Fighting Fraud and Corruption Locally – Written evidence (FDF0030)

Introduction

This submission is made on behalf of the Fighting Fraud and Corruption Locally Operational Group. The Group was set up in response to a number of recommendations made in the document "Fighting Fraud and Corruption Locally: A Strategy for the 2020s" (being the local government counter fraud strategy for England). The Strategy called on local authorities to work together to illustrate the benefits that can accrue from fighting fraud more effectively. The FFCL Operational Group contains local authority representatives from all of the regional counter fraud networks in operation across England and Wales and is therefore able to receive representation from the majority of councils.

This submission is the result of a consultation process involving the members of the Operational Group and the councils that they represent. The content has been discussed and agreed by the Group prior to submission.

RESPONSES

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. b) for local government, the key risks are serious and organised crime; cyber fraud; application fraud (in relation to benefits, grants and other awards); identity fraud; payroll and payments diversion; procurement (including bribery and corruption); social care (residential care, direct payments).

1.2. Key reasons include: political pressure to make payments quickly; streamlining of processes to improve the "customer experience"; move to online transactions reducing physical contact with applicants/ individuals; lack of effective joint working between local government and central government; lack of formal powers under Fraud Act to require information from organisations or individuals in relation to investigations; lack of effective tools to verify identity of individuals.

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. Increased level of online transactions and applications makes it harder to verify individuals (and their location) and increases opportunities to commit cyber-enabled fraud; more widespread use of crypto currencies increasing money laundering risks; general cyber fraud risks (denial of service, ransomware).

2.2. Mitigations could include better information about online data, for example strength of validation of the individual, verification of geographical location, access to IP addresses for online applications. Tech companies could provide more integrated solutions for online identity verification. There is a high need for investigators to acquire the technical skills to understand the operation and impact of new technologies, and better communication between local authorities, the Police and the NCSC, for example with formal Memoranda of Understanding in place to demonstrate commitment to joint working.

2.3. Better integration of IT systems, both within local authorities and between local authorities and central government, to identify potential fraud at point of entry. Better use of Digital Economy Act powers to analyse and share information across government. Data sharing legislation that applied to data held abroad.

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. No. Often difficult to engage police forces in fraud-related investigations. Joint working, for example with DWP, has declined with many cases being viewed as a matter of compliance rather than fraud. Most resource to support counter fraud work has gone to central government rather than local government, so many councils are unable to make fraud a priority.

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

4.1. Not an area for which there is real intelligence in relation to local government. Some cases relating to organised attempts to defraud COVID grant schemes indicated the involvement of foreign actors. Most risks likely to relate to cyber fraud and cyber-enable fraud.

4.2. Barriers are generally those as identified at Question 2 above, plus the fact that there is little incentive for the financial sector to co-operate with investigations, particularly if money is moved out of the country.

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. Seen as still fragmented – local police forces often lack the resource or skillsets to deal with fraud; mixed picture in relation to Regional Crime Units – some good examples of Memoranda of Understanding, fraud panels, information-sharing between Police, Trading Standards and local authority counter fraud at regional level. Unclear how NFIB influences national activity – often seen as too London-centric.

5.2. Action Fraud seen as unresponsive, acknowledging both that there is a lack of resource to deal with the volumes of referrals, but also that it is important to still make referrals in order to build up the intelligence picture. Would be helpful to know more about how Action Fraud / NFIB score their referrals so that local authorities can understand which cases are more likely to lead to action – examples identified of referrals being made with detailed supporting information included, but returned as having "no identifiable lines of enquiry". Generally felt that in most cases responsibility still rests with the local authority to investigate.

5.3. Mixed experience of making referrals from the COVID grant schemes to NATIS – few requests for further information received in relation to the number of referrals made.

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. Widely acknowledged that it can be difficult to get the police interested in fraud cases – specialist teams are overwhelmed with work and local police often lack a proper understanding of the complexities of fraud cases.

6.2. The length of time taken to deal with cases that the police and CPS do take on is an issue – many councils prefer to do their own prosecutions, so any extension of local authority powers to prosecute would be welcome, coupled with a widening of the scope of summary offences in relevant areas.

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. From a local authority perspective, it is seen as important that the private sector is engaged in a co-ordinated response to fraud, both strategically and operationally (for example via the Home Office Joint Fraud Taskforce)

7.2. Consider incorporating a responsibility to help safeguard against fraud as a required element of companies' corporate governance obligations.

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. GDPR is generally seen as a helpful piece of legislation by adding clarity to what can and cannot be shared and providing defined routes for information-sharing. The main obstacles are:

8.1.1. Lack of understanding by other bodies (including private sector companies) of the permissive elements of the legislation. In some cases, companies are asking authorities to obtain court orders to access information that should be disclosable under GDPR.

8.1.2. A reluctance on the part of some organisations' information governance teams fully to support data sharing initiatives.

8.2. The costs that local authorities have to incur in accessing some data sets required for fraud prevention can also be a barrier – for example to carry out enhanced matches under the National Fraud Initiative. It is unclear where the boundaries lie between these areas and those potentially under the scope of the Digital Economy Act. This area may benefit from a centrally-funded and co-ordinated approach nationally – at present, it is not clear to all local authorities what data-sharing projects are being supported and implemented under the Digital Economy Act powers.

