TCG0006

Written Evidence from Dr Jennifer Collins

1. I am Associate Professor in Law at the University of Bristol and a Fellow of the Alan Turing Institute. My research expertise is in criminal law and criminal justice. I have published widely in criminal law doctrine and theory in leading law journals. I joined the case-commentary team at the Criminal Law Review in 2021 and am an elected member of the Education Committee of the Criminal Bar Association.

2. I have active research interests in fraud, as well as in emerging technologies and criminal law. I was Principal Investigator on a UKRI/AHRC grant, 'Fraud During a Pandemic: Identifying and Appraising New Challenges for the Criminal Justice Response in England and Wales' (2021-22). I am currently writing a book on cutting-edge issues in fraud and fraud governance with Hart Publishing.

3. I welcome the Public Account's Committee's focus on public sector fraud and corruption. I focus on the following two issues in this submission to the Committee: (i) understanding the current fraud risk to government; and (ii) government capability to tackle fraud and corruption risks. I use my expertise in doctrinal criminal law, and in emerging technologies and criminal law, to focus on these areas in my evidence. I record my thanks to Bonnie Venter, University of Bristol, for research assistance.

A. Understanding the Current Fraud Risk to Government

4. As is now well-known, the nature of fraud is rapidly changing. This is linked to many everyday interactions now being conducted online exchanges, such as online shopping and banking. The online sphere has been used by fraudsters as a medium which allows for fraud at larger scale and across borders. For example, relevant to the public sector is account takeover fraud. This involves a public official being tricked into sending information to an account that looks legitimate but is controlled by a fraudster.

5. Less explored are the new risks posed to the public sector through emerging technologies. One of the challenges in this area is 'keeping up' with the very rapid innovations in technology—their capabilities and limitations. Another lies in understanding how these technologies are being used by those involved in fraud. Emerging technologies allow for new means of committing fraud at scale, across borders and with broad reach. There is scope for these technologies, especially technologies involving deep learning, to be

utilized by 'bad actors'. For example, there are new risks to the public sector through e-commerce fraud which uses technology to exploit personal information data. The sale of personal information to others becomes a powerful tool in the hands of an individual who acquires this information if they have access to AI algorithms. Algorithms can be used to find matching credentials (such as username/password and card details). This poses a risk for information held by the public sector, and it demonstrates the importance of 'information-capital' to fraud.

6. A current area of fraud-innovation against the public sector involves ChatGPT. This is a form of generative AI. I look in some detail at ChatGPT as an illustrative example of a new fraud-risk posed by emerging technologies to the public sector.

