Association of Chief Trading Standards Officers – Written evidence (FDF0018)

1. The Association of Chief Trading Standards Officers (ACTSO) is the membership organisation representing senior Trading Standards managers from councils across England and Wales. ACTSO is focussed on providing effective leadership at the national level while supporting members to lead their services locally and regionally.
2. National Trading Standards (NTS) has a Board made up of senior Heads of Trading Standards from England and Wales with an independent Chair. It uses funds provided from Government to commission Trading Standards' related work, utilising our commissioning model with local authorities. NTS's aim is to protect consumers and safeguard legitimate businesses by tackling serious national and regional consumer protection issues and organised criminality and protecting food supplies by ensuring the animal feed chain is safe.
3. This is a corporate response from the Association of Chief Trading Standards Officers and National Trading Standards, 1 Sylvan Court, Sylvan Way, Southfields Business Park, Basildon, Essex SS15 6TH.
4. 21st April 2022

Q1. 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. **Individuals** - We note that the terms "scam" and "fraud" are often used interchangeably. Distinguishing between fraud and scams has allowed "scams" to be viewed as less serious. We believe that Scams are Fraud and Fraud is a Crime.
6. Criminals have become increasingly sophisticated in their techniques, and they move between different forms of contact, so the same victim is targeted multiple times. For example, victims are often targeted by criminals who promise, for a fee, to help them recover the money they have already lost to scams.
7. Anyone can be a victim of scams and fraud, but some people are more susceptible due to their circumstances or the market place (digital competence, financial hardship, unemployment, social isolation, mental health issues etc). As circumstances change, so does vulnerability.
8. Historically fraud was all about face-to-face dishonesty but now much has moved online. Risks to individuals increasingly change as more and more transactions are made on-line. This gives criminals greater scope for purporting to be something they are not.
9. Technology has enabled criminals to exploit frauds that have existed for many years at an unprecedented scale and speed. Targeted social media advertising, manipulation of search engine results, professionally designed websites and emails, spoofing of communications and the like (all linked

to forms of social engineering) mean that traditional approaches to tackling the problem do not work effectively.

10. The rapid change in people's behaviour due to the pandemic highlights the speed with which criminals can adapt to exploit particular circumstances. The advent of 'missed parcel delivery' texts and e-mails, offers of 'cures' for the virus and non-existent PPE being sold to consumers are all perfect examples of how criminals rapidly adapt to the prevailing climate to defraud consumers.

11. It is important not to overlook the traditional frauds (e.g. doorstep crime, rogue traders, counterfeiting, used cars, aggressive sales practices etc). These frauds continue to be carried out through traditional means, including face-to-face (often on the doorstep), by telephone, and by mail. These frauds are just as serious as online scams, and are often targeted at individuals who are made vulnerable by their circumstances.

12. Another significant challenge is balancing the risk of frauds where the individual loss can be significant, against 'high volume, low value' fraud where the individual loss can be relatively small. Trading Standards have prosecuted cases where the number of victims is in the hundreds of thousands, with in some instances the individual loss being less than £100. However, the criminal proceeds were in excess of £40 million.

13. **businesses -** Business risks (especially those experienced by micro-businesses and SMEs – where Trading Standards may investigate) can be very similar to those experienced by individuals. Fraud is often perpetrated against small businesses and self-employed people who may not have the time or resources to protect themselves. Many do not realise that the protections they have as consumers do not apply to them when acting as businesses.

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?

14. There will be new frauds linked to new products, like crypto-currencies.

15. The cost-of-living crisis will make people more susceptible to fraud.

16. Home energy improvement scams will continue to be a growing area due to the current energy crisis. The market place, such as NET ZERO, may see consumers being targeted with "green deals" providing complex information; and the likelihood of more people making unwise decisions based on imperfect or misleading (fraudulent) information will rise.

17. Artificial Intelligence will have a greater role in both committing and combatting frauds.

18. Government and law enforcement, and technology and tech companies, will have to find new ways to tackle fraud as more and more payments move online without human intervention, for example at the branch or on the telephone which can be key opportunities to stop fraud. Developing algorithms to detect suspicious activity, identifying false identification and

the ability to identify individuals through computer use could all contribute to combatting fraud.

19. It is increasingly difficult for Local Authority Trading Standards Services (LATSS) to police internet and social media sites because they have neither the specialist skills or resource to tackle these effectively.

20. The NTS eCrime Team has done a lot of excellent work at a national level and provided training and support to local LATSS but there needs to be greater Government investment in digital enforcement capability at a local level.

