Royal United Services Institute – Written evidence (FDF0036)

This submission is made by the Royal United Services Institute (RUSI). It represents the views of the research team members who have contributed their expertise as it relates to the wide-ranging themes covered by the inquiry. It does not represent the views of RUSI itself.

Queries about this submission should be forwarded to the Senior Programme Manager, Alanna Putze.

About RUSI

RUSI is an independent think tank engaging in cutting edge defence and security research. A unique institution, founded in 1831 by the Duke of Wellington, RUSI embodies nearly two centuries of forward thinking, free discussion and careful reflection on defence and security matters. The institute prides itself in providing world-class and policy-relevant analysis and training built upon our evidence-based approach. RUSI is frequently the podium of choice for world leaders and policy makers in the defence and security realm; the institute is frequently a forum in which policy makers and politicians alike seek to provoke debate and critical thinking on matters of national security.

Our research focuses on the threat of fraud as it relates to money laundering, cybercrime and international security. Fraud remains largely a 'silent threat', with the scale of its impact on citizens, the private sector and the public purse met with a significantly under-resourced response. In this context, the prevailing political narrative fails to convey the full impact of fraud beyond financial losses or the psychological impact on victims. To inform a new approach to tackling fraud, RUSI's research explores the social, economic and criminological impacts of fraud and their intersection with the broader security landscape in the UK and internationally. We seek to pave the way for fundamentally different pathways of responding to the problem.

Summary of our response

Over the following pages, we have set out our response to the Committee's Call for Evidence. For ease, we have summarised the key points of our response below.

1. The UK has seen an unprecedented rise in the types of online-enabled volume frauds or scams that have the hallmarks of organised crime. Low barriers to entry and high rewards have made these types of fraud increasingly attractive to criminals.
2. Fraud has not historically been seen as a priority for government or law enforcement. There is a 'responsibility vacuum'[1] in relation to fraud with ownership fragmented across different Government departments and law enforcement bodies.
3. It is clear that many law enforcement and other Government organisations are under resourced compared to the volume of fraud. Increased funding is vital, but this should not simply be a 'more of the same' approach, but part of a clear strategy for funding the right skills, in the right places, under a new set of clearly defined roles and

[1] https://static.rusi.org/the_silent_threat_web_version.pdf

responsibilities of different agencies involved with targets and measurable outputs.

4. The current structure for policing fraud is not fit for purpose. Urgent reforms are needed to the funding of fraud policing, the operational structures supporting this, the nation tasking model and the standing of fraud within the Strategic Policing Requirement, set by the Home Secretary.
5. The international nature of the fraud threat, particularly in relation to cyber-enabled frauds, means that a traditional criminal justice approach needs to be combined with more disruption-based law enforcement tactics, including disrupting the channels used by fraudsters to reach UK victims. There is, however, a dearth of intelligence in relation to fraud actors and, in particular, there is a gap around the specific nature of the international threat from fraud
6. Information and data sharing are crucial to the fight against fraud however there has been limited progress to date in establishing mechanisms for sharing, particularly cross-sector. GDPR, and to a lesser extent Competition Law, are often cited as a reason for a reluctance to share but there is currently a lack of clarity as to specific barriers to information sharing. The barriers often appear to be cultural rather than a result of any legislative or regulatory impediment. Proactive communications from regulators may be helpful here in overcoming any reluctance to share.
7. In our opinion, the Fraud Act 2006 provides an adequate range of offences and simplifies charging decisions. There are, however, limitations to its scope particularly in relation to the current epidemic of international cyber-enabled volume fraud. This is a not an issue that can be remedied easily with legislative change and should be addresses by a comprehensive national fraud strategy which considers the correct balance between criminal justice interventions, disruptive law enforcement techniques, the role of the UK intelligence community and the role of the private sector.
8. The introduction of a corporate criminal offence of failing to prevent fraud may help to drive cultural change and increase the willingness of telecommunications, social media and online platforms to implement process changes which reduce the ability of perpetrators to reach victims via their communications channels.
9. The UK's response to the current fraud epidemic would be bolstered by improved leadership within Government through the appointment of a cross-department, statutorily appointed 'Commissioner' responsible for holding the Government to account for reducing the impact of fraud on individuals, businesses and the public sector.

Fraud Landscape

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

1.1 The last few years have seen a rapid growth in the level of fraud in the UK. While the true level is likely greater than has been reported, the Telephone-operated Crime Survey for England and Wales (TCSEW) estimated that 4.6m fraud offences were carried out in the year to 31 March 2021[2]. In particular, the UK has seen a rise in the types of online-enabled volume frauds or scams that have the hallmarks of organised crime. Low barriers to entry and high rewards have made these types of fraud increasingly attractive to criminals. This has led the UK to be called the 'bank scam capital of the world'[3].

