Association of Consumer Support Organisations – Written evidence (FDF0033)

The Association of Consumer Support Organisations (ACSO) welcomes the opportunity to comment on the House of Lords Committee on the Fraud Act 2006 call for evidence. This letter constitutes our response.

ACSO represents the interests of consumers in the civil justice system and the reputable, diverse range of organisations who are united in providing the highest standards of service in support of those consumers. The protection of vulnerable people and those exposed to fraud is therefore a priority for us, as is exploring ways in which the wider industry can work together to combat fraud.

Just as with many aspects of our lives, fraud is becoming increasingly digitised. As one example, and as noted in a recent report, 'pre-internet' the UK police estimated that the average bank robbery would net criminals around £25,000-£30,000 with a high chance of being caught. Online, however, fraudsters can reap highly lucrative rewards often with much less chance of prosecution. It is perhaps no surprise therefore that the UK Office for National Statistics estimates that cybercrime now accounts for half of all crime in the UK.[1] ACSO therefore welcomes the government's renewed focus on digital fraud and ensuring consumers can enjoy increased safety online.

'Ad spoofing', for example, is having a particularly damaging effect not only on consumers but also on insurers, law firms, claims management companies and vehicle hire and repair providers. In such cases, fraudsters are able to pose as insurers by buying Google AdWords, a pay-per-click advertising service, in order to appear at the top of internet search results. Consequentially, when people run a search to find their insurers' details after an accident, they are often misled and exploited by these advertisements. It must be noted that these scams do not just affect those classed as vulnerable, and the embarrassment about being scammed means many victims may not report the issue.

Similarly, for businesses, spoof advertisements can be hugely detrimental to their reputation and day-to-day operations. Indeed, many firms have neither the capacity nor the resources to monitor fraud and impersonation constantly, in turn putting their customers at a heightened risk of fraud. Responsibility for the better prevention of fraud therefore lies increasingly with 'Big Tech' and those whose platforms facilitate or in any way condone or encourage such fraudulent behaviours.

While individuals can be well advised and well equipped to recognise the warning signs of fraudulent online behaviour, there will always be instances where this is not the case. With this in mind, it is imperative that more responsibility is given to Big Tech companies to remove and monitor online fraud. With regards to ad spoofing, many search engines do not require any proof of identification or of a verified business, meaning that fraudsters can create convincing adverts in just a couple of hours. Perhaps more concerning, one third of victims who reported a fraudulent advert on search engines said it was never taken down.[2] Outside of the UK, some platforms have introduced verification programmes which ensure all advertisers are legitimate. Even then, however, the measures allow

[1] Synectics Solutions, *The power of data-sharing in preventing fraud*, January 2018.

[2] Which?, *'Two in five victims of online scam adverts don't report to host platforms'*, April 2021.

advertisers 21 days to submit documentation, during which time their adverts will remain live, providing them with a grace period to continue to carry out fraudulent activity. As search engines can therefore profit from both the fraudulent adverts themselves and the anti-fraud campaigners paying to introduce alert systems, there may not be enough financial incentive for these platforms to intervene meaningfully. Without external pressure from government and regulators alike, this could continue to be a low priority for online advertisers.

With many instances of digital fraud going undetected due to consumer embarrassment, there is a need for more intelligent systems of detection in order to paint a full picture of digital fraud in the UK. Therefore, firms must make deliberate attempts to find fraud and ensure there are comprehensive ways in which consumers can alert them to it. Once detected, data-sharing will be of paramount importance to ensure swift and united action to combat fraud.

In his Mansion House speech in London in 2016 David Clark, National Lead for Fraud with the City of London Police, said: "Collaboration and information sharing is vital because fighting fraud and cyber-crime is often like trying to complete a jigsaw puzzle without knowing who has the next missing piece." The National Fraud Initiative is a good example of the benefits of collaboration, having helped prevent more than £2 billion in losses and facilitating the data-sharing of more than 1,200 organisations across the public sector.[3]

However, reluctance towards such collaboration is largely driven by a fear of breaking General Data Protection Regulation (GDPR) laws. However, these laws are designed within a framework which aims to help businesses be confident they can share personal data lawfully, while protecting the people whose data is being shared. More needs to be done to educate businesses on how to share the data they collect safely and within GDPR confines.

ACSO believes it is crucial that any industry data collected regarding fraud, for example that collected by the Association of British Insurers to assess the extent of motor insurance fraud, should be independently verified, perhaps by the Office for National Statistics. This will help ensure that any public policy decisions are made based on reliable and impartial information, and will also help both educate consumers and protect them from unreasonable accusations of fraudulent behaviour. Combined with better data sharing within both the public and private sector, this type of response could render action against fraud considerably more efficient.

22 April 2022

[3] Cabinet Office, *National Fraud Institute*.