National Anti-Fraud Network – Written evidence (FDF0055)

This is a joint submission from organisations within the NAFN membership.

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?

The fraudscape has evolved significantly over the past 16 years since the Fraud Act 2006 was introduced, with fraud enabled by the digital transformation of social, business and public sector communications becoming more prevalent.

Individuals are vulnerable to fraud risks and scams as cyber-crimes are extremely relevant via digital channels, such as the internet, email and text. By moving to digital and online, there is an apparent lack of transparency as fraudsters are hidden and borderless, essentially making this type of fraud easier to commit. As IP addresses are not always captured by online submissions it is therefore difficult to prove if the individual submitting the information is as reported.

The Government are also at risk of digital fraud, with schemes and initiatives being targeted, e.g. Covid-19 Grants and the new cost of living council tax rebate and discretionary fund. Fraudsters find creative ways to defraud the public purse, particularly where central and local government are not working in concert. The LGA proposes that local government must recognise the cross boundary nature of fraud, and central government must create the right environment for local authorities to protect public funds by ensuring that the guidance for the administration of this type of fund is clear and robust. Local authorities would see the removal of barriers to information sharing, and a review of the use of powers by local authorities and how they can be harnessed more effectively. Procurement fraud is also an area of significant concern, with an increase in the number of fraud incidents reported during the pandemic – 2020-21 and 2021-22.

Businesses are particularly vulnerable to digital fraud, especially those is the SMB sector. The NCSC has created and promoted content to support businesses to adopt a mind-set of awareness and action, but this needs to be more widely publicised and support offered at local level with strategy and implementation as well as training. A National Minimum Standard in fraud prevention and awareness could be implemented. Charitable organisations and other social health/wellbeing/care providers are soft targets, with the interception of legitimate emails on the rise.

2. What future economic and technological developments are likely to impact how fraudsters seek to commit crime over the next five to ten years?

With constantly developing technology rapidly outpacing current training and cyber-security practices, we are approaching a point at which the need for continuous development and across the board implementation in these areas becomes crucial and, potentially, mandatory.

Online marketplaces, for example, will continue to fall victim to fraud, as they have no accountability for who and what is on their site.

3. How might these be prepared for and mitigated?

Stronger anti-fraud measures and funding could be provided by central government, and through legislation, to support local government intervention to check and evaluate support. Stronger deterrents and consequences are needed to recover losses and public sector organisations could have a fraud clause included in their contract, as within employment laws. A practical example would be where software suppliers should capture IP addresses, the Fraud Act could be amended allowing it to be less onerous for police and public authorities to prove online fraud.

4. What role can technology and tech companies play in combatting fraud across this timescale?

Tech companies and software suppliers can assist in combatting fraud by capturing IP addresses helping to identify or register locations to make users transparent. Linking devices and mobile numbers to addresses and locations would support intelligence gathering under the IPA, and reduce the time taken to build an Intel packet, which can be used to aid prosecution.

5. Is fraud and its victims treated as a priority? If not, what are the reasons for this?

Fraud and victims of fraud are not treated as priorities, as factors such as time, resourcing and the cost to pursue fraudsters are a big loss and cost savings are perceived as more important to most organisation. These factors helps to incentivise fraudsters as they are aware there are little to no comeback or consequences.

6. What is the role of international actors in the UK's fraud landscape?

The role of international actors is to communicate and share intelligence. For example, the International Public Sector Fraud Forum shares best practice in counter fraud with other countries to improve how we prevent, detect and measure public sector fraud.

7. What are the barriers to tackling borderless fraud?

There are many barriers to tackling borderless fraud. These include data protection, and more joined up working could be incentivised here. There tends to be a lack of communication around identifying lead officers or identifying if there is an ongoing investigation. Need to identify from the beginning who and where to be fully transparent.

Connections with other organisations such as Banks need to play a bigger role in regards to tracking where money goes and who is involved. Some good work has been done in this area for example, with National Hunter supporting local authorities in identifying bank accounts belonging to fraudsters during the Covid-19 grant phase.

8. How effective is the current structure for policing fraud?

Ineffective. Policing fraud is not currently a statutory service in the public sector, meaning that not all public sector bodies have counter fraud teams or capabilities. Fraud powers can often be dismissed, as fraud generally relates to money and is not often connected to harm and loss to individuals, therefore fraud is seen to be less important.

9. 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?

