

## **Social Market Foundation – Written evidence (FDF0026)**

### About the Social Market Foundation

The Social Market Foundation (SMF) is Britain's leading cross-party think-tank, standing proudly in the centre-ground of politics since 1989. The Foundation's main activity is to publish original papers on key topics in the economic and social fields, with a view to stimulating public discussion on the performance of markets and the social framework within which they operate. The SMF is a registered charity (1000971) and a company limited by guarantee. It is independent of any political party or group and is funded predominantly through sponsorship of research and public policy debates. The SMF is overseen by a Board of Trustees and Chair.

### **SUMMARY**

Fraud generates considerable individual psychological, social and economic costs. However, despite intermittent efforts over the past 20 years to improve the law enforcement and wider societal response to fraud, the situation has worsened not improved.

Therefore, the debate about how to effectively tackle fraud – the most frequently perpetrated crime against people and households in England and Wales – needs a renewed vigour. A revival of old – but promising – ideas that have not yet been tried and an injection of new ideas are needed to help drastically improve the counter-fraud response by politicians, policymakers, the police, and other relevant agencies.

An effective response requires leadership from the top of government and a sustained commitment from politicians and policymakers. Equally important is the long-term provision of financial, human, technological and legal resources commensurate with the scale of the problem. An effective response also needs to recognise the interconnections between fraud and other types of crime, such as cyber and organised crime, and money laundering. Reform efforts will need take into account such linkages, to be successful.

The current disjointed counter-fraud landscape is ineffective and needs an overhaul. However, that overhaul should not be limited to changing policing structures (though important). Solving a problem like fraud requires a "systems approach", whereby tackling it becomes a national objective, underpinned by a long-term coherent plan that involves sustained and complimentary counter-fraud, cyber and organised crime and anti-money laundering efforts across multiple domains, which add up to a whole – in terms of effectiveness – that is greater than the sum of its parts.

We believe effective actions can be taken across ten areas, which together would make a significant impact on the levels and cost of fraud to society. These are:

- Understanding the nature and scale of the problem better.
- Stronger political leadership and rigorous governance arrangements to oversee a more effective counter-fraud response.

- Re-organisation of policing structures and a redistribution of policing responsibilities – within an overall envelope of higher expenditure on law enforcement
- Substantial increases in the capacities and capabilities of law enforcement and prosecutorial agencies.
- A more pro-active private sector incentivised by a new legal framework.
- Modernisation of the current stock of laws relevant to economic, cyber and organised crime, as well as an expansion of civil powers available to the authorities (including improved asset recovery efforts) and revisions to other laws and rules (e.g. company, insolvency and consumer laws, financial services regulation and other legal powers such as licensing functions) that could help compliment the criminal law in tackling economic, cyber and organised crime.
- An overhaul of the criminal justice process.
- A greater focus on the international dimension, including strengthening networks of law enforcement cooperation, updating the international legal landscape around such crime and supporting enforcement in developing countries.
- A more open and honest public discussion about economic crime in general and fraud in particular.

## **Fraud Landscape**

**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?**

1. Technological change is likely to continue to provide more opportunities for criminals to commit crimes such as fraud. The development of “crime as a service” tools will expand and put the ability to perpetrate frauds into the hands of more criminals. Further, the growth of automation and technologies such as AI will mean that the tools at criminals’ disposal will become more sophisticated. In addition, technological trends such as the spread of the internet of things and greater use of new forms of data such as biometric data – among other technologies coming on-stream – will generate new vectors of attack for those trying to de-fraud people, businesses, and the public sector.
2. One potential avenue for mitigating some of the fraud risk – but which has yet to be properly attempted – is to try and make vulnerable technologies more secure and the services that fraudsters utilise (whether to commit their crimes or launder their criminal gains) more difficult to access and use. This will require a change of mindset among policymakers and the public towards the digital and economic infrastructure across which crimes such as fraud (as well as associated criminality such as cyber-crime) is committed and through which its proceeds are stored and “cleaned”. That

means policies that encourage infrastructure providers to “internalise” some of the crime-related negative externalities created by their activities and to design-out crime.

