Association of British Insurers – Written evidence (FDF0051)

About the Association of British Insurers

The Association of British Insurers is the voice of the UK's world-leading insurance and long-term savings industry. A productive and inclusive sector, our industry supports towns and cities across Britain in building back a balanced and innovative economy, employing over 310,000 individuals in high-skilled, lifelong careers, two-thirds of which are outside of London.

Our members manage investments of nearly £1.7 trillion, collect and pay over £16 billion in taxes to the Government and support communities across the UK by enabling trade, risk-taking, investment and innovation.

We are also a global success story, the largest in Europe and the fourth largest in the world.

The ABI represents over 200 member companies, including most household names and specialist providers, giving peace of mind to customers across the UK.

Executive Summary

1. **Fraud continues to be the most prominent threat facing the UK. Online scams have become prominent over recent years, with existing laws failing to keep pace with online criminals. We are pleased that the Government has listened to the many different sectors and organisations, including the ABI, which called for online paid-for scam ads to be brought within scope of the Online Safety Bill. We will, however, scrutinise the Bill closely to ensure that no gaps are left for scammers to exploit.**

2. **While it is difficult to predict what the UK economy will look like over the next five to ten years, history shows that during times of financial hardship, fraud tends to increase. While counter fraud professionals use technology to combat fraud, fraudsters exploit technology to commit fraud.**

3. **We do not believe that fraud is suitably prioritised. Despite being the most prevalent crime committed against individuals, only 1-2% of police resource is allocated to tackling fraud. More could be done to deter fraud and we would welcome a review of the Sentencing Guidelines, as well as consideration of new ways to restrict the freedom of those committing fraud.**

4. International actors have a key role to play in understanding the exposure to international crime within the UK fraud landscape, in improving the prevention, investigation and prosecution of cyber-enabled fraud, in building capacity in law enforcement in the judiciary, and in working with businesses to raise awareness of the cyber threat and enable consumers to take action to protect themselves.

5. It is imperative that the next [third] iteration of the National Fraud and Cyber Reporting Centre ('Action Fraud'), which is due to go live on 31 May 2024, is fit for purpose, with referrers being kept apprised of case progress. Version 1 was manual and cumbersome, and Version 2 failed to provide the desired functionality.

6. **We wholeheartedly support the recent DCMS confirmation that the scope of the Online Safety Bill will be extended to cover paid-for advertisements and that 'fraud and financial crime' offences will be designated as a 'priority offence'. However, the Bill will not reach the statute book for some time.** During the interim, the tech platforms must up their game and we would welcome the introduction of a Tech Sector Fraud Charter, overseen by the Joint Fraud Taskforce.

7. Overall, insurers' experience of the Fraud Act has been positive. However, we do believe that the Act is currently under-utilised due to the challenges around delays in judicial processes.

8. More criminal justice outcomes must be delivered. Due to significant budget cuts to the police and Crown Prosecution Service (CPS), many confirmed insurance frauds are not being prosecuted. The pandemic and lockdown increased pressures on the public justice system, as jury trials were suspended in early 2020, adding to an already extensive backlog of cases. **There would be merit in the judiciary seeking to learn from other areas of criminal investigation, such as forensic science, to ensure that the fragmented nature of the current judicial landscape is more joined-up, with processes streamlined and ultimately more criminals brought to justice.**

9. Raising awareness of the grave consequences of committing fraud can play an important role in deterring opportunistic fraudsters from committing insurance fraud. However, organised fraudsters, who commit fraud for a living will only be dissuaded from committing fraud if they are deprived of their liberty and lifestyle. **Overall, while insurers saw some significant sentences handed down for insurance fraud in the wake of the revised Sentencing Guidelines, more recently custodial sentences are rare and, when they do happen, are invariably relatively short.**

10. **It is vital that counter fraud strategies are comprehensive, built around the three core pillars of prevention, detection and disruption/enforcement. They must also be agile and responsive to changing circumstances, so that they remain fit for purpose. Collaboration, including through enhanced information and intelligence sharing, is vital to underpin a holistic approach to stay ahead of increasingly sophisticated and highly mobile fraudsters.**

Detailed Comments

Fraud Landscape

Q1] What fraud risks are (a) individuals, (b) the Government and (c) businesses particularly vulnerable to today and what are the reasons for this

11. Fraud continues to be the most prominent threat facing the UK – being the single largest crime type in England and Wales[1]. Fraud is thought to cost up to £190bn per year[2]. An estimated 86% of fraud is committed online[3] and this is a growing problem. In 2019, the FCA issued 573 scam warnings. In 2020, that figure had grown to 1185, a 52% increase.

