

## Fraud Advisory Panel – Written evidence (FDF0048)

The Fraud Advisory Panel welcomes the opportunity to comment on the House of Lords Committee on the Fraud Act 2006 and Digital Fraud's call for evidence, published on 08 March 2022, a copy of which is available from this [link](#).

The Fraud Advisory Panel (the 'Panel') is the UK's leading counter fraud charity. We act as the collective voice of the counter fraud profession and provide practical support to more than 200 corporate and individual members. Our members come from a wide range of professions and sectors who are united in their determination to stop fraud.

Our trustee and director, Mr Arun Chauhan, gave oral evidence to the Committee on Thursday 03 March. His evidence is not repeated herein. Instead, we've highlighted other issues we believe merit consideration by the Committee.

We're happy to discuss any of our comments and to take part in all further inquiries on the issues we've highlighted to the House of Lords Committee.

### FRAUD LANDSCAPE

#### Question 1:

What fraud risks are UK individuals, the Government and businesses particularly vulnerable to today, and what are the reasons for this?

1. The fraud risks to UK individuals, the Government and businesses are well-documented and well-publicised so it is not our intention to repeat them here<sup>1</sup>, suffice to say that the amount of reported fraud continues to grow and now accounts for almost half of all crime in England and Wales.
2. The reluctance of the successive governments to invest adequately in counter fraud activity means that the risk of detection, investigation, and prosecution is so low that fraud has become an attractive and lucrative career choice for many criminals.

---

<sup>1</sup> See for example Office for National Statistics (27 January 2022). *Crime in England and Wales: year ending September 2021*, available from:

<https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2021#fraud>; PwC (2022). *PwC's Global Economic Crime and Fraud Survey 2022*, available from <https://www.pwc.com/gx/en/forensics/gecsm-2022/PwC-Global-Economic-Crime-and-Fraud-Survey-2022.pdf>; Cabinet Office (February 2020). *Cross-Government Fraud Landscape Annual Report 2019*, available from [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/864268/Cross-Government\\_Fraud\\_Landscape\\_Annual\\_Report\\_2019\\_WA\\_\\_1\\_.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/864268/Cross-Government_Fraud_Landscape_Annual_Report_2019_WA__1_.pdf); UK Finance (2021). *Fraud – The Facts 2021*, available from: <https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf>; National Crime Agency (2021). *National Strategic Threat Assessment of Serious and Organised Crime*, available from: <https://www.nationalcrimeagency.gov.uk/news/online-is-the-new-frontline-in-fight-against-organised-crime-says-national-crime-agency-on-publication-of-annual-threat-assessment>; KPMG (February 2022). *Fraud Barometer 2021* available from: <https://assets.kpmg/content/dam/kpmg/uk/pdf/2022/02/fraud-barometer-2022.pdf>; BDO UK *Fraudtrack 2022* available here: <https://www.bdo.co.uk/en-gb/fraud-track>

**Question 2:**

What future economic crime and technology 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 combating fraud across this timescale?

3. Our ability to predict future risks and respond quickly to these by introducing appropriate safeguards early on to protect consumers and business is fundamental to our fight against fraud. This requires the sharing of knowledge and expertise between government and other sectors as is done for critical national infrastructure.
4. More proactive thought needs to be given to the way we live, work and interact with one another now and how this is likely to change in the future. We must consider what new and emerging technologies are underpinning these changes and how they might give rise to fraud.<sup>2</sup> This includes advances in machine learning and artificial intelligence (including deep fakes), biometrics, robotics, the blockchain, cryptocurrencies, miniaturisation, big data, and the virtual world (the 'metaverse').
5. We need to encourage all businesses, particularly tech companies, to think more proactively about the potential dark sides to their innovations, to design fraud out from their products and services before they come to market, and to do more to educate their customers on how to protect themselves from fraud. We also need tech companies to take greater responsibility when they do not by using more effective regulation, supervision and enforcement.

**Question 3:**

Is fraud and its victims treated as a priority. If not, what are the reasons for this?

