powers of regulators. You may refer to any legislation and are not limited to the Fraud Act 2006.

I. Existing legislation is not effective in tackling fraud. That is why there were over 5 million cases of fraud in England and Wales alone last year. It is the most commonly experience crime in the UK and the costs are enormous.

II. Tech firms and social media companies have huge power and resources but are regulated as if they did not. The financial services industry is heavily regulated by bodies with enormous power to enforce and penalise banks and rightly so. However, the largest social media firms and tech companies (who are some of the largest companies in the world) are regulated as if they have no power or responsibility to their users.

III. TSB believes that as commercial organisations the best way to get these companies to act is to make the cost of inaction higher than the cost of action.

IV. TSB believes it is right, and in the best interest of the customer, that their bank is the point of contact to request a refund for the cost of fraud. However, we would like to see a mechanism whereby banks are then able to seek a refund from the company that enabled the fraud to happen.

V. This approach would ensure that the costs of fraud are distributed to the entities that are able to take steps to prevent fraud. If social media firms, for example, began to see the cost of fraud in the UK costing them hundreds of millions or billions of pounds then we are confident that there would be little need to regulate that they take fraud seriously.

12. Is the current system in place for prosecuting fraud cases working effectively? If not, what are the key barriers to prosecution?

I. Many fraudsters aren't in the UK.

II. With 5 million frauds last year there is no conceivable way that the UK could ever investigate or prosecute a meaningful proportion of these.

III. Because of limited resources priority is given to larger sums meaning poorer people are less likely to see justice.

IV. Prosecution of fraudsters can only occur once a fraud has happened – meaning there is already a victim and the harm has been done.

V. Investigations are complex and take a long time.

13. Are sanctions and penalties for criminals who commit fraud an effective deterrent against future criminal activity, and if not, what might be more successful? Respondents may choose to refer to penalties imposed by the judicial system or by specific sectors.

I. The scale of fraud affecting the UK is evidence that sanctions and penalties are not effective.

II. Even if the UK had life sentences for fraud the chances of getting caught and convicted are basically zero. When you consider a lot of fraud is carried out by organised criminals with global networks, it is clear that a strategy that focuses on penalties as a deterrent will never be particularly effective.

III. These criminals rely on a few technologies owned by even fewer companies to operate. Closing down routes to potential victims would have the most meaningful impact on fraud levels in the UK and could protect thousands of people every year from becoming a fraud victim. Fraud is occurring at its current levels because it is so easy and cheap to target people. Criminals respond to economics as much as businesses do and if the cost of stealing £1 is higher than 99p then they will look elsewhere. The way to increase these costs is to make it more time consuming to target victims, to make it more likely they will have less time to target their victims and to make it more likely they will be blocked from services before they target their victims.

Best Practice

14. What lessons can be learned from effective policy interventions and schemes both in the UK and overseas?

I. TSB has demonstrated best practice. By bearing the true costs of the fraud experienced by our customers we have created a mechanism whereby the only way we can reduce costs is to prevent fraud occurring.

15. Can you suggest one policy recommendation that the Committee should make to the Government?

I. First and foremost, Payment Service Providers (PSP) should reimburse fraud victims. The true harm being done by fraud is at the level of the individual and triaging this issue means fraud victims must be protected from the financial harm caused by fraud. We stress that this must apply for every PSP – if a PSPs is unable to adequately protect their customer from the financial harm of fraud they should not be allowed to operate. The PSR is working toward this outcome.

II. Thereafter the most impactful reform that could be made would be to create a cost sharing mechanism whereby banks could seek to recover the costs of reimbursement of fraud victims from the platforms which enabled their customers to be targeted.

<u>Annex: Recommendations</u>

We have outlined a number of reforms that we believe would also be effective in addressing systemic failings within the fraud ecosystem. Again, these are built on three simple but powerful principles:

- **Make those able to prevent fraud responsible when it occurs.**
- **Drive better and more consistent accountability across businesses and government.**
- **Inform consumer choice through greater transparency of fraud and refund rates.**

Make those able to prevent fraud responsible when it occurs

- Require all Payment Service Providers (PSPs) to refund innocent fraud victims – recognising the role and responsibility PSPs have in protecting their customers.
- After mandating reimbursement from PSPs, government and regulators must create a financial redress mechanism for PSPs to seek costs (partial or total) from sectors which have enabled fraud.
- Drive forward a cultural shift in institutions, public and private, as well as society more generally that treats fraud victims as victims and does not blame them.
- Encourage victim reporting and significantly improve the consistency of support for fraud victims.
- In reducing fraud, consider the benefits of introducing more friction into the payment system to enable banks and customers more time to identify and respond to fraud. This may involve amendments to the Payment Services Regulations and other regulation.

Drive better and more consistent accountability across businesses and government.

- Create a requirement on all large businesses (telecoms firms, social media firms, technology companies etc) to measure the volume and value of fraud that occurs on their platforms and report it annually, display it prominently and share real time information with PSPs and regulators.
- Require sectors such as crypto exchanges, where security and know your customer (KYC) has typically been poor, to tighten up their standards and to accept responsibility for reimbursing users suffering fraud on their accounts.
- Require co-ordinated action between the cryptocurrency industry, social media firms and the Financial Conduct Authority (FCA) to crack down on fake "crypto" investments.
- Establish a cabinet level and cross-departmental minister for fraud with oversight and power over the entire fraud landscape.
- Ensure that the Online Safety Bill does not create inconsistent regulatory and legal approaches to fraudulent adverts due to the platform they appear on. Currently adverts which appear through search engines will be treated differently to those on social media.
- Pursue a robust approach to online advertising through the Online Advertising Programme – which places significant and meaningful requirements on firms to limit fraudulent adverts and which imposes severe consequences on those who fail to comply.

Inform consumer choice through greater transparency of fraud and refund rates.

- Require all PSPs to report their fraud refund rate based on agreed industry criteria and display them prominently (physically and digitally).
- Require reimbursement rates to be published on PSP apps and not just on PSP websites – recognising that many people rarely use internet banking and instead use mobile apps.
- Require non-banking sectors to publish data on fraud and to display it to their users/customers.

4 May 2022