National Economic Crime Centre – Written evidence (FDF0044)

The National Economic Crime Centre (NECC) was created to deliver a step change in the UK's response to, and impact on, economic crime including Fraud. The NECC brings together law enforcement and justice agencies, government departments, regulatory bodies and the private sector with a shared objective of driving down serious organised economic crime, protecting the public and safeguarding the prosperity and reputation of the UK as a financial centre.

The NECC is responsible for coordinating and tasking the UK's response to economic crime, harnessing intelligence and capabilities from across the public and private sectors to tackle economic crime in the most effective way. We work with partners from across the public, private and third sectors to pursue serious and organised fraudsters, make individuals and businesses more resilient to fraud and other economic crimes, and, wherever possible, to return funds to victims.

It will jointly identify and prioritise the most appropriate type of investigations, whether criminal, civil or regulatory to ensure maximum impact. It will seek to maximise new powers, for example Unexplained Wealth Orders and Account Freezing Orders, across all agencies to tackle the illicit finance that funds and enables all forms of serious and organised crime.

The NECC will ensure that criminals defrauding British citizens, attacking UK industry and abusing UK financial services are effectively pursued; that the UK's industries and government agencies know how to prevent economic crime; and that the UK's citizens are better protected.

The NECC is hosted within the National Crime Agency (NCA) and includes officers or representatives from a number of other member agencies including the Serious Fraud Office (SFO), City of London Police (CoLP), HM Revenue & Customs (HMRC), the Crown Prosecution Service (CPS), the Financial Conduct Authority (FCA) and the Home Office (HO).

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 Fraud is the largest crime type (estimated at around 40% of all crime) and it is increasing. Over 3.7 million UK citizens were victims of fraud last year, with an estimate that fraud against the individual costs the UK around £4.7bn a year [1.] The threat from fraud is growing as we spend more time online and technology advances. Globally, the UK is disproportionately targeted by criminals engaged in fraud due to widespread use of English as a second language and the high uptake of digital banking and shopping in the UK, accelerated by Covid.

1.2 There are many factors that impact on fraud harm and therefore all these need to be considered in order to accurately assess and

[1] Home Office, Economic Crime Plan, 2019 to 2022, Policy Paper

prioritise fraud types. The National Fraud Intelligence Bureau (NFIB) assessment uses an established UKLE model to assess fraud risks. This considers the impact of the crime such as victim, financial, community, moral and organisational impact and compares this to the likelihood of offences using volume and frequency of offending.

1.3 For the financial year to March 2021, the NFIB assessment[2] identified the highest harm priority frauds as payment diversion, investment, romance, cheque, plastic card and online bank account, courier and computer software service fraud:

Fraud Types	**Financial Year – April 2020 to March 2021**		
	Total Loss (m)	**No. of Reports**	**Calculated Average Loss[3] (=Total Loss/No. of reports)**
Payment Diversion Fraud	£145.7	4,681	£31,126
Investment Fraud	£317.7	12,228	£25,981
Romance Fraud	£73.9	7,754	£9,531
Cheque, Plastic Card and Online Bank Account	£183.9	27,773	£6,622
Courier Fraud	£14.1	3,266	£4,317
Computer Software Service Fraud	£22.1	18,811	£1,175

1.4 Within these fraud types the victim-base will vary depending on the specific fraud. All fraud can cause harm; individual victims suffer psychological and financial impacts, which can be particularly significant for some personal frauds such as romance fraud. Continued fraud against businesses undermines their customer and wider public confidence.

1.5 In 20/21 there was a change in the ratio of individual victims to business victims reporting to Action Fraud, with victims being individuals increasing to 90% from 86%. The reason for this is not fully known but could be due to the impact of the pandemic lockdown

[2] National Fraud Intelligence Bureau (NFIB), Annual Assessment 2020-2021, Assessment of the threat posed to the UK from fraud.

[3] The calculated average loss is the total loss divided by the number of reports. This includes reports were no loss was recorded.

with many businesses not operating at full capacity and many more people working remotely.