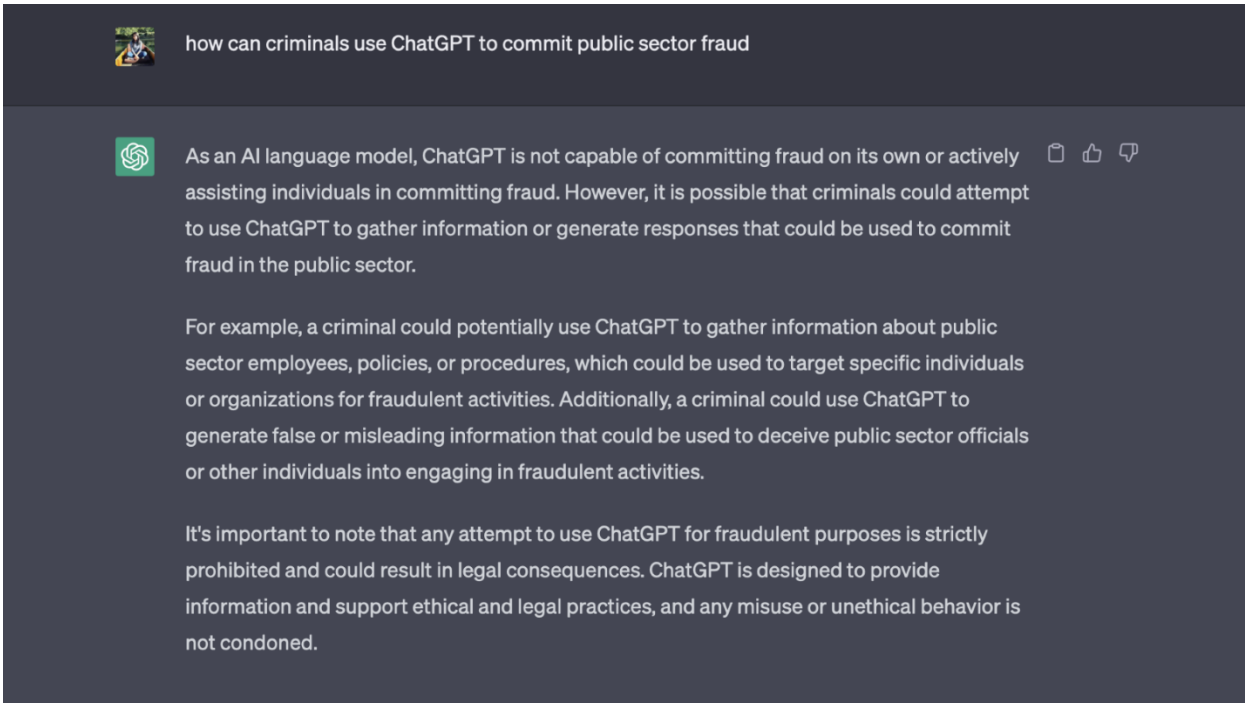
7. ChatGPT is developed by Open AI. It is based on a Large Language Model (LLM), a subfield of AI based on deep learning techniques. ChatGPT is based on Generative Pre-trained Transformer (GPT) architecture. This involves training using a neural network designed for natural language processing. Significant amounts of data were trained to understand and generate natural language text. The dataset involved in ChatGPT's training was over 45 terabytes of text from the internet, including books, articles, websites and other. Open AI has made clear that the data used to train ChatGPT is publicly available. But further information has not been given, with the company citing competition and security reasons. Since its launch, ChatGPT has become the fastest growing consumer app in history. 100 million users were recorded within two months. The most recent version for subscribers of ChatGPT Plus is GPT-4. This was released in March 2023. The latest version claims to be able to solve more advanced problems more accurately.

8. While not without restrictions (for example, there is a content moderation policy to assess whether content is sexual, hateful, violent, or promoting self-harm), the potential of this technology in the hands of fraudsters is significant. Arguably ChatGPT increases the risk of public sector fraud in the following two ways:

9. *First, by automating self-learning, ChatGPT gives potential fraudsters a powerful means of accessing contextualized knowledge quickly.* This could include acquiring contextualized information on how to carry out a fraudulent scheme or by providing information about specific public sector bodies, their means of organization and/or operating systems. When my research team asked ChatGPT (version 3) on 22 April 2023

how it can be used by criminals to commit public sector fraud, it provided the following examples:

Figure 1



10. There is also potential for public sector employees to use ChatGPT to disseminate confidential information. It was recommended in an February 2023 report into innovation in Britain that ChatGPT be used in public service delivery. This could also occur negligently or innocuously. A recent report notes an example of an employee cutting and pasting a firm's 2023 strategy document into ChatGPT in order to generate a PowerPoint presentation. This is a live concern. It is estimated that 11% of information that employees copy and paste into ChatGPT is confidential. This has already led to requests to the Department for Science, Information and Technology to direct civil servants on appropriate use of ChatGPT for government work.