3. A new comprehensive domestic legal framework is required to create a system of incentives which will encourage banks, manufacturers, software vendors and digital platforms and incorporate the designing out of crime, such as fraud, into their development and operational processes. In particular, digital platforms need to face some liability for the criminality that is committed using them. Further, financial intermediaries (such as banks) should be more directly liable too, with legal obligations to reimburse individuals and businesses that fall victim to fraud. In addition, intermediary services, sometimes referred to as “key enablers” (such as lawyers, accountants, property professionals, among others) need to face stricter sets of legal obligations around identifying and preventing fraud and be subject to more effective enforcement where they fail in their obligations.
4. The framework should include previously touted proposals for creating “corporate liability for economic crime”. Such a measure needs to be clear on legal responsibility. Ambiguity over liability in the area of corporate frauds has been identified as significant deficiency in the current law, according to the Serious Fraud Office (SFO).<sup>1</sup>
5. The best way authorities can prepare for how future economic and technological developments might facilitate ever greater amounts of criminality, is to engineer a legal framework and enforcement response that is flexible enough to adapt as the economy, technology, and the capacities and capabilities of criminals evolve.

**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.**

6. Fraud and its victims are not treated as a priority. This is clear in the paltry amount of resource the government and police dedicate to dealing with fraud committed against individuals, households, and businesses – relative to its scale, sophistication and the quantum of harm it causes. The low priority given to such crime has been highlighted by several sources, including HM Inspectorate of Constabulary (HMICFRS) and the recent Strategic Review of Policing by Sir Michael Barber.
7. Limited police resource is dedicated to tackling economic crimes such as fraud. According to official statistics, in England and Wales, just 0.8% of police workforce in 2021 (1,753 staff) were focused on such categories of crime despite, for example, fraud accounting for more than four in ten crimes committed against people and households in 2020-21. In other

---

<sup>1</sup> ‘Outdated laws helping big companies to get away with fraud’ | The Times

words, for each police officer and civilian working on economic crime there were 2,500 frauds committed, in 2020-21.

8. Reasons for this low prioritisation are multiple. One reason is the complexity of the counter-fraud landscape, and the inadequate incentives embedded in it, to encourage police action on a scale commensurate with the scale of criminality and the detriment it causes. Specifically, the City of London Police (CLP – the national lead on fraud which looks after Action Fraud and National Fraud Intelligence Bureau (NFIB)) is disincentivised from long-term planning for their counter-fraud activities because they are reliant on inconsistent, short-term funding (which are also inadequate in quantum) to pay for appropriately trained policing on the scale needed to adequately tackle the sophistication and the amount of fraud that is currently perpetrated.
9. Another reason is that the CLP cannot direct or hold local forces to account, where much of the (inadequate) counter-fraud capacity and capability and responsibility for investigating (most) frauds resides.
10. A third factor helping ensure economic crime in general, and fraud in particular, are low priorities include the scarcity of skilled counter-fraud investigators, and the lack of forensic accountancy and cyber forensic capabilities across English and Welsh constabularies. Consequently, there are few police staff that can investigate such crimes.
11. A fourth element is the prioritisation by the leadership of the 43 geographic forces of other criminal activities, which have a higher profile locally and nationally. Under the conditions of limited financial resources, there is little incentive for Police and Crime Commissioners (PCC) and Chief Constables to prioritise economic crimes such as fraud.
12. A fifth is an inadequate understanding and lack of accurate mapping of the fraud landscape and fraudsters and the total direct and indirect personal and economic cost to society, which inhibits the optimal allocation of human, financial, and technological resources.