To ensure Government organisations and wider police forces can tackle fraud and support victims, fraud could be made a statutory service and grants could be provided by central government to all public bodies to help support them.

Prosecutions are expensive for councils and there is little to no funding for this. Following on, prosecutions are rare as the majority of cases have light sentences and recovering the costs is difficult. There need to be more incentives to bring fraud cases into the court and the public domain.

10. What are the responsibilities of the private sector in protecting the public against digital fraud?

The private sector relies on the General Data Protection Act to protect the public against digital fraud. Transparency is also required with comprehensive communication where there is suspicion and better co-operation with the police. Private sector companies currently do not have to provide information to Authorised Officers for enquiries submitted under the DPA. Perhaps if the requirement to provide information could be compelled under the Fraud Act it would drive awareness and promote more robust and uniform approaches to training, processes and best practice in this sector.

11. To what extent is work done to combat fraud across the private sectors undermined by siloed or independent working practices?

There is insufficient communication through agreed protocols and no incentive to do things the right way. There are also no consequences for fraudsters.

12. What are the legislative or regulatory impediments to sharing fraud risk data across and between the private and public sectors?

    a. For example, to what extent does General Data Protection Regulation (GDPR) limit data sharing?

GDPR makes it very difficult unless there is a specific individual involved where exemptions from the act can be applied. More communication and data sharing should occur in the form of data matching with providers and organisations and this should be regulated when regarding the sharing of information for the purposes of fraud prevention. This communication should be government lead.

13. What is the role of the individual in relation to fraud?

Individuals should not be blamed. More needs to be done to educate the public on the dangers of digital fraud and what to do if they fall victim to such. With wider education, individuals can better protect themselves online and be more aware of the types of communications scammers/fraudsters use. Victims of fraud should be regarded as victims, and treated accordingly, with all allegations of fraud being subject to investigation.

14. 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?

All bodies and organisations need continuous improvement. Regulators such as OFCOM should be mandated to ensure that media platforms promote fraud awareness.

15. What are the most effective methods of educating the public about fraud crime and prevention?

Fraud crime and prevention educations should begin with schools, colleges and universities, so that taking responsibility for personal digital safety becomes the norm. To reach the older generation who are vulnerable to this type of crime and who are not as digitally capable as the younger generation, more promotion is needed via other media, specifically local newspaper, television and radio.

16. What is your assessment of the Fraud Act 2006?

Currently local authorities can and do prosecute for offences under the Fraud Act 2006 but have no Powers to acquire information. It would make sense to have Powers to acquire information specifically for fraud offences under the Fraud Act, as currently prosecuting authorities have to rely on intelligence gathered under DPA and Poshfa, for example. These Powers would compel organisations to assist in inquiries. Powers under the Fraud Act would be especially useful for Trading Standards.

17. What has been the impact of the Act and is it having any unintended consequences; if so, what are these?

The Fraud Act 2006 is considered to be too weighty for lower level fraud. Due to the online move it can be difficult to prove who has made the fraud attempt. It has become far more effective to seek financial gains rather than seek prosecution under the act.

18. Is existing legislation effective in tackling the increase in modern forms of fraud?

    a. If not, is there a legislative remedy, or should fraud be addressed primarily through implementation of existing provisions?

Legislative remedies such as amendments to GDPR and capturing digital information for the purposes of identification and prevention would have considerable impact.

Prosecutions are expensive to bring forward therefore there needs to be stronger incentivised methods of bringing fraud into the public domain. More fines and supported recovery would help support this.

19. Is the current system in place for prosecuting fraud cases working effectively?

    a. If not, what are the key barriers to prosecution?

Key barriers to prosecution include the cost and resources. Prosecution is too expensive for few outcomes, and not cost effective.

20. Are sanctions and penalties for criminals who commit fraud an effective deterrent against future criminal activity, and if not, what might be more successful?

Enforcing the Proceeds of Crime Act (POCA) would help deter criminal and fraudulent activity.

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

Collaboration and the communication of good practice across the fraudscape to ensure that all key stakeholders are consistently applying the same methods and standards.

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

Introduce Authorised Officer Powers to compel data providers including banks, building societies, financial institutions and utility companies to release information in respect of fraud and crime investigations. This must also have an inspection regime, similar to that of IPCO in relation to the IPA, to govern the use of these Powers.

Using and organisation like NAFN with nominated Authorised Officers as a Gateway and Gatekeeper would ensure a single point of access, uniformity, consistency and stringent legal compliance.

22 April 2022