11. *Second, ChatGPT provides a tool to commit sophisticated and far-reaching fraud via more authentic phishing, malware delivery capabilities, social engineering, or impersonation.* It can 'upskill' individuals who would otherwise hold limited skills or personal capabilities in these modes of delivery. It can also reproduce language patterns to allow for impersonation of a particular speech style or technique. For example, Europol's March 2023 report notes that ChatGPT has the ability to draft highlight authentic texts which may have previously been detectable due to poor spelling and/or

grammar. This could be used to create authentic-looking content-specific texts or e-mails to public sector employees. This could be beneficial to those who lack English-language skills. Overall, the effect is to allow for online fraud which can be created faster, more authentically and at an increased scale and reach.

B. Capability to Tackle Fraud and Corruption Risks and Recommendations

12. On capability to tackle public sector fraud risks, there is a recent history of needing to do better. This is illustrated in relation to fraud on the Bounce Back Loans scheme. It is estimated that in 2020-21 there was between £33.2 billion and £58.8 billion of fraud and error in government spending and income unrelated to the Covid-19 pandemic. Funding for recovery must be robust, combined with political willpower to avoid losses to the public purse. There must also be greater transparency about losses and recoveries in relation to fraud in the public sector.

13. I confine my written comments to issues relating to emerging technologies and criminal law measures to tackle public sector fraud, given my expertise in these areas.

(I) Criminal Law Legislation

14. Criminalization ought not to be the first or only port of call in responding to pressing social issues. The criminal law is a coercive tool, and its use must be carefully justified. There is a strong public interest in tackling public sector fraud given that these are losses to the public purse. I would go as far as to suggest that there may be positive obligations to tackle public sector fraud which are normatively distinct from obligations to address fraud against the private sector. If this approach is accepted, clarity is needed on the precise scope of these obligations, and if and how they require criminal law interventions.

15. On existing criminal law measures, there is a question about whether existing criminal offences are sufficient to penalize fraud against the public sector. Some of the examples cited above show how, due to the rapidly changing nature of fraud, it will become more difficult to trace fraudulent activities and subsequently to prosecute it. It is conceivable that central cases of fraud will depart from the models of fraud in section 1 of the Fraud Act 2006. That is: fraud by false representation, failure to disclose information, and abuse of position. For example, facilitated by emerging technologies, 'phishing' exercises and malware adaptations may be more central to the *modus operandi* of fraud than previously thought.

16. A similar enquiry has recently been undertaken in relation to private sector fraud. The House of Lords' Fraud Act 2006 and Digital Fraud Committee published their report, 'Fighting Fraud: Breaking the Chain' in November 2022. In chapter 6 of their report, they argue that fraud offences, including offences found in the Fraud Act 2006 and the Computer Misuse Act 1990, are sufficient to tackle new forms of private sector fraud. This was also the approach taken in the Ministry of Justice's June 2022 'Post-legislative Assessment of the Fraud Act 2006'. The argument is that existing offences, such as section 1 Fraud Act 2006 offence, are wide enough to capture new forms of fraud.

17. Is this reasoning robust in relation to public sector fraud, enabled by emerging technologies? The example given in Part A above of public sector employees negligently or otherwise using ChatGPT to disseminate public sector confidential information could lead to greater use of fraud by abuse of position. Moreover, new forms of phishing may increase the use of fraud by false representation.

18. But alongside section 1 of the Fraud Act 2006, I note potential for push onto conspiracy to defraud to 'mop up' new forms and iterations of fraud. It is common to see claims about conspiracy to defraud's 'mopping up' value to prosecutors (most recently in the Ministry of Justice's Post-legislative Assessment of the Fraud Act 2006 (June 2022)). This is the case despite the breadth of the general fraud offence found in section 1 of the Fraud Act 2006 and assurances that conspiracy to defraud's use would be reduced since the implementation of the Fraud Act 2006.