21. Tech firms should do more to protect consumers including having better resourced and more responsive dedicated law enforcement gateways to make it easier to suspend or take-down fraudulent content**.**

Q3 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.

22. National Trading Standards prioritises investigations and related work that focuses on its priority areas such as doorstep crime, intellectual property theft, fair trading fraud, used vehicle fraud etc, and can support dedicated regional teams within local authorities to pursue large scale national cases.

23. LATSS try to prioritise vulnerable people who are at risk of fraud, and have successfully tackled many fraudulent businesses (where consumers are affected) despite having no statutory role or specific powers. However, LAs have many statutory functions they also have to prioritise and are hampered by a lack of resources after ten years of austerity restrictions.

24. Fraud does not seem to be a high priority for most police forces. The police rely on Action Fraud to divert any scam or fraud complaints to LATSS. Reports made by members of the public can be dismissed as "not a fraud" because the "consumer agreed to it" and reports are often written off as "civil matters". There is often little consideration, if any, as to the circumstances in which the consumer found themselves agreeing to something. The police and Action Fraud need to have a greater understanding of what fraud is, of threat and what consumers face.

25. Co-operation is limited by silos and partner resources. Despite the Home Office taking on a bigger role in co-ordinating action across government, the response remains fragmented. However we appreciate this is very difficult to fully resolve due to the breadth and differing nature of frauds.

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

26. Criminals targeting UK consumers tend to operate in different jurisdictions making investigation and prosecution difficult. Online fraud by definition is borderless. Whilst there are good examples of international co-operation (for example the International Consumer Protection Enforcement Network, ICPEN), the arrangements for co-operation can be

cumbersome which will prevent an agile and proactive response. There is room for improvement and sharing of best practice.

27. Trading Standards have no real recourse for overseas offenders beyond referral to other agencies or trying to secure website takedowns.

28. Data sharing is increasingly a challenge across borders, particularly as the UK has now left the EU.

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 force for fraud?

29. The current structure is flawed because it is too police-orientated. The City of London Police do not appear to be aware that other non-police fraud agencies, such as Trading Standards, also tackle fraud. Overall, there needs to be much stronger leadership and clearer ownership of fraud as a crime type along with the authority to direct resources at a regional and national level. The current approach also tends to reinforce some of the systemic attitudes that fraud "is a matter for the police" when in fact many other agencies can, and do, play an active role in tackling fraud. The City of London Police, if they are to continue their role as national lead, need to understand and support non-police agencies; and they must resolve long-standing data sharing issues with local authorities.

30. Data sharing also remains a challenge. There needs to be much greater collaboration and data sharing, particularly between ActionFraud and other agencies (such as trading standards) who play a leading role in tackling fraud.

31. There are too many sources for "prevent" materials, which give different messaging, and the single referring point of ActionFraud gives a false impression that action will be taken when on most matters none is taken.

Q6 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.

32. The very nature of the question reinforces stereotypical views that **only** the police tackle fraud and support victims. Government needs to understand the breadth of fraud, the agencies charged with combatting it and resource it beyond the conventional route of the police to ensure success.

33. There is a strong case to argue that there are insufficient resources targeted at tackling fraud, and in particular online fraud.

34. There needs to be a whole system approach to tackling the problem including much greater use of technology, far great sharing of data and more effective use of analytics to make use of that data, alongside upskilling and investment in frontline staff.

35. Trading Standards (locally and nationally) take many substantial fraud related cases, and conduct and fund their own prosecutions; they could prosecute many more with more resources.

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?

36. The private sector's role is primarily in preventing fraud.

37. There are more opportunities to stop fraud at the point of payment that must be explored. Transaction analysis should be improved so that banks can build up a picture of what transactions are unusual for an individual, rather than just identifying unusual transactions.

38. Telcos can do more to prevent spoofing of telephone numbers and to shut down numbers that are being used to commit fraud.

39. A vibrant and competitive online environment is an important part of the UK economy. However, this must be balanced against the need to ensure consumers are better protected from exposure to fraudulent content online. Modern fraudsters operate as a 'business'. They use all the same tools and techniques that a legitimate business does, but for nefarious means. For example, in NTS funded prosecutions, the criminals have been seen to adapt their use of keyword advertising on search engines, to monitor how effective the changes are and then look at website visitors and conversion rates (i.e. what percentage of website visitors result in a 'purchase'), to optimise the fraud and up their return on investment.