1.2 There are a number of reasons why the UK – including individuals, businesses and the public sector – are particularly vulnerable to these types of fraud. One of the key factors is the use of the English language. Another is the widespread digitisation of everyday life in the UK and our significant adoption of online services like e-commerce and online banking without sufficient education in digital safety. We would also argue that the UK's lacklustre enforcement regime in the last few years has enabled fraudsters to flourish.

1.3 While there are clearly specific fraud typologies which target individuals, such as romance frauds, or target businesses, such as Business Email Compromise (BEC), many of the underlying techniques that fraudsters use, such as identity theft and social engineering, are similar. Considering frauds through the silo of the types of victim, as the Government response to fraud is structured, may therefore not be an effective way to tackle the fraudsters who do not tend to work in such silos.

2. 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?

2.1 As we have seen over the last few years, fraudsters are able to adapt their techniques to changes in society, technology and the latest trends or world events. Investment scams, for example, often taken advantage of people's interest, and lack of understanding, in topics such as cryptocurrencies or the metaverse. The fraudsters also mirror our behaviour – as our lives have moved online, so have their techniques. It is likely, therefore, that fraudsters are going to continue to take advantage of changing behaviours to exploit gaps and vulnerabilities. Given that technology has been, and will likely continue to be, the force that has changed our behaviours the most, greater consideration of vulnerabilities at the stage of product development will be essential in protecting consumers and equipping customers with the appropriate education to protect themselves online.

---

[2] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2021#fraud

[3] https://inews.co.uk/inews-lifestyle/money/saving-and-banking/uk-bank-scam-capital-world-lack-police-resources-1351256

2.2 While new technology will pose risks to consumers, there are also huge benefits in fraud prevention and detection that we are likely to see from technology; for example, advanced data analytics techniques can take advantage of the huge amount of data that businesses have generated to better spot unusual behaviour and drive actionable insight. Furthermore, information sharing across law enforcement jurisdictions and country borders is enabled through secure communication channels.

2.3 While the impact of these organised volume frauds is a crucial focus of the Committee's work, it should also be expected that other 'traditional types' of fraud including asset misappropriation, accounting fraud and corruption may well increase in the short to medium term due to the expected economic pressure on individuals and businesses. Counter-fraud practitioners often point to the 'fraud triangle'[4] developed by Dr Donald Cressey which identifies three motivations for a fraudster – incentive, rationalisation and opportunity. Both incentives and the ability to rationalise a fraudulent act are often increased during times of economic difficulty, as we are experiencing now. As a result, we can expect to see more 'insider' frauds as well as the increased risk that employees and those with access to data and systems may be more inclined to provide criminals with access or information in return for payment.

3. 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.

3.1 RUSI has previously described a 'responsibility vacuum'[5] in relation to fraud with ownership fragmented across different Government departments and law enforcement bodies. As a result, fraud is not seen overall as a priority. This is partly a result of the multi-faceted nature of the fraud threat however there are examples of other cross-cutting issues where there is established leadership thereby encouraging a more 'joined up' response across government and with law enforcement and the public/private sectors. Of particular note is the siloed approach to fraud and cybercrime, despite the two being deeply interwoven as a result of the digitisation of society as previously mentioned. The complex nature of digital or cyber fraud will continue to lack the appropriate prioritisation so long as the siloes continue. We are supportive of the idea of the appointment of an 'Economic Crime Commissioner' to act as a central focal point and to hold the Government to account akin to the Independent Reviewer of Terrorism Legislation.

3.2 Within policing, there are a number of issues which contribute to fraud being seen as a lower-tier priority, including the lack of public visibility for the crime; as noted in the 2019 HM Inspectorate of Constabulary Report (HIMCFRS) "Fraud: Time to Choose" examining the policing response to fraud[6] , fraud doesn't 'bang, bleed or shout', meaning it is often deprioritised in favour of more visible street crimes. Furthermore, the geographical disbursement of victims across multiple force areas means that individual cases, in isolation, score poorly against the policing operational prioritisation model, MoRILE[7].

---

[4] https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud

[5] https://static.rusi.org/the_silent_threat_web_version.pdf

[6] "Fraud: Time to Choose", HMICFRS, June 2019.

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

4.1 As we have previously identified, there is a 'dearth of intelligence' in relation to fraud actors and, in particular, there is a gap around the specific nature of the international threat from fraud[8]. There appears to be a significant overseas element to a number of the common scam typologies, for example 'romance frauds' are often associated with groups in parts of West Africa, however the cross-border nature of scams and the rise of 'crime as a service' tools means that fraudsters can be located anywhere in the world. The nature of borderless fraud is a challenge for a number of reasons not least the difficulty in gathering evidence across borders, via cumbersome Mutual Legal Assistance channels, particularly in uncooperative jurisdictions. This largely means an approach which blends traditional criminal justice outcomes with more disruption-based law enforcement tactics should be part of the approach, including disrupting the channels used by fraudsters to reach UK victims.