12. Online scams have been prominent in recent years. As the FCA itself recognised, there are few barriers to online scams[4]. Both the general insurance (GI) and long-term savings (LTS) sectors are impacted by financial scams perpetrated via online paid-for advertisements, with the problem exacerbated during the pandemic as people look at ways of boosting their income or returns through attractive investment opportunities or making savings by securing cheaper motor insurance.

13. Existing laws relating to online fraud have failed to keep pace with the criminals. Tech companies are currently under no obligation to identify the legitimacy of those placing adverts nor to take down harmful content. Moreover, they're spurred by the fees received from scammers for hosting fraudulent adverts, as well as the fees they receive from the FCA and insurers/investment firms to post warnings on platforms. As such, they essentially profit thrice.

14. Professional enablers of fraud and organised criminal gangs (OCGs) often steal identities to facilitate fraud. For example, technology is used to manipulate caller ID when cold calling or sending SMS texts to impersonate trusted firms and defraud their victim or steal their identity. The GI market, together with other sectors, has worked hard to improve its onboarding ID checks, as well as supporting victims of ID fraud.

15. Fraudsters look for vulnerabilities in controls to exploit and, as insurers have got better at combatting fraud, fraudsters have targeted individual policyholders who have received money from their savings, life or pension policies. Fraudsters are increasingly sophisticated and adapt to changing circumstances e.g. fraudsters now understand that people cannot normally

---

[1] Fraud accounts for 40% of all criminal investigations, rising to 50% of all financial crimes - Priti Patel, MP, Home Secretary, UK Finance Economic Crime Congress 13-14 September 2021.

[2] https://www.crowe.com/uk/croweuk/-/media/Crowe/Firms/Europe/uk/CroweUK/PDF-publications/Annual-Fraud-Indicator-report-2017

[3] Home Office, Fraud Review – Headline Findings, February 2020

[4] FCA letter to Stephen Timms MP, Chair Work & Pensions Committee; Financial Promotions Online – 11 June 2021

access a pension before age 55, so change their fraud typology. By way of a further example, some LTS providers have seen impersonation fraud perpetrated by South African based criminal gangs[5].

16. It is important to note that these issues are exacerbated by a lack of law enforcement resources, which we detail more in later questions.

Q2] 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?

17. **Five to ten years is a long timeframe over which to try to predict fraud trends and changes to the fraud threat landscape. We suggest a full PESTLE analysis would be required to acquire a more complete picture.**

18. **While it is difficult to predict what the economy might look like over such a long timeframe, history shows that during times of financial hardship, fraud tends to increase[6]. Insurers particularly anticipate an increase in opportunistic fraud, application fraud, uninsured drivers and cloned vehicles, as well as more cybercrime perpetrated against individuals e.g. ransomware attacks on digital devices, motor vehicles and homes with internet of things connections.**

19. **Insurers operate in a highly competitive fast-paced environment. Like many other goods and services providers, insurers are dealing with 'hybrid' customers who value their free time and who are highly dependent on the internet for making purchases. Digitisation provides insurers with the opportunity to deliver a smoother customer journey. But consumer expectations are also heightened. Insurers must process applications and claims quickly, with decisions made expeditiously. This means that insurers develop and adapt systems that balance delivering a frictionless customer experience, whilst at the same time deploying robust fraud controls.**

20. **Criminals are already using technology to commit fraud, for example, to exploit keyless vehicles which has caused a rise in vehicle theft claims. As the internet of things grows, it is likely that other devices will emerge that create other opportunities for fraudsters. As such, insurers would welcome legislation to stop**

[5] Simple impersonation of policyholders to fraudulently surrender policies now also involves impersonation of their relatives pretending the policyholder is deceased to claim pension monies.