40. To break this cycle, the private sector has an increasing role to play. Aside from all the 'big players' such as search engines, social media sites and the like, many other services form part of the overall 'fraud supply chain'. 'Fake review farms' offering to give a false impression of a company, companies providing search engine optimisation and companies offering to manage and place online advertising are just a few examples of what now forms a part of most online frauds. Organisations such as these (or their representative bodies) need to work much more closely together, and alongside law enforcement, to break down some of the barriers and silo working that still exist.

41. Online 'trusted trader' style services are becoming the medium of choice for rogue traders. Those businesses offering a platform for such sites should be encouraged or required to display information to consumers on the checks that are carried out for the businesses they host, and a gateway for law enforcement to have suspected rogue operators suspended/removed.

Q8 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?

42. A lack of understanding of the available legal gateways for sharing data is one impediment.

43. GDPR and other data protection legislation is often used by agencies and industry as an excuse not to share data. This is rarely an impediment in itself because in most cases there are sufficient exemptions to allow

organisations to share data on fraud. More robust guidance on this from government and regulators would help to overcome these challenges.

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?

44. The role of the individual is to avoid becoming a victim of fraud. However, given the sophistication of fraud attacks and the circumstances that make people vulnerable, a much wider community approach to tackling fraud is needed, rather than expecting individuals to always be able to protect themselves.

45. Consumers receive conflicting messages about the risks of fraud from various agencies.

46. Consumer education is key and should also try to remove the stigma associated with being a victim. Fraud prevention messages need to be consistent, simplified advice on how to protect themselves.

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?

47. The Fraud Act 2006 is a very useful tool with a wide enough scope to cover many forms of fraud that Trading Standards might investigate. Section 9 (and the similarly worded offence in s.993 of the Companies Act) has been particularly useful in tackling businesses that either deliberately set themselves up to commit fraud or develop fraudulent practices over time.

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? 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

48. The legislation is effective for some types of fraud but there are no powers in the Fraud Act specifically for local authorities and it would be helpful if this was addressed.

49. There are currently no powers or formal mechanisms by which online content linked to fraud can be removed. Clearly the Online Harms Bill aims to address some of the broader issues around content hosted online, but it does very little to tackle the problem of online fraud.

50. Whilst the police, trading standards and others have developed mechanisms to seek the removal of illegal online content, it is very much based on direct relationships with online platforms and the willingness of the platform to cooperate. There are very few effective legal measures if a platform is unwillingly to co-operate.

51. We believe there is an urgent need for a formal legal framework that gives powers to appropriate regulators to remove and/or block access to harmful content. For example, the EU Consumer Protection Cooperation

(CPC) Regulations contain a provision that stipulates the relevant member state regulators should have the power to "*remove content or to restrict access to an online interface or to order the display of warnings to consumers accessing an online interface; to order a hosting service provider to remove, disable or restrict access to an online interface; or to order domain registries or registrars to delete a fully qualified domain name and to allow the competent authority concerned to register it*"

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

52. No, it is not. These cases can be complex to present at trial, especially online frauds as there can be complicated technical information that needs to be explained in a way a jury understands.

53. In terms of non-CPS supported regulators, the barriers are:

- resources relating to the time and cost of bring fraud cases.
- backlogs in the Courts are creating enormous delays in getting fraud cases to Court
- burdens of digital disclosure have grown exponentially.
- trading standards are still unable to submit digital bundles to courts

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? Respondents may choose to refer to penalties imposed by the judicial system or by specific sectors.

54. The maximum penalties available in the Act are sufficient. There are sentencing guidelines to support Judges and Magistrates.

55. For national cases supported by NTS' funding, the sentences and other sanctions handed down have been significant for the most part. However, given fraud continues to grow rapidly, it is arguable whether these sentences act as an effective deterrent.

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

56. Multi-agency collaboration is essential to tackling fraud. Information sharing can speed up investigations, prevent duplications, and ensure that victims get necessary support.

57. The NTS Scams Team ran a multi-agency pilot to improve the response to fraud in North Yorkshire and Lincolnshire (2017-1019). It brought together local police, trading standards, adult social care, and third sector and other agencies. They pooled intel, data, knowledge and resources, and improved fraud awareness and education. The pilots saved over £8m for individuals and society. This led to a toolkit on how to establish a multi-agency approach that is now being rolled out across England and Wales.

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

58. Greater recognition of non-police (such as trading standards) involvement in the investigation and prevention of fraud by providing better powers, resources and data sharing arrangements.

21 April 2022