19. The overwhelming view of practitioners in the 2022 review (above) is that conspiracy to defraud is an effective and essential tool in combating fraud. An 'interests of justice' argument is put forward. In complex cases—for example involving several distinct types of criminality; cross-jurisdictional cases; multiple victims; organised crime involvement--conspiracy to defraud allows an overall picture to be presented, avoiding dividing issues into several different trials. This argument has been repeated many times. It is an attempt to balance a 'usefulness' and 'overall picture' argument against the obvious rule of law defects of the offence, which gives rise to 'interests of justice' reasoning. In other words, the interests of justice 'can only be served by presenting to a court an overall picture' of a complex case, and the conspiracy to defraud offence allows for this. This argument is problematic because it gives even weight to these competing interests despite the serious rule of law concerns which speak against the offence.

20. The Committee's review of existing offences to target fraud ought to engage with detailed literature which makes the point that legal certainty is not respected by the conspiracy to defraud offence. For example, the post-Fraud Act 2006 discussion of conspiracy to defraud which held the offence to be inconsistent with legal certainty, on which see the Joint Parliamentary Committee on Human Rights, *Fourteenth Report: Review of International Human Rights Instruments* (2006), HL.99, HC 264, para. 2.12. Detailed engagement with Article 7 ECHR (European Convention on Human Rights) and its jurisprudence is needed, given that this right continues to be protected in the proposed Bill of Rights Bill.

21. The focus should also be on the principled limits of preventing fraud against the public sector using the criminal law. A failure to prevent fraud offence has been added to the Economic Crime and Coporate Transparency Bill. As of 2 May 2023, this Bill is in the House of Lords at the Committee Stage. The proposed offence would make it a criminal offence for companies to fail to prevent their employees, agents, or contractors from committing fraud on their behalf. This would provide an alternative route for corporate prosecutions, overcoming difficulties with proving the 'directing mind and will' of a company was involved in fraud. It would sit alongside existing Money Laundering Regulations. The proposed failure to prevent fraud offence would apply to all large corporate bodies (as defined by the Companies Act 2006 definition) and partnerships and includes incorporated public bodies. It is estimated that 24,900 relevant bodies will fall within the scope of the offence. A company will be able to rely on a defence if it can prove that it has adequate controls and measures in place to prevent the offence. It therefore requires public sector bodies to review their risk assessments and pushes towards a fraud-prevention culture. Should the Economic Crime and Corporate Transparency Bill receive Royal Assent, the government will publish guidance on reasonable fraud prevention procedures.

22. Enforcement of any new legislation of fraud prevention is key. It is doubtful the extent to which the proposed offence would lead to criminal law convictions in practice. In line with limited enforcement of the failure to prevent bribery offence, it is anticipated that there will be a rise in Deferred Prosecution Agreements should the failure to prevent fraud offence be enacted. This would allow public sector organizations to circumvent admission of criminal liability. The substantive offence of failure to prevent bribery, found in section 7 of the Bribery Act 2010, has been little used since its implementation in 2010. To the best of my knowledge, this has led to three section 7 corporate convictions. The offence of failure to prevent the facilitation of tax evasion (ss. 45 and 46 of the Criminal Finances Act 2017) has resulted in no convictions since its implementation. A 2020 Freedom of Information request showed that HMRC had 30 live investigations into the offence of failure to prevent tax evasion (9 criminal enquiries have been opened and 21 are under review. As of January 2023, HMRC had 28 potential cases under consideration. The government has been keen to emphasise that criminal investigations are not the sole measure of success of this criminal legislation, and that legislation was enacted to drive behavioral change. There is a strong possibility that this will be the pattern followed by any failure to prevent fraud offence.

23. I will give a lecture to the Criminal Bar Association about a failure to prevent fraud offence on 9 May 2023, should this event be of interest to the Committee.