[6] In 2008, GDP fell by 2.1%, while fraud increased by 7.3%.

devices, whose sole purpose is to commit criminality, being openly sold online.

21. **GIs use technology extensively as part of their suite of counter fraud tools. The overarching aim of the GI sector's data strategy is to simplify the landscape and aspire to a single point of access to rich seams of intelligence and to drive efficiencies through economies of scale. For example, as part of the industry's drive towards streamlining industry data services, in September 2021 the Insurance Fraud Bureau (IFB) announced its new combined technology platform that hosts confirmed fraud and suspected fraud data in a single platform. This will allow IFB customers to support their fraud investigation processes by instantly matching suspected fraud with similar instances of confirmed fraud, allowing for faster and more accurate decision-making. It is also vital that technology is agile and future-proofed so that it able to adapt to external influencers quickly.**

22. **Technological innovation to develop a reliable means of verifying the identity of customers would be highly beneficial. In the LTS market particularly, when a policy claim is made, it can be difficult for insurers to establish whether they are dealing with genuine customers or fraudsters impersonating them. Moreover, fraudsters are increasingly able to produce convincing fake documents, such as passports, driving licences and bank documentation.**

23. **Insurers need a more reliable method of being able to verify customers' bank accounts, especially prior to making payments, to help stop fraudsters stealing customer funds. Many insurers make bulk/batch file payments to customers, which are not included in the Banking Industry's Confirmation of Payee (CoP) service[7]. This means that insurers must resort to other means of verifying payees' bank accounts. Despite previous indications that the CoP service would be expanded in the future to include bulk/batch payments, this has not as yet been progressed. Greater reliance on digital ID is also likely to have a positive impact on validation of consumer identities.**

24. **With reference to our response to Q.1, most fraud is now committed online. We are pleased that the Government has listened to the many different sectors and organisations, including the ABI, which called for online paid-for scam ads to be brought within scope of the Online Safety Bill. We will, however, scrutinise the Bill closely to ensure that no gaps are left for scammers to exploit.**

[7] https://www.ukfinance.org.uk/confirmation-of-payee

25. **Fraud must be tackled holistically with a collaborative approach being taken between different parts of the private sector and between the private and public sectors. The sharing of information and intelligence is key to combatting fraud more effectively.**

Q3] Is fraud and its victims treated as a priority? If not, what are the reasons for this? [NOTE: 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]

26. No. Combating fraud does remain a priority for the insurance sector, with ABI GI members' spending around £200m per annum to this end, including on collaborative utilities such as the IFB and the Insurance Fraud Enforcement Department (IFED).

27. However, while fraud is currently the most prevalent crime committed against individuals, only around 1-2% of police resource is dedicated to fighting fraud[8] (see response to Q.5).

28. There are various barriers to more effective cooperation between the private and public sectors, for example, the public sector does not have a particularly mature data sharing infrastructure. It was extremely disappointing that, after many years of discussion and development, the Counter Fraud Data Alliance (CFDA) – which would have permitted the sharing of confirmed fraud data between the public and private sectors - was aborted following the pilot. The insurance sector (via the IFB) was in favour of transitioning the pilot exercise into a longer-term data exchange, though HMRC and DWP were not convinced as to the returns that would accrue for the public sector.

29. As an industry, insurers support and fund the IFB and IFED to help tackle fraud, which has seen resolutions such as cease and desist letters issued in recent times to help disrupt fraudulent activity and reduce the impact on the CPS, courts and prisons. However, we believe more can be done to deter those who might be considering committing fraud. We would therefore welcome a review of the Sentencing Guidelines and consideration of restricting the freedom of those committing fraud e.g. considering use of tags and curfews (if imposing custodial sentences remains challenging in light of prison capacity limitations).

30. It would help to raise the profile of fraud if it was featured more prominently within the NCA Strategic Threat Assessment. The 2021 edition[9] includes

[8] Following on from the addition of 30 additional investigators to the City of London Police in 2021, we understand that the Spending Review aims to add 350 further officers to the NCA, CoLP and regional organised crime units as part of the Government's Economic Crime Plan.

[9] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/533-national-strategic-assessment-of-serious-and-organised-crime-2021/file

general commentary which focuses on Covid-related fraud, including bounce back loan fraud.