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

13. There are a number of significant gaps in the criminological understanding of fraud and those who commit it. One of the gaps is the extent to which the large number of frauds that are perpetrated every year against the public originate from criminals based abroad or in the UK. Not having this detail is a key barrier to the appropriate allocation of policing resources, especially judgments about whether more need to be focused upon international or domestic efforts.
14. Policing and other authorities involved in counter fraud activities such as the Crown Prosecution Service (CPS), HMRC, the FCA and Trading Standards among others, need to be more international in their outlook than perhaps they have in the past, to improve the response to fraud. While it is natural for these bodies and others to primarily look inwardly at the UK, there needs to be a concerted effort to devote more time and

resources to building, deepening and then effectively utilising international networks between law enforcement authorities, prosecutors, regulators etc, for anti-crime purposes. This aspect should be central to policymakers thinking when considering reforms to the counter-fraud institutional landscape.

15. Other barriers to tackling cross-border crime include the international legal landscape, which has not yet caught up with the global nature of some criminality, including fraud. The various bilateral, regional, and international treaties relevant to these kinds of crimes need to be reviewed, strengthened, and the unhelpful divisions between cyber-crime, organised crime and economic crime done away with, where possible. In an ideal world, there would be a comprehensive global convention put in place, which sets out an internationally agreed framework for cooperation between countries and relevant authorities across all three types of crime, reflecting their interconnectedness, complimented by a "beefed up" Interpol.
16. Short of this optimal solution, more countries need to be encouraged to sign-up to existing international instruments which help improve international collaboration such as the Budapest Convention on cyber-crime and the European Convention on Mutual Legal Assistance. In addition, the UK's other Mutual Legal Assistance Treaties (MLATs) need to be upgraded. Some, for example, are narrowly focused upon specific types of crime. Another problem with many of them is that the procedures for assistance are insufficiently swift and hinder law enforcement efforts unnecessarily. This needs mutually agreed-upon reform.
17. Specific improvements to the international legal framework that could be made include harmonisation of technical forensic standards, for the exchange of information between law enforcement agencies. Further, ambitions for reforming the relevant international legal frameworks should examine measures which would dramatically reduce the "frictions" in international collaboration, such as the mutual recognition of warrants, evidential standards and other investigative tools and methods used in other jurisdictions across economic, cyber and organised crime enforcement efforts. Work should also be done on the viability of extra-territorial laws passed by one country being routinely enforceable by another country's domestic authorities and greater flexibility over where prosecutions can and should take place to help avoid reliance on lengthy extradition procedures.
18. Changes to the international legal landscape are necessary but not sufficient conditions for effectively tackling the international dimension to economic crime in general and fraud in particular, as well as cyber and organised crime. Ultimately, the law enforcement capacity and capability of all countries needs to be substantially enhanced. However, this is particularly the case in middle and low-income countries where such capacities and capabilities lag those of advanced industrial countries, which are also inadequate to the task, in many cases.

### **Action to Tackle Fraud**

**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?**

19. The current structure for policing fraud is ineffective. The two key metrics of policing performance i.e., the level of (fraud and cyber) crime as measured by the Crime Survey of England and Wales (CSEW) and the “clear-up” rate, illustrate that the police (and by implication the existing structures and approaches of the police) are failing.
20. There are a number of problems in the current organisation of the police response to fraud, which help result in the performance failings described above. A key one is the role of the CLP, which is the lead force for fraud in England and Wales, yet it is under-funded and under-staffed relative to the scale of the crime. Further, its funding is uncertain as it depends on the settlement negotiated by the Treasury with the Home Office triennially and then decisions by the latter about where to allocate its revenues within the overall funding envelope. This makes long-term investments (i.e., over five-to-ten-year horizons) in capacity and capability difficult.
21. In addition, the CLP has no ability to marshal and direct the counter-fraud resources in the 43 local constabularies and yet relies on the latter to do the bulk of the investigation and apprehending of offenders. However, fraud is not a priority for most local forces, who face squeezed budgets, competing priorities and a lack of sufficient skilled officers and civilian staff to investigate complex crimes, that are time and labour intensive to deal with. The result is that the parts of the police service of England and Wales that are worst placed to deal with fraud are ultimately the ones that – in most cases – are expected to deal with it. Consequently, they fail to do so.
22. Action Fraud has been roundly criticised for being ineffective. The problems faced by Action Fraud have most recently been described by Sir Craig Mackey in a 2020 report into the efficacy of the CLP as the national lead force on fraud.<sup>2</sup> Quite simply, Action Fraud is failing to deliver the kind of service required if the public are to have confidence in it and use it.<sup>3 4</sup>
23. The effectiveness of the National Fraud Intelligence Bureau (NFIB) is another vital component of the current counter-fraud effort. However, like Action Fraud, it has many deficiencies. An analysis by HMICFRS in 2019 found many problems, including long delays in key actions such as reviewing cases. A number of problems with NFIB were also identified by the Mackey report. These included technical problems with the NFIB’s operating system as well as resourcing shortages.<sup>5</sup>
24. However, any potential effectiveness it might develop going forward, through improvements to operating systems or boosts to NFIB’s funding,