4.2 RUSI research found that Interpol plays a particular role in accessing jurisdictions and intelligence that is difficult to attain in bilateral relationships.[9] Furthermore, financial services organisations have access to intelligence and law enforcement agencies in difficult to reach jurisdictions much easier than UK law enforcement agencies, due to their international operations. UK law enforcement is hampered by difficult diplomatic relationships with some of the countries that fraudsters often operate from.

<u>Action to Tackle Fraud</u>

5. 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?

5.1 The current structure for policing fraud is not fit for purpose. Urgent reforms are needed to the funding of fraud policing, the operational structures supporting this, the nation tasking model and the standing of fraud within the Strategic Policing Requirement, set by the Home Secretary.

5.2 In terms of funding, as many commentators have argued including most recently the Social Market Foundation[10], the level of police resource dedicated to fraud, around 1%, is out of step with the scale of the challenge. Significant uplifts in dedicated, ring-fenced fraud policing funding are needed to recruit, train and retain experienced officers, financial investigators and specialist prosecutors.

5.3 From a structural perspective, while the lead force model for fraud policing (currently sitting within the City of London Police) is the right approach in terms of having a single view of the intelligence picture, the model is undermined by the limited operational assets held by the lead force themselves and their inability to task local and regional policing assets to investigate. Too frequently, cases referred to local forces for progress simply

---

[7] https://www.gov.uk/government/publications/management-of-risk-in-law-enforcement-morile-based-scoring

[8] https://static.rusi.org/the_silent_threat_web_version.pdf, pages 19 - 22

[9] The UK's Response to Cyber Fraud: A Strategic Vision (rusi.org)

[10] https://www.smf.co.uk/commentary_podcasts/fraud-is-britains-dominant-crime/

go un-investigated due to limited resources and the issues noted above regarding policing prioritisation models.

5.4 Significant improvements could be made by implementing a clearly defined budget, operating under a single tasking and coordination model with clear roles and responsibilities at national, regional and local policing levels. All of this should be supported by greater recognition of fraud as a priority crime type, particularly within organised crime policing, within the Strategic Policing Requirement set by the Home Secretary[11].

5.5 Within a renewed, coherent policing response to fraud, there is a need to specific address the place of the victim within the response, with a better articulated, honest and realistic strategy for dealing with fraud victims. There have been significant improvements under the roll out of the National Economic Crime Victim Care Units, however the misalignment between the public perceptions of the roles of Action Fraud in practice has led to a lack of confidence in the law enforcement response, leading, at least in part, to the significant under-reporting of fraud by victims.

6. 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.

6.1 It is clear that many law enforcement and other Government organisations are under resourced compared to the volume of fraud. Increased funding is vital, but this should not simply be a 'more of the same' approach, but part of a clear strategy for funding the right skills, in the right places, under a new set of clearly defined roles and responsibilities of different agencies involved with targets and measurable outputs.

6.2 While increasing the numbers of police officers and prosecutors specifically dedicated to tackling fraud is obviously part of the response, there is a need to address the recruitment and retention problems of specialist civilian financial investigators within the system, as noted in a recent RUSI/Spotlight on Corruption paper[12]. Core to tackling fraud and wider economic crime is also better use of data analytics and strategic intelligence analysis to pin-point key problem sets, therefore addressing the skills gap in government around data science and intelligence skills is also key. Furthermore, there is also a notable skills gap, particularly in relation to cyber fraud skills, with much of the expertise residing in the private sector. This needs to be addressed by making public sector work more attractive to private sector participants, via attractive pay and conditions packages.

7. 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?

---

[11] https://www.gov.uk/government/publications/strategic-policing-requirement

[12] https://ik.imagekit.io/po8th4g4eqj/prod/rusi-spoc-white-paper-economic-crime-enforcement.pdf

7.1 The private sector has a key role to play in protecting consumers from fraud, particularly the financial services, technology and telecoms sectors. While there are some good examples of collaboration across sectors, for example Stop Scams UK, a membership organisation made up of representatives from the three sectors, the reality remains that the incentives for preventing and/or detecting fraud vary between different types of organisations. For banks, the drive to reduce the amount of fraud suffered by their customers is as much driven by financial considerations as consumer protection; this has been heightened by the introduction of the Contingent Reimbursement Model (CRM) for banks in relation to Authorised Push Payment (APP) frauds. This provides banks with a powerful financial incentive to work to combat fraud. The incentives within other sectors are different although we welcome the proposed introduction of a duty of care to protect users from fraud for search engines and online platforms in the Online Safety Bill[13], including in relation to paid-for adverts.

8. 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?