Q4] What is the role of international actors in the UK's fraud landscape? What are the barriers to tackling borderless fraud?

31. It is estimated that around three-quarters of UK fraud cases have an international element[10]. International actors have a key role to play in understanding the exposure to international crime within the UK fraud landscape[11], in improving the prevention, investigation and prosecution of cyber-enabled fraud, in building capacity in law enforcement in the judiciary, and in working with businesses to raise awareness of the cyber threat and enable consumers to take action to protect themselves.

32. The UK Government has stated its intention to engage with international partners to learn from their experiences and build consensus around shared approaches to tackling online harms that uphold the UK's democratic values and promote a free, open and secure internet. The Government expects Ofcom to take an international approach – working with other international regulators - to ensure effective enforcement and promote best practice at a global level.

33. Barriers to tackling borderless fraud include differences between individual States in terms of legal systems, cultures and priorities. For example, throughout Europe, notwithstanding that the GDPR was meant to introduce harmonisation, there still exist many differences in its interpretation (e.g. because of derogations). This can impact industry's ability to share data. There is no European central database for data sharing. Moreover, some EU States do not have their own counter fraud databases.

34. There also exists post-Brexit uncertainty as to the level of engagement between the UK and Europol, with UK requests likely to be lower priority and the power of the UK to influence the law in this area limited, not least because the UK is unlikely to be given a role in the management team. We note also that no non-EU country has yet been permitted access to the EU Criminal Records Information System (ECRIS).

Action to Tackle Fraud

Q5] 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 fraud for fraud?

35. Since 2021, ABI members have invested more than £45m in IFED, a police unit housed within the City of London Police (CoLP) dedicated wholly to combatting insurance fraud. IFED uses the full suite of enforcement tools at

[10] Commons Justice Committee evidence session on Fraud and the Justice System – 20 April 2022

[11] The NECC has recently engaged JMLIT+ members to better understand the exposure to international financial crime threats.

its disposal, including issuing cease and desist letters and disruption via website takedown. Insurers will also pursue civil remedies, such as 'contempt of court' proceedings.

36. However, notwithstanding the insurance sector's ongoing investment in law enforcement capability, and the positive work of the CoLP as the national lead force for economic crime, there is currently insufficient investment in national police resourcing to fight fraud.

37. While recognising that there is now a three-year policing strategy for tackling fraud, the HMICFRS review[12] (August 2021) of its 2019 fraud report, found that the detrimental effect of fraud is as great today as it has ever been. Moreover, there is a disparity between the amount of work fraud creates for the police and the resources allocated to it. Regional forces must complement the work of the funded police units and ensure that tackling fraud is suitably prioritised within their crime strategies. We hope that police efficiency initiatives (such as 'Transform' and the 'Lead Force Operations Room') will help to build bridges and partnerships between the CoLP and regional forces and drive more national police engagement in fighting fraud.

38. Whilst the experience and structure of the organisations mentioned in Q.5 is good, the resource challenges in the CPS and courts impact the benefit that they can deliver. This includes bringing fraudsters to justice and protecting victims, with cases being dropped, and charging decisions and trials being delayed. We would be supportive of increasing the priority afforded to fraud in regional forces, but it must be in conjunction with the right training to tackle these issues. Otherwise, CPS and court time risks being wasted by cases that are likely to be defeated by technical knockouts or errors in the use of evidence.

39. Insurers current experience of Action Fraud is not particularly positive, as so few referrals are progressed to investigation and charge[13]; this applies both to cases where insurers have lost money to fraudsters or have successfully prevented a fraud. The default response from Action Fraud is often that it has not been possible to identify a line of enquiry that could be pursued[14]. Int elligence gleaned from greater information sharing (e.g. bank account details) could present a line of enquiry that could be pursued.

---

[12] 'Fraud: A Time to Choose': https://www.justiceinspectorates.gov.uk/hmicfrs/publications/a-review-of-fraud-time-to-choose/

[13] Life and pensions cases rarely seem to be reviewed and investigated by Action Fraud. One LTS provider has advised that it recently reported a number of cases to Action Fraud which were not taken forward. Following direct engagement with local police, these cases were found to be part of a wider existing investigation.