---

<sup>2</sup> Action Fraud report (redd-monitor.org)

<sup>3</sup> Action Fraud investigation: victims misled and mocked as police fail to investigate | News | The Times

<sup>4</sup> Action Fraud ‘unfit for purpose’, Which? finds – Which? News

<sup>5</sup> Action Fraud report (redd-monitor.org)

will be severely blunted by the wider structural problems with the current organisation of the policing response. For example, the NFIB can build up an intelligence picture for the police, but the linkages in the chain between analysis and action, by a local constabulary for example, are broken. The policing depends on having sufficient manpower, technology and expertise to proceed with an investigation and many constabularies do not have these.

25. A further structural weakness of the current organisation of the policing of fraud is its detachment from the policing of other crime which is closely associated with fraud, such as cyber-crime, money laundering and organised gangs. For example, while fraud sits with the CLP and local constabularies, responsibility for organised crime is split between the National Crime Agency (NCA), the Regional Organised Crime Units (ROCU) and local constabularies, but with an overarching power for the NCA to "task" and "coordinate" national, regional and local resources to specific anti-crime efforts.<sup>6</sup> .
26. A more rationally organised policing structure would look to align and integrate the policing of these different but closely linked types of crime, in order to maximise the organisational and investigative benefits of pooling expertise and generating a critical mass of skilled specialists, to make it easier to organise and incentivise effective action and to generate economies of scale and scope in the use of resources. Therefore, local constabularies should lose responsibility for economic and cyber-crime and for all but the most local organised criminal activity. An expanded NCA should be the entity policing inter-regional, national and international economic crime, cyber offences and organised criminality. This should involve folding into the NCA the CLP's fraud responsibilities as well as those of the SFO. The ROCU network should remain but be enhanced and put on a permanent footing. Further, they should be jointly run by the NCA and the local constabularies within each region. They should focus upon intra-regional economic, cyber and organised crime.
27. Finally, two further indispensable elements of restructuring the policing landscape to better deal with economic, cyber and organised crime, is the prioritisation of such crimes at the highest political levels and robust governance of the reformed institutional arrangements. One way this could be achieved is through the establishment of a new leadership group at the highest level of government, co-chaired by the Chancellor, Home Secretary and Secretary of State for Justice. This group would set the overall aims for policy and enforcement, monitor the performance of the various law enforcement and regulatory organisations concerned with economic, cyber and organised crime and hold those leading them to account for their efforts.