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. Local authorities have broad responsibilities to protect individuals and create safer communities, and Trading Standards teams have specific roles in relation to public protection, which are usually well-publicised. Many Trading Standards Teams have "champions" within the community who can help to spread the message around risks to the individual. Some authorities work in partnership with the Police and other "blue light" services to promote fraud risk awareness and identification.

9.2. Losses incurred by vulnerable or elderly individuals may have an indirect impact on the public purse, for example if someone is scammed out of their life savings and falls into requiring care and support. There is scope to increase the level of awareness of financial safeguarding risks amongst social care staff and others working in this sector – many do not see it as important as other safeguarding risks, or do not engage in financial matters.

9.3. There is a risk here that there may not be a unified, consistent message between local authorities and other law enforcement agencies – at present, Home Office lead on fraud against individuals, and Cabinet Office lead in relation to fraud against the public sector. Who ensures that there is appropriate co-ordination of effort and adherence to best practice?

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. On balance it is seen as positive, particularly in the change in emphasis on proving an intent to gain or cause loss rather than relying on having to prove intention to permanently deprive. The offence of fraud by abuse of position is helpful when positions of trust are involved. The smaller number of offences compared to those in the Theft Act also makes it easier to define a prosecution case.

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. The limitation of the definitions of "gain" and "loss" in the Fraud Act to money or other property prevents local authorities from using the Act more widely, for example to prosecute someone providing false information on residence in relation to schools admissions.

11.2. Local authorities only have a narrow range of specific legal powers in relation to fraud, for example via Council Tax Support Regulations or the Protection of Social Housing Fraud Act. For other areas with significant economic impact, for example business rates, social care assessments or direct payments, there are no requirements to provide correct information or to inform the local authority of any changes in circumstances that would affect eligibility. This can be a significant disincentive to investigate such areas.

11.3. Local authorities have a general power to institute legal proceedings in their own name under s.222 of the Local Government Act 1972, but this is at risk of challenge if used for economic crime cases, as this may not be considered necessarily to meet the requirement under s.222 that the action taken is expedient for the promotion or protection of the interests of the inhabitants of the area.

11.4. In relation to the private sector, tighter verification procedures in areas such as Companies House registration and bank account opening would reduce the risk of bogus individuals or entities entering financial systems.

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

12.1. One of the main barriers is the ability of CPS unilaterally to take over and then drop cases without contacting the local authority.

12.2. Lack of resource is an issue – some councils lack the expertise to gather evidence to support a case, police forces lack capacity, and in some cases, the understanding, to deal with more complex cases. CPS lack capacity to make decisions on cases in a timely manner. Council

staff were being encouraged to join the Government Counter Fraud Profession before the pandemic, but this no longer seems to be a priority, which increases the risk that qualified and experienced counter fraud staff will gravitate towards central government or the private sector. Further investment or support would be welcome, either from government or the private sector, to upskill local authority investigators in how to identify and deal with current fraud risks.

12.3. The extent of either way offences may act as a deterrent to prosecution owing to the potential cost and time delay if a case is referred to Crown Court.

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. There is a lack of sanction options for lower levels of fraud than currently covered by the Fraud Act. The option for councils to impose civil or financial penalties, or other sanctions, is limited to certain areas, for example via The Prevention of Social Housing Fraud Act or the Council Tax Support Regulations.

13.2. Unlawful profit orders (in relation to unlawful subletting of social housing) seen as effective – avoiding the requirement to use Proceeds of Crime Act

13.3. The fact that only a tiny proportion of all estimated economic crime leads to a successful prosecution means that there is unlikely to be a significant deterrent effect. An extension of powers to award fines or civil penalties may produce a greater effect, particularly if they can be issued in a timelier manner.

13.4. More effective intelligence and data sharing between public and private sector bodies, with the possibility for creating a legislative mechanism for doing so, could create a significant deterrent effect, subject to appropriate safeguards being in place to prevent unauthorised or inappropriate use of such.

Best Practice

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

14.1. The Counter Fraud Fund, established by MHCLG in 2014, showed that sustainable improvements could be made to local authority counter fraud capacity by way of targeted investment, but this was a one-off scheme and there has been no follow-up from central government (financially, or by way of policy) to encourage the wider take-up of the more successful schemes. Local government has had to develop its own infrastructure to share best practice, but this has been done without the resource made available to some central government departments.

14.2. Many councils, particularly the smaller ones, lack the resource to support a dedicated counter fraud function. Should consideration be given to supporting the development of regional counter fraud "hubs" to pool councils' resources? Some of the Counter Fraud Fund projects supported such initiatives, often linking in with Trading Standards, local police and Regional Crime Units, but there is no consistent national strategy for this.

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

15.1 An extension of powers of local authorities, to improve the efficiency of investigations. Key areas to enable this would be:

a) An extension of powers to enable local authority Authorised Officers to require the provision of information in relation to suspected offences under the Fraud Act to mirror those in the Protection of Social Housing Fraud Act for example.

b) An extension of the scope of summary offences to enable more cases to be heard in Magistrates' Courts.

c) Additional powers for local authorities to issue fines or civil penalties, similar to those currently available under Council Tax Support legislation, in relation to other services.

21 April 2022