8.1 There is currently a lack of clarity as to specific barriers to information sharing, particularly in the private sector. GDPR, and to a lesser extent Competition Law, are often cited as a reason for a reluctance to share but the barriers often appear to be cultural rather than a result of any legislative or regulatory impediment. Proactive communications from regulators may be helpful here in overcoming any reluctance to share.

9. 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?

9.1 The role of the individual in relation to fraud is deeply embedded with the relationship between user and device or digital service. While campaigns such as Take 5 or Cyber Aware aim to improve public knowledge of digital services, cyber awareness campaigns are riddled with issues and tend to struggle to create impact. Educating the public on fraud prevention should be as much the private sector's responsibility as it is the government and law enforcement. Products should be built with security by default and regular user communications should be used to improve knowledge and skills in digital safety.

<u>Legislative Remedies</u>

10. 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?

10.1 The Fraud Act 2006 was introduced in an attempt to simplify the law in relation to fraud. The Law Commission note in their 2002 recommendations that 'A general offence of fraud would be aimed at encompassing fraud in all its forms. It would not focus on particular ways or means of committing

[13] https://www.gov.uk/government/news/major-law-changes-to-protect-people-from-scam-adverts-online

frauds. Thus it should be better able to keep pace with developing technology.'[14] In our opinion, the Fraud Act 2006 provides an adequate range of offences and simplifies charging decisions.

10.2 There are, however, limitations particularly in relation to the current epidemic of cyber-enabled volume fraud. As noted in our response to (4), the international nature of many frauds makes it more difficult to successfully prosecute overseas offenders. This, however, is a not an issue that can be remedied easily with legislative change and should be addresses by a comprehensive national fraud strategy which considers the correct balance between criminal justice interventions, disruptive law enforcement techniques, the role of the UK intelligence community and the role of the private sector.

11. 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

11.1 As noted above, there are practical difficulties with tackling modern forms of fraud through an approach which views the issue as primarily a criminal justice one; as noted in a 2021 RUSI paper[15], the scale, nature and impact of fraud means it should be viewed as a national security threat, which means calibrating the response through a 'whole of government' intelligence-led model. The limitations of dealing with increasingly cyber-enabled fraud purely through a criminal justice response are clear, particularly where victims and perpetrators are based in different jurisdictions.

11.2 One area, however, which may however increase the private sector's contribution to tackling fraud, however, is the introduction of a corporate criminal offence of failing to prevent fraud. As highlighted in the Law Commission's consultation on the topic[16], the 'identification principle' (whereby 'only the acts of a senior person representing the company's "controlling mind and will" can be attributed to the company') has meant that it is difficult, if not impossible, to prosecute large corporates for misconduct carried out for and on behalf of the company. The introduction of such an offence could help to drive cultural change and increase the willingness of telecommunications, social media and online platforms to implement process changes which reduce the ability of perpetrators to reach victims via their communications channels.

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

12.1 The government's plans to open a specialist Economic Crime Court in the near future are welcome and will help to overcome some of the challenges faced by prosecutors. However, this court will have limited capacity and will likely only deal with the highest tier of cases. We would welcome further proposals to introduce a system of specialist ticketed economic crime judges to aid the court process

---

[14] https://www.lawcom.gov.uk/app/uploads/2015/03/lc276_Fraud.pdf, paragraph 1.6(4)

[15] https://rusi.org/explore-our-research/publications/occasional-papers/silent-threat-impact-fraud-uk-national-security

[16] https://www.lawcom.gov.uk/project/corporate-criminal-liability/

Best Practice

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

14.1 The nature of the global fraud threat is such that there is no single policy intervention which will solve the issue. However, there are some good examples of industry interventions which have helped to disrupt the business model of fraudsters, such as Confirmation of Payee and the 159 anti-fraud telephone line. The objective of any legislative and/or regulatory change should be to continue to make it incrementally more difficult for fraudsters to commit their crimes while also ensuring that there are sufficient resources dedicated to prosecution and enforcement.

14.2 There are also examples of how technology innovation has had an impact on fraud levels. For example, the introduction of Strong Customer Authentication (SCA) across Europe as part of the Second Payment Services Directive (PSD2) has resulted in a "significant reduction in the volume and value of fraudulent e-commerce card- based payment transactions" according to the European Banking Authority[17]. Given that SCA only came into force in the UK in March 2022, we have not yet seen the impact that it will have on fraud levels in the UK however the evidence from countries that have already implemented suggests that it will lead to a reduction in some types of fraud.

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

15.1 The UK's response to the current fraud epidemic would be bolstered by improved leadership within Government through the appointment of a cross-department, statutorily appointed 'Commissioner' responsible for holding the Government to account for reducing the impact of fraud on individuals, businesses and the public sector.

22 April 2022

[17] https://www.eba.europa.eu/eba-publishes-report-data-provided-psps-their-readiness-apply-strong-customer-authentication-e