**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.**

---

<sup>6</sup> National Crime Agency inspection: national tasking, coordination and governance of the response to serious and organised crime - HMICFRS ([justiceinspectorates.gov.uk](http://justiceinspectorates.gov.uk))

28. The fight against fraud is underfunded compared to the scale of the problem. This also appears to be the case with cyber and organised crime, too. Across the 43 constabularies of England and Wales, official data suggest that of the 135,301 police officers and 75,858 other police staff in England and Wales, a mere 0.8% (1,753) are focussed upon economic crime. This equates to around 2.1 officers and other staff working on economic crime, for every 1,000 fraud offences recorded by the police.
29. The more accurate CSEW, which has been recording the quantum of fraud committed against households and individuals in England and Wales for several years, suggests that the ratio of police staff to the most likely amount of crime is worse, with one officer or civilian worker for every 2,500 frauds committed. This ratio of crimes to police staff is so high that it makes it impossible for the police to dedicate sufficient effort to tackling such crimes. The ratio needs to be re-balanced through more resources, including extra officer and expert civilian staff. However, the true picture is likely to be worse still as the CSEW does not capture frauds perpetrated against businesses. Data from the Federation of Small Businesses (FSB) suggested that across the years 2017 to 2019 22% of SMEs suffered from digital/ online invoice fraud, 14% were subject to other kinds of fraud committed by a third party against the business and 5% suffered from fraud committed by an employee.<sup>7</sup>
30. If policing resources were allocated more proportionately across the crimes that are recorded by the police, then around 30,000 officers and other staff should be focussed upon economic crimes such as fraud. If the police had the funding and manpower, a proportionate allocation of resources based upon fraud and cyber-crime recorded by the CSEW would see the police putting around 80,000 staff into the fight against such crimes.
31. Policing is already stretched, as the recent Barber review made clear. Analysis suggests that in 2020-21 there were around 36 police recorded crimes (excluding fraud and cyber) per police officer in England and Wales. Using CSEW estimates of crime (excluding fraud and cyber) the ratio of crimes to officers increases to 42 (non-fraud and cyber) crimes per police officer. Further, compounding the high numbers of crimes per officer is a detective shortage across England and Wales, which was noted in a HMICFRS in a 2019 report. In addition, even if the police had sufficient police and civilian staff to shift into dealing with economic crime such as fraud, the deficit in skills and expertise would make it impractical.
32. Therefore, merely switching existing resource at such scale into economic (and associated criminality such as cyber) crime is unrealistic. Additional recruitment of people to work specifically on economic and associated crimes – on top of the current 20,000 uplift in officers – is required to tackle this problem. We estimate that, a further 30,000 uplift of police officers and expert civilian staff would cost in the region of £3.5 billion per annum. If 80,000 were to be recruited, this would require an increase in expenditure of around £9.2 billion a year. The additional uplift would need to be undertaken considering the development of a long-term workforce

---

<sup>7</sup> Calling-time-on-business-crime.pdf

plan for the police service, to ensure that the officers and staff that were recruited had the right aptitudes for the roles they would be needed for, and the appropriate training and development was delivered.

**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?**

33. The private sector builds and operates the information technology infrastructure through which the digital fraud takes place. Consequently, no policy aimed at tackling fraud can ignore the importance of the technology sector.
34. At present, the attempts at building a partnership between the state and private sector (e.g. through forums such as OFSG) is not addressing the problem effectively enough. Those problems include fraud that is committed with relative impunity across digital platforms, service providers collecting and hosting personal data that is hacked by criminals which in-turn is used to perpetrate fraud, payments taken or made from UK banks to fraudsters and insufficient attention paid by key intermediaries such as lawyers, accountants and others, to what criminal acts they may be inadvertently facilitating.
35. As noted earlier in this submission, new comprehensive legal framework is required to tackle this "intermediaries" problem, which places more responsibility on private actors to be more proactive in their efforts to deter crimes like fraud. A central aim of designing a new body of law is to incentivise the designing out of crimes such as fraud and cyber-crime from digital technology products and services and financial networks.
36. Another important aspect of that new legal framework should be corporate liability for economic crime, building on the example of the current obligations on businesses towards modern slavery and anti-money laundering. To encourage compliance - as well as mechanisms such as fines - large public companies should be obliged to report annually to shareholders and the public on their efforts to reduce the risk of fraud being committed against and through their business.
37. Further, the current Suspicious Activity Reporting (SARs) system aimed at detecting instances of money laundering should be expanded to include suspected fraudulent activities. However, the current regime has been identified as falling short in a number of ways.<sup>8 9</sup> Therefore, any expanded regime will have to be a reformed regime, for example, taking on board the kinds of reforms recommended by the Law Commission in 2019<sup>10</sup> and the Treasury Select Committee.<sup>11</sup>