1.6 An estimated 80% of fraud reported nationally continues to be digitally enabled, with social media and online communications platforms being exploited by criminals to enable fraud. Social and economic changes related to the Covid-19 pandemic, including greater reliance on online services, will likely persist. It is anticipated that a higher proportion of fraud will become digitally enabled, with criminals continuing to adapt technologically.

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 noted above digital fraud is estimated to account for 80% of all fraud.

The last 20 years has seen a number of new technologies become entrenched in day-to-day life for most people. Improving computer technology, internet accessibility, the introduction of smartphones and the rise of social media have all coincided and are commonly agreed to be correlated with the drastic increase in reported fraud. Looking forwards, the increasingly likely adoption of virtual assets, block chain technologies and the Metaverse provide further opportunities for new types of frauds.

2.2 Consequently, the role of technology and tech companies designing out vulnerabilities is critical. For example, multi factor authentication including the use of Biometrics is a vital defence against fraud. This is to ensure that only genuine users are accessing their accounts or services. This includes increased use of facial and fingerprint biometrics, alongside voice, linguistic and behavioural biometrics. This will improve safeguards, particularly in the financial services sector. Although, the use of such technologies is still relatively nascent, criminals are already having to adapt how they operate.

2.3 As criminals adapt to an increasingly hostile environment this may drive focus onto the consumer as the weakest link in the chain. There has been an increase in Authorised Push Payment (APP fraud) in which criminals seek to have the individual/victim access their financial accounts and divert funds to the criminal, overcoming the authorisation controls.

2.4 A Public-private partnership which can itself adapt quickly to the evolution of the fraud threat is thus essential in tackling fraud. It is vital that the tech sector and online companies work closely with policy makers and law enforcement to ensure there is an aligned response. In October 2021, the Home Office relaunched the Joint Fraud Taskforce (JFT), chaired by the Security Minister. The JFT includes representation from the tech/online sector. To coincide with the first meeting in October 2021, three new fraud charters were

published (covering the retail banking, telecommunications and accountancy sectors). These commit industry leaders to work with government to deliver projects with the purpose of reducing fraud and protecting the public. The NECC is working in partnership with the private sector to identify vulnerabilities and agree collective initiatives to combat the evolving fraud threat.

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 There is an increased understanding of the scale of fraud in the UK and the harm it can cause. Far from being a victimless crime, the impact on victims can be long lasting.

3.2 It is recognised that there needs to be a better system response to fraud including the law enforcement response. The NECC and its partners, critically the City of London Police, the lead force for Policing, have coordinated several successful projects to disrupt more criminals and understand more about certain high harm threats. Recent funding uplifts will over time enable significantly more to be done.

3.3 Changes in legislation that can help reduce the Fraud threat have also been identified. For example, the NECC has worked with partners to encourage the inclusion of fraud in the draft Online Safety Bill, and specifically paid for advertising. This places a requirement for online platforms to be proactive in stopping fraudulent material from reaching the UK public, as well as removing it when reported. Measures in the recent Economic Crime and Transparency Act and those proposed for follow on legislation, to increase corporate transparency will have a positive impact on the fraud threat. Additional proposals to further facilitate the sharing of information between the private and public sectors are also welcome.

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

4.1 For the year 2021 it is estimated that approximately 23% of fraud is committed by UK based offenders, 47% from offenders in the UK and overseas working together and 30% is committed primarily from offenders overseas. This is based on an evaluation of Action Fraud reporting combined with the known intelligence picture for each fraud type classified by Home Office Code[4]

4.2 International cases are complex and often lengthy due to different priorities, capacity, capability, and legal limitations within each jurisdiction. The NCA continues to make full use of its international

4. An estimate from NFIB and the NCA's National Assessment Centre, 2022.

reach to investigate fraud. The NCA has a significant international liaison capability and overseas presence. It is working closely with international partners to identify the organised crime groups causing the greatest harm to the UK, wherever they may be based.

Action to Tackle Fraud

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 City of London Police as the lead force for fraud are a key partner of the NECC. Their NFIB disseminates triaged packages of Action Fraud crime reports from victims to national police forces, where the majority of national dedicated fraud resources sit.