[14] Reports of fraud and cyber crime have risen every year since 2015/16. However, in the period from the start of 2019/20 to end of September 2021, only 1.2% (11,692) of those reports led to charges – Labour Party Press Release (19 April 2022).

40. It is imperative that the next [third] iteration of the National Fraud and Cyber Reporting Centre ('Action Fraud'), which is due to go live on 31 May 2024, is fit for purpose, with referrers being kept apprised of case progress. Version 1 was manual and cumbersome, and Version 2 failed to provide the desired functionality (e.g. bulk loading of records; real time tracking of progress etc).

41. For frauds such as clone investment scams, the police actively take-down fake domains and websites used by fraudsters. However, **the harsh reality is that as soon as a URL is taken down, a new URL with a very similar address will take its place. Alternatively, the scammer will** set up a new website using the name of a different provider, advertising a slightly different investment opportunity. In short, the issue moves so quickly that simply listing domains will always be outpaced by new domains emerging. Prosecution is therefore vital to deter future fraudulent activity.

Q6] Are sufficient resources available to Government organisations (such as the Serious Fraud Office and the Crown Prosecution Service) and wider police forces to tackle fraud and support victims and how should this be addressed if not? [NOTE: Answers need not be limited financial resources]

42. Please refer to our responses to Qs 5 and 12.

43. We do not consider that the organisations referenced are sufficiently resourced. Government financial cuts to the CPS and law enforcement agencies mean that fraud is not investigated to the extent it merits, with violent and other high harm crime being prioritised.

Q7] 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?

44. The Government has emphasised that, during the COVID pandemic, digital technologies have brought huge benefits, including helping people to work remotely and stay in touch with family and friends. Moreover, the Government has stressed that the framework of the new online regime forms part of its pro-innovation approach to regulating the digital technologies.

45. **However, consumers' confidence is being eroded by the ongoing proliferation of online financial scams, including those predicated on impersonation of financial services providers[15]. We note and welcome that some tech companies have begun to implement** due diligence measures[16] designed to prevent online scam advertisements. However, these are purely voluntary measures and further action is required to mandate these processes and supplementary obligations. Online scams will

[15] Impersonation scams now account for 37%of all FCA warnings issued since 2010.

[16] E.g. Google has introduced measures that aim to ensure that advertisers are properly vetted before adverts are posted, and that adverts promoting unrealistic rates of return on investments are filtered out.

only be tackled effectively if preventative and remedial measures are suitably robust, incur significant consequences for non-compliance and are implemented uniformly across the tech sector.

46. **We wholeheartedly support the recent DCMS confirmation that the scope of the Online Safety Bill will be extended to cover paid-for advertisements**[17] **and that 'fraud and financial crime' offences will be designated as a 'priority offence'. However, the Bill will not reach the statute book for some time**[18]**.** During the interim, the tech platforms must up their game. We understand **that the Online Fraud Steering Group is working with some tech platforms to consider the introduction of a tech sector charter which would comprise a series of sector commitments to strengthen resilience against online scams. The ABI would be supportive of such a charter which would be overseen by the revamped Joint Fraud Taskforce, chaired by the Minister for Security.**

47. **The GI and LTS sectors have taken significant action to combat online financial scams. For example, in relation to clone investment fraud, under the chairmanship of an insurance sector representative, a Public-Private Threat Group Fraud cell**[19] **has looked at how the private sector can adopt best practice to prevent and disrupt clone investment fraud. The insurance sector also supports the Take Five to Stop Fraud'**[20] **campaign, which aims to give consumers the confidence, knowledge and ability to question situations when they could be facing a scam or fraud.**

48. **Similarly, the insurance sector has sought to tackle google ad spoofing**[21] **proactively. It has, for example, provided advice to enable consumers to protect themselves against being scammed**[22]**. Insurers also incur significant ad expenditure to outbid claims companies on mobile browser ad listings. Insurers train frontline staff on how to identify these scams, use detection tools to identify scams and issue 'cease and desist' letters and collate spoofing cases which can then be shared with law enforcement agencies, including Trading Standards, with a view to potential enforcement action.**

Q8] What are the legislative or regulatory impediments to sharing fraud risk data across and between the private and public sectors? For

---

[17] Major law changes to protect people from scam adverts online - GOV.UK (www.gov.uk)

[18] https://twitter.com/nmdacosta/status/1516279277561466885?s=20&t=CTv5teOar-mLkkSK2s9WIA

[19] Under Operation GIANTKIND

[20] https://takefive-stopfraud.org.uk/

[21] Google Ad Spoofing is where CMCs 'hijack' the motor claims process by posing as the claimant's insurer

[22] https://insurancefraudbureau.org/media-centre/news/2020/beware-click-to-call-insurer-ads/

example, to what extent does the General Data Protection Regulation (GDPR) limit data sharing?