---

<sup>8</sup> Shape Up or Ship Out: Time for Wider Reform of the UK AML Supervisory Regime | Royal United Services Institute (rusi.org)

<sup>9</sup> Economic Crime - Anti-money laundering supervision and sanctions implementation (parliament.uk)

<sup>10</sup> Economic Crime - Anti-money laundering supervision and sanctions implementation (parliament.uk)

38. The sharing of good data is key to building up a clear intelligence picture of fraud risks. Access by both relevant private sector organisations and the public sector – in particular, law enforcement – and its judicious use would enhance both fraud prevention efforts by companies and individuals and in the pursuit and prosecution of fraudsters by the police and CPS. Relevant private sector organisations should be obliged to share appropriate data with each other and the authorities and vice versa. Organisations like Cifas are good examples of this happening voluntarily and the SARs regime is an example of the private sector sharing data with the government (albeit with many flaws). However, there is no overall rationale behind or coherence to the data sharing that currently goes on and the legislative framework governing data protection is poorly designed for supporting effective data sharing between multiple organisations and across public and private sectors at the scale and granularity required, to help make a difference to fraud. Ultimately, the current arrangements are not built upon a clear analysis of what data is needed by whom, to help prevent fraud being perpetrated successfully and aid in the effective pursuit of criminals. Putting a more coherent system in-place (with data security a key balancing consideration) will require a rethink of what is currently in-place.
39. The private sector could have a greater role in augmenting the capacity and capability of law enforcement to pursue economic criminals. Much of the stock of investigative skills that is needed to tackle fraud resides in the private sector. Efforts to harness this for the public good need to be made. However, this would require the government being more open than it usually is to cooperation with the private sector, especially with intelligence. Ways of harnessing this private sector expertise should be investigated by policymakers. One option could be to set up a system for contracting out the pursuit of economic and cyber criminals, perhaps on the basis of “deputising” competent private individuals and organisations to undertake investigations in lieu of the police and regulators. Complimentary to utilising more private sector investigatory capability and capacity would need to be greater scope for more private civil action and prosecutions against fraudsters, in addition to the work of the CPS. The review of the criminal and civil laws and relevant regulatory rules, proposed below, would be a good opportunity to examine the obstacles to more private prosecution and use of civil remedies.

## **Legislative Remedies**

**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? 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.**

40. While the Fraud Act 2006 is generally considered a useful updating of the various deception offences that existed before the Act became law.<sup>12</sup> <sup>13</sup> it is only one piece of legislation among many (along with common law offences such as conspiracy to defraud), which are relevant to dealing with economic (and associated types of) crimes. As has been noted earlier in this submission, a key aspect of successfully tackling fraud has to be understanding its interconnections with other types of crime such as organised crime, cyber offences and other economic crimes such as money laundering, and not treating it in isolation. Therefore, rather than focusing on laws that pertain to fraud alone, or even economic crime more broadly, what is needed is an extensive review which leads to the updating and consolidation into a single code of the panoply of laws that are relevant to economic crime, cyber-crime and organised crime. Central to that updating must be to ensure the revised stock of laws are comprehensive, mutually reinforcing, reflect modern crime trends and are as “future-proofed” as possible. This will likely require an initial expert review process that could take up to a year, plus subsequent time for legislating. In addition, regular reviews would need to be undertaken on a cross-government basis, to ensure the consolidated code of rules were kept updated.
41. Alongside the criminal law, ways the civil law might play a more prominent role in helping tackle fraud and associated crimes and potential reforms to enable this should be examined as part of the same review. The specific possibilities for the widespread use of civil tools such as civil sanctions, injunctions and compensation as either alternatives or compliments to criminal prosecutions needs to be explored and specific proposals developed where practical to do so.
42. The review should also undertake an analysis of the way the current approach to asset recovery operates, where a number of failures have been highlighted.<sup>14</sup> <sup>15</sup> The objective of having it within scope of the review should be to identify improvements in the effectiveness of this important tool and make appropriate recommendations to policymakers in government for reform.
43. Further to the criminal and civil law there are likely to be a range of ways regulatory requirements and administrative rules can be utilised to help the fight against economic crime. For example, Company and Insolvency laws, consumer law, financial services regulations and licensing activities by regulators, local authorities and others are all potentially relevant to “cracking down” on organised crime in general and fraudsters. In addition, the nature of the (statutory and professional) rules which govern key professions such as lawyers and accountants and other industries such as property development and estate agency, all of which can be “key

