SnapDragon – Written evidence (FDF0020)

1. SnapDragon is pleased to provide evidence to the committee to help inform its deliberations on the Fraud Act 2006 and Digital Fraud. We welcome the committee's work and believe the UK needs to take robust action to tackle fraud, protect consumers but also to protect businesses from intellectual property infringements and related fraud.

About us

2. SnapDragon is a female-led, global tech business based in Edinburgh with a diverse, international team and in 2020 we were winners of a Queen's Award for Innovation.
3. SnapDragon fights fakes online with the aim of keeping brands' reputations, revenues and customers safe using our powerful, proprietary technology which monitors e-commerce sites, social media and the wider internet 24 hours per day, 7 days per week.
4. We protect consumers from the dangers of fakes by identifying and removing these fakes from online sale to disrupt the flow of illicit funds to fraudsters, counterfeiters and organised crime around the world.

Our response

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

5. As the committee will no doubt be aware there are a vast number of fraudulent scams in circulation which continue to increase in sophistication. Due to the way that SnapDragon operates the vast majority of our remarks are in connection with online fraud.
6. Our business works to identify and remove fake products online – from e-marketplaces, social media and domains. Fake products not only pose significant health, safety and environmental risks but also the money generated by scammers is often linked to the funding of organised crime. In addition, sites which are, in themselves fake, have the ability to seize card details and perpetuate further fraud on behalf of the unsuspecting individual.
7. Online fraud and the sophisticated methods of fraudulently obtaining an individual's card details are on the rise. Whether it be fraudsters sending text messages claiming to be from Royal Mail asking them to pay for the delivery of fictitious parcels or more sophisticated scams such as romance or befriending fraud (as highlighted in the recent Netflix documentary Tinder Swindler), individuals in the UK are under almost daily attack – both at home and at work - from fraudsters trying to obtain their private information.

8. Governments are also susceptible to being the victim of fraud and this usually happens at times of national emergency when items or services need to be purchased in a hurry. This has been particularly salient recently with Government purchases of PPE, which has left the UK taxpayer footing a bill for the purchase of substandard products which carry fake CE or ISO certification due to the fact that the supply chain cannot be ethically confirmed. In our view, not enough people are aware of the issues of fake certification and if they are, do not pay the issue the necessary level of attention.
9. Businesses – similar to Government – experience the same issues in so much as they often do not expect B2B products to be faked. These products, which can range from spare machine parts to pesticides, have the potential to cause great harm to businesses but also the UK consumer who will be the eventual recipient.
10. Businesses also must contend with employment fraud – where individuals obtain employment based on falsified documentation. In many of these instances those providing falsified documents are victims of human trafficking who are hidden within the UK in plain sight.

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?

11. What is in little doubt is that instances of attempted fraud will continue to rise worse as criminals become more sophisticated in their attempts to deceive. Individuals, Government and Individuals need to be aware and constantly vigilant and this can only be brought about by awareness raising amongst the general public of the dangers of fake products and what the proceeds of such crime is spent on – more crime. Businesses, as part of their corporate social responsibility initiatives, should be monitoring constantly for fake products – particularly if they are manufacturers or suppliers - and be vigilant for fake domains.

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.

12. In our experience there is very little evidence to suggest that fraud and its victims are treated as a priority. On a near daily basis, we hear stories from individuals who have suffered the personal and professional impact as a result of fraud and there appears to be little joined up thinking on fraud at a government level. It is our hope that the revitalised Intellectual Property (IP) Crime Group – led by the Intellectual Property Office (IPO) and the Police Intellectual Property Crime Unit (PIPCU) will help better

facilitate the sharing of information between Government, law enforcement, public and private sectors.

13. There is a view expressed by some that fraud is 'just money' however this takes no account for the fact that having money taken from you, illegally, can be devastating and exhausting for an individual or business.

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.

14. It is difficult to assess whether sufficient resources are in place to tackle fraud and support victims. Perhaps a more salient question to ask would be whether support exists at lower levels for individuals and SMEs. Our perception, whether this is a correct perception of not, is that the Serious Fraud Office would only seek to tackle fraudulent activity on a large scale.

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?

15. HMRC sends out multiple communications to businesses and it is our view that these should be used to highlight issues of fraud, training/webinars/guidance and advice which can be circulated to team members. These communications should be simple, easily understood and not frightening for the uninitiated. Fraud permeates through every part of society – from romance fraud to phishing, from fake B2B supplies and fake websites to cautionary tales regarding messages supposedly from national institutions such as Royal Mail or HMRC.

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?

16. As outlined above we do not believe that businesses and individuals are well informed about the risks of fraud, but also the consequences of purchasing fake and counterfeit products. We believe there should be a focused awareness campaign for the general public.

21 April 2022