49. On implementation of the GDPR, the overarching message from the Information Commissioner was that, if an organisation was complying with the former privacy regime, then the transition to the GDPR-led regime should be one of evolution, rather than revolution. This is reflected in the fact that there are several grounds on which insurers can process personal data (in the absence of 'consent'), such as where processing is in the legitimate interests of the data controller[23].

50. It is of course imperative that firms are set-up to comply, otherwise they do not have the right solid base on which to launch counter fraud data sharing initiatives[24]. The GDPR has introduced various requirements such as the appointment of a Data Protection Officer, subject access requests and data breach reporting. Of particular note, it is vital that 'Impact Assessments' are considered for all new projects. This is compulsory where the data sharing initiative carries significant risk and is good practice otherwise.

51. There is currently a lack of collaboration and data sharing between the private and public sectors. As an industry, we hold significant intelligence which could be beneficial to public sector organisations, such as HMRC, DWP and law enforcement agencies. Similarly, insurers would appreciate easier access to information, including from the public sector, when investigating cases of insurance fraud.

Q9] 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?

52. As well as a legal duty not to commit fraud, consumers have a moral duty to take reasonable measures to be aware of the risk of being defrauded and to take necessary precautionary measures. For example, consumers are expected to undertake necessary due diligence when they authorise a banking transaction e.g. they give their bank an instruction to make a payment from their account, in line with the bank's terms and conditions. Regulations state that if a customer hasn't authorised a payment, the bank should refund the money – so long as the customer hasn't acted fraudulently or with "gross negligence". The FOS takes the view that "gross negligence" is a suitably high bar that goes well beyond carelessness[25].

[23] The GDPR should facilitate, rather than limit, data sharing. There is no reason why thematic intelligence (where there is no specific personal data) cannot be shared. Tactical intelligence can be shared under various grounds for processing of personal data.

[24] The overarching requirement is that data processing must be restricted to what is legal, necessary and proportionate for fraud prevention purposes and comply with obligations on data minimisation, accuracy and retention records.

53. The FCA encourages consumers to report scams, potential harm or bad conduct to the FCA[26] The FCA will publish warnings about firms. The FCA's ScamSmart campaign targets people most at risk of investment fraud

54. **The most effective way to educate the public is using targeted messaging in awareness campaigns that clearly outline the threat to particular groups; what consumers should look out for; what measures they can take to better protect themselves; and how they can report suspected instances of fraud (reinforced where possible through case studies of industry action that has resulted in successful disruption/prosecution of fraudsters). The GI sector has also supported a number of consumer awareness campaigns through the IFB and IFED (e.g. on ghost broking[27]). Furthermore, individual insurers raise fraud awareness with their consumers, including via online bulletins, webpages, and social media posts with advice on how consumers can better protect themselves from fraud.**

Legislative Remedies

Q10] 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?

55. The objectives of the Fraud Act were to clarify and modernise the law and to make fraud law more straightforward for juries and practitioners. The offences contained in the Act were intended to provide law enforcers and prosecutors with a modern flexible fraud law capable of combating the increasing sophistication of fraudulent activity and the rapid technological advances made by fraudsters.

56. In 2012, the Ministry of Justice undertook a post-legislative assessment of the Act to assess whether the Act was fulfilling its objectives. We note that the review concluded that, overall, the Act has successfully achieved its initial objectives of modernising the former array of deception offences[28].