5.2 The next generation Fraud and Cyber Crime Reporting and Analysis Service (FCCRAS) will make a big difference to this when it comes online as it will improve the NFIB's ability to disseminate simple cases quickly (some instantly) so that they can be actioned in a timely fashion, and better identify networks of criminal fraudsters impacting multiple victims for investigations.

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 The scale and breadth of fraud criminality is challenging for existing resources in law enforcement to significantly impact the threat.

6.2 £400 million of HMG funding has been made available to tackle economic crime including fraud, over the next three years. The NCA will be growing its fraud capabilities and a national police fraud network of specialist fraud investigators across regional and local forces is being built to tackle the threat.

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?**

7.1 The Private sector has a crucial role in protecting against fraud. It is only by the private sector and law enforcement working together with a shared understanding of the threat that we will be able to effectively protect the public.

7.2 The NECC is delivering a strengthened public-private endeavour moving beyond the existing relationship we have with the financial

sector to include the tech sector. This partnership working has been pivotal in delivering actions in the landmark Public Private Economic Crime Plan (ECP). As mentioned, enhanced information sharing is key, and this will only be achieved though closer working, and supported by legislation.

7.3 Generally private sector companies recognise the shared benefits in combatting fraud and although cost can be involved, effective fraud controls can also provide customers reassurance and support growth.

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 Effective and efficient data sharing mechanisms are crucial in the swift and effective investigation of fraud. Data is shared with the NECC/NCA via the Section 7 gateway (Crime & Courts Act 2013), on a voluntary basis.

8.2 The Data Protection Act (DPA) 2018 and the introduction of the UK General Data Protection Regulation (GDPR), specifically with regards to civil liability, has resulted in different risk thresholds impacting the willingness of some organisations to engage in data sharing initiatives.

8.3 The NECC work closely with the Home Office on shaping changes to information sharing legislation.

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 current anti-fraud campaign landscape is relatively crowded albeit the threat is diverse.

9.2 Despite there being some relatively successful campaigns, which have evolved and developed over time, a core challenge in anti-fraud communications remains overcoming consumers' cognitive 'blind spot' when it comes to seeing themselves as a potential victim and getting victims to report fraud (due to shame and lack of belief in the impact). There is perceived to be a clear opportunity for stronger collaboration, partnership and consistency in anti-fraud communications. The NECC is working with partners to identify key messages that will resonate with audiences across the existing landscape.

Legislative Remedies

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 NECC has not identified any significant impediments to the Fraud Act 2006 achieving its objectives.

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 Member agencies of the NECC, specifically the CPS have indicated the potential for a 'failure to prevent fraud' offence, similar to that within the Bribery Act 2010. The NECC supports the consideration of this additional measure which could be a useful tool in preventing fraud through the systemic changes in strengthening internal policies and structures for organisations in response to such a provision.

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 drop in criminal justice outcomes for fraud over the last ten years indicates the wider criminal justice system is not working as effectively as it could to support victims of fraud. The NECC are working closely with the Home Office in delivery of their Fraud Strategy which seeks to make improvements to redress the issues which impact on the outcome.

13. 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.

13.1 The NECC would welcome a review of the sentencing guidelines for fraud offences, the current maximum sentence is not proportionate when one considers other crime types and the victim impact of serious fraud which can result in serious economic and psychological harm.

13.2 We believe the current sentencing does not act as a sufficient deterrent. Criminals committing some of the highest harm frauds where tens of millions are taken from vulnerable members of the public still face less than the maximum 10-year custodial sentence.

Best Practice

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

14.1 Working with member agencies, and through public private partnerships, the NECC helps to identify and test new concepts and initiatives identified to tackle fraud across the '4P' approach of Protect, Prepare, Prevent and Prepare.

14.2 The NECC uses this knowledge to assist the Home Office in identifying and considering different policy inventions that could be applied for fraud through learning from the response to different serious and organised crime threats including money laundering initiatives and cyber crime responses within the UK.

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

15.1 There are a range of policy initiatives that the Home Office are providing that the NECC supports including those referenced earlier such as in relation to data sharing and criminal justice enhancements.

22 April 2022