---

<sup>12</sup> Post legislative assessment of the Fraud Act 2006 ([justice.gov.uk](http://justice.gov.uk))

<sup>13</sup> Text ([sas.ac.uk](http://sas.ac.uk))

<sup>14</sup> The Party's Over: Confiscating Proceeds of Crime and Corruption in the UK | Royal United Services Institute ([rusi.org](http://rusi.org))

<sup>15</sup> 201906\_op\_reaching\_the\_unreachable\_web.pdf ([rusi.org](http://rusi.org))

enablers" of economic crime, are also important and should be part of the review.

44. The proposed review would need to have a wide scope and would require careful management as a result. However, the former is necessary to avoid disjointed policy making and ensure any updated body of law is coherent and well drafted. Evidence from the Netherlands suggests that operating in a more coordinated and strategic way can deliver positive results. There, the authorities developed a cross-government "combined approach" to tackling organised crime, which attacked organised criminals on two fronts; combining traditional law enforcement with extensive administrative measures in complimentary ways.<sup>16</sup> Consequently, there are likely to be lessons that the UK government can learn from the Dutch experience.

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

45. The current system in place for prosecuting fraud is not working effectively, as evidenced by the substantial growth in instances of fraud at the same time as there has been a significant decline in convictions (some estimates suggest a fall of around two-thirds in ten years).<sup>17</sup>

46. Concerns about the efficacy of the criminal prosecution process are not new and have been around for some time, yet the nettle has not been fully grasped either by successive governments or the judiciary. For example, some of the difficulties of prosecuting complex fraud were touched upon by Sir Robin Auld in the early 2000s in his review of the criminal courts. Many were also noted by the Government Fraud review, published in 2006.

47. Some of the problems are reflections of general failings in the criminal justice process, not least the sometimes-difficult relationship between the police and the CPS and the general under-resourcing of both services. These more general problems require long-term structural solutions. However, they will hinder the prosecution of criminals until they are resolved.

48. Other obstacles are more specifically related to the challenges associated with prosecuting complicated crimes like fraud, as well as cyber-crimes, money laundering and organised criminality. Evidence gathering is particularly challenging, when much of it is electronic and requires considerable expertise to analyse. Expert testimony is also often required in fraud trials and can be a barrier to swiftness. Further, the length of some cases and issues of understanding among jurors of complex events and evidence are also challenges. Another problem is the small number of specialist prosecutors available to the CPS to prosecute (swiftly) complex crimes like fraud, relative to the scale of the problem.

---

<sup>16</sup> (PDF) Going Dutch? Comparing Approaches to Preventing Organised Crime in Australia and the Netherlands (researchgate.net)