57. Overall, insurers' experience of the Fraud Act has been positive. However, we do not believe that the Act is currently utilised enough due to the challenges

---

[25] https://www.financial-ombudsman.org.uk/businesses/complaints-deal/fraud-scams

[26] https://www.fca.org.uk/about/protecting-consumers

[27] https://insurancefraudbureau.org/media-centre/news/2021/new-drivers-urged-to-avoid-car-insurance-scams-on-social-media/

[28] https://www.justice.gov.uk/downloads/publications/corporate-reports/MoJ/2012/post-legislative-assessment-fraud-act-2006.pdf The review concluded that the Act provides a clear statutory basis for fraud offences, targets complex fraud and introduces new offences specifically designed to assist in the prosecution of technology focussed crime.

referenced in Q.5 around the delays in judicial processes. To better understand the relative effectiveness of the Fraud Act, there might be merit in comparing the number of successful prosecutions for fraud with those for other crimes, such as burglary.

Q11] 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? [NOTE: 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?]

58. Please refer to our responses to Qs. 1, 7 and 10.

Q12] Is the current system in place for prosecuting fraud cases working effectively? If not, what are the key barriers to prosecution?

59. More criminal justice outcomes must be delivered. Due to significant budget cuts to the police and Crown Prosecution Service (CPS), many confirmed insurance frauds are not being prosecuted. The pandemic and lockdown increased pressures on the public justice system, as jury trials were suspended in early 2020, adding to an already extensive backlog of cases.

60. The CPS reviewed its priorities in the wake of the pandemic. The 'Coronavirus: Interim CPS Case Review Guidance' and 'Interim CPS Charging Protocol' indicate that certain serious, but non-urgent, cases are likely to be deprioritised.

61. The need to clear the CPS backlog will become even more acute if insurance and other fraud escalates in the light of increased financial hardship experienced including, for example, as a result of the ending of Government support schemes for individuals and businesses and escalating household costs. At the same time, consumers can be more vulnerable to scams perpetrated by professional fraudsters.

62. Progress has been made with the CPS Specialist Fraud Division to ensure more complex insurance fraud cases are dealt with by specialist fraud prosecutors. However, the process needs to be formalised to ensure a consistent and timely service can be delivered for victims of insurance fraud. CoLP and IFED will continue to work with the CPS to progress this relationship.

63. In relation to online crime, i**nsurers have faced challenges in preserving and presenting evidence in a way that is suitable for juries to understand. There are often restrictive timescales for the presentation of evidence from communications providers in fraud**

investigations, as well as large volumes of data that can often be overwhelming for juries. This can mean even relatively straightforward cases can take several weeks to be heard in court.

64. **There would be merit in the judiciary seeking to learn from other areas of criminal investigation, such as forensic science, to ensure that the fragmented nature of the current judicial landscape is more joined-up, with processes streamlined and ultimately more criminals brought to justice. Intelligence and evidence must be captured and shared in a way that enables the CPS, courts and juries to quickly understand the facts of a case, avoid lengthy trial preparation times and reduce the number of cases dropped where organised fraud is committed.**

Q13] Are sanctions and penalties for criminals who commit fraud an effective deterrent against future criminal activity and, if not, what might be more successful? [NOTE: Respondents may choose to refer to penalties imposed by the judicial system or by specific sectors]

65. Raising awareness of the grave consequences of committing fraud can play an important role in deterring opportunistic fraudsters from committing insurance fraud. However, organised fraudsters, who commit fraud for a living will only be dissuaded from committing fraud if they are deprived of their liberty and lifestyle.

66. **The ABI welcomed the 2014 Sentencing Guidelines for Fraud, Bribery and Money Laundering, which place the victim at the centre of consideration when determining the appropriate sentencing level. As research conducted on behalf of the Sentencing Council indicated, economic crimes are not solely about financial loss. Victims of online scams, for example, can suffer deep emotional distress. People who have experienced mental health problems are three times more likely to have fallen victim to an online scam than the wider population (23% compared to 8%)[29]. Four in ten (40%) online scam victims have felt stressed and three in ten (28%) have felt depressed as a result of being scammed[30]. People with mental health problems also have lower typical incomes and comprise half of those in problem debt[31], meaning if a scam does result in financial losses, the harm caused can be severe.**

67. **Crash for cash scams can involve fraudsters gambling with the lives of innocent motorists[32]. And deaths have also resulted from fraudulent arson claims[33]. We were therefore pleased that the**

---

[29] https://www.moneyandmentalhealth.org/press-release/vulnerable-people-online-scams/

[30] Holkar M, Lees C. Caught in the web. Money and Mental Health Policy Institute 2020

[31] Ibid

[32] https://www.bbc.co.uk/news/uk-england-london-21473080

[33] https://www.bbc.co.uk/news/uk-england-46700151

Sentencing Guidelines recognised, for the first time, the serious physical harm that insurance fraud can cause and put sentencing periods on a par with crimes that had traditionally seen tougher sentences (e.g. banking fraud and confidence fraud).