6. Fraud is not a priority, nor are its victims. Fraud is under-resourced, under-investigated and under-prosecuted.
7. To date the focus on economic crime has been on tackling money laundering (of which fraud is a growing predicate offence). Such an approach fails to recognise that fraud and money laundering are essentially different sides to the same economic crime coin. The Economic Crime Plan 2019 to 2022 contains just seven actions related to fraud (out of a possible 52); four of which are now overdue.<sup>3</sup>

---

<sup>2</sup> Fraud Advisory Panel (2018), *Fraud Futures: Understanding the old to prepare for the new*, available from: <https://359zpa2vui8h3p4u7j2qlmlg-wpengine.netdna-ssl.com/wp-content/uploads/2018/06/Fraud-Futures-WEB-July-2018.pdf>

<sup>3</sup> RUSI Economic Crime Plan Online Tracker, available from <https://rusi.org/ecp> [accessed on 13/04/22]

8. Consumer frauds are often referred to as 'scams'. This term trivialises the crime and its harmful effects on victims. We need to rethink vulnerability (anyone can be vulnerable at different times of their lives) and address gaps in the aftercare and support available to victims.
9. We welcome signs that government is now beginning to take the issue of fraud more seriously with its proposed 10-year fraud strategy. However, this must be supported by meaningful and timely resources. We'd like to see more urgency, more attention, and more resources given to addressing the problem.

**Question 4:**

What is the role of international actors in the UK's fraud landscape? What are the barriers to tackling borderless fraud?

10. Fraud often involves criminals (including organised crime groups) operating from overseas 'hard-to-reach' jurisdictions, where cooperation with local law enforcement is ineffective or impossible. Therefore, more emphasis needs to be placed on reducing the opportunities for fraudsters to target UK-based victims by strengthening the safeguards within the mechanisms they regularly use to facilitate their crimes (e.g. through the internet, computer hacking, mobile applications and through bank payment mechanisms).

## **ACTION TO TACKLE FRAUD**

### **Question 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?

11. Our police forces are constrained by national police boundaries. Fraudsters are not. This makes the effective policing of fraud difficult (if not impossible). The inadequacy of existing resources (both people and money) compounds this.

### **Question 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?

12. No. The criminal justice system – and fraud policing, investigation and prosecution more specifically – have been systematically under-funded and under-resourced for years. There has been a deeply rooted reluctance to properly fund national counter fraud activity which has resulted in our current inability to take meaningful action to stem the growing tide of fraud. This is part of the reason why fraud now accounts for more than 40% of all crime.
13. It is well-evidenced that very few fraud reports result in a criminal investigation and even fewer in a judicial outcome. This is no deterrent. For the consumer who has lost their life savings to fraud, or the business owner who has laid off staff or even closed, or the charity that has closed its doors because it can no longer support those in need – this is simply not good enough.
14. Much counter fraud activity is still undertaken in silos without sight of the bigger picture and is focused on 'high harm' frauds. We are concerned that this means that resources devoted to fraud in the criminal justice system will be focused on certain types of fraud at the expense of others, leaving victims of other types of fraud without a realistic prospect of access to justice, and leaving substantial gaps which fraudsters will seek to exploit.

### **Question 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

siloes or independent working practices?

15. Online fraud cannot continue unchecked. Online companies must step up and play their part in tackling online fraud. Prior to the Online Harms Bill – and mounting pressure from consumer and counter fraud bodies such as ours – there was very little incentive for them to do so.
16. We need to encourage businesses to do the right thing and design fraud out from their products and services before they bring them to market or face the risk of regulatory and enforcement action. Voluntary codes are not enough and do not work in a consistent or effective manner.