<sup>17</sup> <https://committees.parliament.uk/oralevidence/10063/pdf/>

49. Some of these problems – to the extent that they impact the bringing and successful prosecution of perpetrators of fraud – could be mitigated by embedding in the law enforcement response to fraud, measures such as the institutionalisation of multi-disciplinary and multi-agency teams to target criminals and solve cases, as well as ensuring leadership and management is of the best quality so that individual, team and agency performance is maximised.
50. Specialism is considered an important way of increasing efficiency in and the efficacy of court systems. Given the challenges in tackling fraud and associated crimes such as cyber and organised crime, the creation of specialist courts that have the requisite expertise among the judges and staff that operate them, along with tailored procedures and rules of evidence to deal with particular types of crimes and policing techniques utilised to bring criminals to justice, should be seriously considered by policymakers as a measure that could improve the prosecution of fraud and associated crimes. Sir Robin Auld – in his 2001 Criminal Courts review – was attracted to the idea of building-into the criminal process more expertise about fraud.<sup>18</sup> A specialist Financial Court was also proposed by the Government Fraud Review in 2006.<sup>19</sup> Sir Robin Auld also proposed replacing juries in complex fraud trials, either with tribunals of judges and specialists or judges sitting alone.<sup>20</sup> This is another long-standing proposal that should be revisited by policymakers.
51. A somewhat organic experiment in South Africa, with Special Commercial Crime Courts (SCCC)<sup>21</sup> might offer policymakers in the UK a model for how the principle of specialist courts focussed on specific categories of crimes could be taken forward. The (albeit limited) evidence suggests that SCCC's are – overall – a positive development. One of their strengths is how they have been able to bring together investigators and prosecutors and embody specialist knowledge in the court system, which enables relatively swift and effective processing of cases through to a conclusion, with a high conviction rate of more than 90%.

**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.**

52. It is well established in the criminological literature that gaol has an incapacitation effect on criminals and consequently prevents specific criminals from committing further crimes while they are incapacitated in prison. However, a key element of the deterrent effect of gaol is the speed with which a case is brought, guilt ascertained, and punishment administered. Therefore, while longer sentences can play a role in increasing the cost of committing crime (which is important when

---

<sup>18</sup> [ARCHIVED CONTENT] Criminal Courts Review (nationalarchives.gov.uk)

<sup>19</sup> bringtobook (fraudadvisorypanel.org)

<sup>20</sup> [ARCHIVED CONTENT] Criminal Courts Review (nationalarchives.gov.uk)

<sup>21</sup> (PDF) A MODEL FOR JUSTICE DELIVERY? The Specialised Commercial Crime Court (researchgate.net)

criminals make their calculations as to the potential risks and benefits of perpetrating a crime) these should not be seen in isolation. Rather, sentence length should be seen as one part of several elements that are interconnected, with speed being just as important.

53. Nevertheless, the comparatively short sentences that are often given out for committing fraud offences have been seen as a problem for many years by observers of this policy space. Professor Mark Button and others pointed out the deficiencies in sentencing as long ago as 2012.<sup>22</sup> A relatively easy change for policymakers to make would be to increase the penalties associated with being convicted of committing fraud and associated offences such as cyber-crime. Further, any enhanced approach to sentencing for existing offences must be reflected in the penalties associated with any new offences created under the review of the criminal law proposed earlier in this submission, too.

54. Another element that will need to be considered by policymakers is the implication of swifter justice and longer sentences on the prison estate and the demand for prison places. Therefore, additional prison places will likely be needed to accommodate more criminals being incarcerated for longer. If other policies result in more frauds being solved and consequent arrests and convictions of perpetrators, then additional places on gaols will be needed. Therefore, any recommendations for an improved law enforcement response, swifter criminal justice processes and longer sentences that are likely to increase the "clear-up" rate need to be considered in the context of the knock-on effects such development are likely to have.

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

55. The one policy that would make the most difference, in our view, would be to ensure police human resourcing more closely matched the scale and complexity of the crime threats to society. More specifically, this requires a substantial expansion of the human resources dedicated to tackling economic crimes like fraud and other associated criminality such as cyber and organised crime. Specifically, this will involve the recruitment of at least 30,000 new police and expert civilian staff specifically employed and trained to pursue perpetrators of these more complex crimes.

*21 April 2022*

---

<sup>22</sup> Microsoft Word - Main Report for Publication July 2012bw