68. **However, experience of late tends to show that the prospect of physical harm to a third party does not tend to feature prominently. One insurance law firm, for example, has seen a whole range of sentences in recent committal cases ranging from a £150 fine for contempt to a 16-month immediate custodial sentence. Whether or not the perpetrator takes part in the proceedings and expresses contrition also appears to be highly relevant[34].**

69. **Overall, while we saw some significant sentences handed down for insurance fraud[35] in the immediate wake of the new Guidelines, more recently custodial sentences are rare and, when they do happen, are invariably relatively short.**

Best Practice

Q14] What lessons can be learned from effective policy interventions and schemes both in the UK and overseas?

70. **Insurance fraudsters are increasingly sophisticated and highly mobile. It is vital that counter fraud strategies are comprehensive, built around the three core pillars of prevention, detection and disruption/enforcement. They must also be agile and responsive to changing circumstances, so that they remain fit for purpose. By way of example, during the first year of the pandemic, insurance fraud detection rates increased, demonstrating that insurers adapted quickly to the unprecedented challenges created by the pandemic.**

71. **Counter fraud strategies must also be based on collaboration. In 2006, the insurance industry established the Insurance Fraud Bureau to spearhead the fight against organised GI insurance fraud. And the establishment of IFED was in response to swingeing cuts in police resource, allied to the advent of locally elected Police and Crime Commissioners, which meant that there was even less focus on tackling economic crime.**

---

[34] One judge sentenced an EL fraudster to a 16 months custodial sentence for contempt of court: https://www.axa.co.uk/newsroom/media-releases/2019/employers-liability-fraudster-sentenced-to-16-month-imprisonment-for-contempt-of-court/. But, the following day, a motor fraudster who attended the hearing and apologised was merely fined £300 for two instances of contempt by the same judge.

[35] https://www.bbc.co.uk/news/newsbeat-24711241

72. **In relation to online harms, the UK G**overnment has stated its intention to engage with international partners to learn from their experiences and build consensus around shared approaches to tackling online harms that uphold the UK's democratic values and promote a free, open and secure internet.

73. The Government expects Ofcom to take an international approach - working with other international regulators – to ensure effective enforcement and promote best practice at a global level.

74. **Many overseas countries are developing new regulatory approaches**[36] **to tackle online harms, prompted by** the growth of online pollution[37] globally. However, many overseas pieces of legislation tend to focus on one aspect of online harms. For example, Germany's Network Enforcement Act 2017 requires online **platforms (with >2m registered users) to remove 'manifestly unlawful content' which contravenes specific elements of the German Criminal Code (e.g. holocaust denial and hate speech). Similarly, in May 2020, France adopted law to tackle the spread of hate speech. In Australia, an e-safety Commissioner has been appointed with responsibility for promoting the online safety of all Australians – the focus being on the provision of information to make consumers more aware of scams and to establish a complaints service on cyber bullying for young people.**

Q15] Can you suggest one policy recommendation that the Committee should make to the Government?

75. **Because fraudsters are highly mobile, there is a good possibility that those fraudsters who are committing, say, insurance or banking fraud are also committing fraud against the public sector. Effective data sharing between the public and private sectors would be a game-changer in disrupting organised fraudsters.**

76. **As we articulated in our response to Q.3, it was disappointing that after many years of discussion and development, the CFDA was aborted following the pilot. We are pleased that the government is considering public-private data sharing as part of the Economic Crime plan and government fraud strategy.**

22 April 2022

[36] For example, the EU GDPR; Germany's Network Enforcement Act; Australia's Violence Amendment Act; California's Consumer Privacy Act.

[37] Disinformation; manipulation; harassment; privacy breaches