**Question 8:**

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

17. Both law enforcement and the private sector are concerned that they may fall foul of the GDPR when considering whether or not they can share data on specific fraudsters, and even on fraud risks. The GDPR legislation is complex and confusing, and as such the easiest position for law enforcement or the private sector is simply not to take the risk of breaching the law, and not to share any data.
18. The Government should provide more guidance on when and what sort of data can be shared and encourage lawful data sharing. To the extent that the law provides a genuine barrier to data sharing, then legislative carve outs should be created in order to facilitate the exchange of data.

**Question 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?

19. Over the past few years there has been a steadily increasing number of consumer-focused fraud campaigns. But ever-increasing numbers of consumers still fall victim.
20. There is widespread consensus that prevention must be the focus of our future endeavours both because prevention is always better than cure and because of the inability of the state to investigate and prosecute most fraud reports. Prevention relies on good collaboration, information sharing and

sustained effort as well as a recognition that to build society-wide awareness and resilience takes time, money and resources.

21. We have long advocated the need for a well-funded and sustained public education campaign to inform consumers about how to protect themselves. The Take Five campaign is a good start, but a government-led national campaign would be more effective in making more people take heed. We look forward to seeing what the National Economic Crime Command does in this respect.
22. Public education needs to start as early as possible. Fraud and cyber education should be mandatory within the national curriculum for all school children with the Department for Education actively involved in such discussions.

## **LEGISLATIVE REMEDIES**

### **Question 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?

23. The Fraud Act 2006 is a good piece of legislation. It is simply under-used because the likelihood of perpetrators being identified and investigated is so low. There are no apparent unintended consequences from the legislation. It should also be noted that the legislation runs in parallel with the charge of conspiracy to defraud.

### **Question 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?

24. Generally, we believe that existing legislation could be effective in tackling modern fraud. The problem is not one of inadequate legislation, but of woefully inadequate resources to investigate and prosecute allegations of fraud effectively.

### **Question 12:**

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

25. The criminal justice system is underfunded and overloaded. It has been well-publicised that the current backlog of cases in the Crown Court is threatening to overwhelm the system. Yet by their very nature, fraud trials are often long, complex and costly. As such prosecutions are infrequently brought, and when they are brought, they are subject to lengthy delays, and often fail for a number of reasons.
26. One area that could potentially benefit from reform is the disclosure regime, in order to simplify the procedure for handing material to the defence. This may assist to ensure that cases do not collapse because of disclosure failures.
27. Another area for potential reform or for increased focus, is the use of incentives for whistle-blowers in fraud cases or for the use of immunities from prosecution for those willing to give evidence against their co-conspirators. Such proactive tools have been used to great effect in the sphere of general crime and in the US in particular, where the Dodd Frank legislation enables whistle-blowers to receive between 10-30% of assets recovered at the end of a successful trial if they provide original information leading to a conviction.
28. Finally, greater use could then be made of out-of-court settlements or plea negotiations for those defendants or offenders who – when they self-report – or when they are implicated – admit their involvement, cooperate and take steps to remediate their wrongdoing, for example as seen in the NatWest prosecution for breaches of the AML Regulations 2007.

**Question 13:**

Are the sanctions and penalties for criminals who commit fraud an effective deterrent against future criminal activity, and if not, what might be more successful?

29. Existing sanctions and penalties for fraud would be more effective if they were applied often enough to deter fraudsters. There is no evidence we are aware of to suggest the potential sentences are too weak to deter economic crime activity.
30. Punishment when caught is a deterrent, as is the fear of being caught in the first place. As such much greater incentives should be provided to whistle-blowers to come forward, in order that more cases can be brought to light, investigated and ultimately, successfully prosecuted.

**BEST PRACTICE**

**Question 14:**

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

31. See above comments as to whistle-blower incentives and the use of immunities from prosecution in the US. As well as the comments in relation to credit being given for self-reporting cooperation and remediation.

**Question 15:**

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

32. Until there are adequate counter fraud resources available to law enforcement and the criminal justice system, we are unlikely to see any reduction in fraud. Indeed, on present projections the numbers of fraud are likely to continue to rise. So, we would welcome the Committee recommending the provision of additional resources to fight fraud.

*22 April 2022*