(II) Emerging Technologies

Emerging Technologies Used for fraud-innovation

24. What are the implications of rapid technological advancement for fraud and corruption in the public sector? The public sector must work hard to stay ahead. This involves having clarity on the capabilities of emerging technology to enable fraud. This challenge exists around generative AI, given the extremely fast pace with which this is developing. As noted in Part A of this written evidence, ChatGPT is the technology currently attracting attention in fraud scholarship. It was surprising that the challenges of generative AI were not specifically highlighted in the government's recent AI Policy Paper, 'Establishing a Pro-Innovation Approach to Regulating AI'. Other examples of the interface between public sector fraud and emerging technologies could be given.

25. A recent paper, 'A New National Purpose: Innovatiion can Power the Future of Britain,' emphasizes the need for proactivity, and this insight ought to apply in relation to fraud against the public sector:

'The UK (United Kingdom) should develop proactive and anticipatory governance of general-purpose AI. This would require better benchmarking of AI progress, even against speculative concerns, as well as improved oversight of the development of advanced systems, such as through monitoring and reporting on computer infrastructure used for training AI.'

26. An anticipatory response requires appropriate expertise input. Recent research into government bodies' understanding of public sector fraud showed that 'only 14% of the 70 organisations assessed understand and measure the fraud and error risks that they face and just 6% could demonstrate a strong return on their counter-fraud investment.' I argue that emerging technologies and AI need to be placed at the forefront of crafting a principled response to public sector fraud. This will require interdisciplinary working between academia and practice, using knowledge-exchange to ensure ongoing horizon scanning, led by specialist research teams with relevant expertise. Research into new fraud threats cannot be undertaken in a siloed way for the public sector. The government's 24 April 2023 announcement of £100 million for an expert taskforce to build and adopt safe AI systems is a welcome development. It must be supported by robust leadership who can deliver internationally leading research in specified periods, so as to avoid delays like those which have beset the new Fraud Strategy.

27. Linked to the need for interdisciplinary teams, is sufficient funding. The Public Sector Fraud Authority estimates that 'even without specific measures of fraud and error risk,

27% of the organisations it assessed showed clear signs of a mismatch between their resources and risk'. Appropriate investment will be required to acquire enhanced cybersecurity tools for the public sector. For example, cybersecurity which can spot spoofed voices.

Emerging Technologies Used for Tackling Fraud

28. The future trajectory for fraud also involves greater reliance on emerging technologies to prevent and pursue fraud. This is in line with the Public Sector Fraud Authority's 2022/2023 Building for Success aim of improving the performance of counter fraud activity across government. The relevance on AI and machine learning to fraud detection and prevention is set to grow on an upwards trajectory. Generative AI, such as ChatGPT, could be used by the government to innovate in fraud-regulation.

29. Alongside this there must be development of principles which regulate the use of AI and emerging technologies to fight fraud. These must not be biased towards benefiting a particular sector. Technological advances can influence the political environment, pushing power towards big tech companies. The way in which technology is used, and who it benefits, is a concern which must be handled transparently. There are examples of other jurisdictions in suspension of technology use until key principles can be mapped out. For example, the Italian Data Regulator made the decision on 30/03/2023 to issue a temporary ban on the processing of personal data of individuals in Italy by ChatGPT. Canada has also launched an investigation into ChatGPT. This came after an allegation that data was being collected, and personal information disclosed, without users' consent.

30. Use of AI or ML (Machine Learning) such as ChatGPT to prevent fraud must respect core principles (such as privacy, transparency and explainability) if the use of technological advances in this area is to be principled and robust. Challenges for building transparency and explainability should be noted in the fraud-prevention context. For example, too much transparency as to how fraud detection mechanisms work may be exploited by fraudsters, allowing circumvention of fraud detection systems.

31. Fraud can be detected using several different ML approaches. Some systems use a combination of supervised and unsupervised learning to detect fraud. Literature on ML notes that unsupervised systems may be more difficult to explain. The ability to explain the AI used should be prioritized where unsupervised ML is used to prevent fraud. These systems pose a greater threat to the rule of law, as far as their outputs can be unforeseen and therefore scrutiny of their outputs is necessary.

May 2023