National Fraud Authority

INFORMATION SHARING PROJECT

REPORT ON DATA SHARING FOR THE PREVENTION OF FRAUD UNDER SECTION 68 OF THE SERIOUS CRIME ACT 2007

JULY 2010

CONTENTS

SUMMARY

1. Our informal survey of use of the gateway under section 68 of the Serious Crime Act 2007[1] suggests that there has been a slow start to data sharing under the provision, but there is good evidence of ongoing discussions and work on product development that should produce results both for the public sector and private sector in their fraud prevention capabilities. It is important to appreciate that any good data sharing arrangement, whether under section 68 or otherwise, will take time to develop and agree.

2. Some of the current specified anti-fraud organisations (SAFOs) see specification as a "badge of honour" and, whilst this may be a laudable outcome, we believe that the Home Office should ensure that any future SAFOs set out how they intend to make use of their status for fraud prevention purposes.

3. There is a need for public sector organisations to recognise that there should be a greater emphasis on preventing fraud before it happens instead of detecting fraud after the event. The report of the Smarter Government Public Sector Fraud Taskforce[2] made a number of recommendations in this area and the National Fraud Authority (NFA) is currently drawing up an action plan to take this forward. Recommendations in the report included encouraging the public sector to take up opportunities for data sharing and data matching with the private sector. Data sharing under section 68 is one way of doing this.

4. The 2006 cross-sector data-sharing pilot lends support to the case for data-sharing and CIFAS points to it in support of its position that public sector membership would result in fraud savings. An estimate in the Regulatory Impact Assessment[3] to the Serious Crime Act 2007 put the savings at between £137m and £273m per annum on an assumption that the Departments that participated in the pilot joined. However, CIFAS has not been successful in encouraging Departments to join. To date, CIFAS has focused the majority of its efforts on the benefits of membership to the public sector and less on other arrangements under section 68 to make public sector data available to their members.

5. It is important not to focus exclusively on the big outcomes that could result from data sharing under section 68. The information sharing arrangement with the Ministry of Justice secured by the Insurance Fraud Bureau (IFB) is a good example of use of the gateway to improve operational outcomes. We believe that there is potential for

[1] 2007 c.27.
[2] A Fresh approach to combating fraud in the Public Sector, the Report of the Smarter Government Public Sector Fraud Task Force, March 2010.
http://www.attorneygeneral.gov.uk/nfa/WhatAreWeSaying/NewsRelease/Documents/A%20fresh%20approach%20to%20combating%20fraud%20in%20the%20public%20sector%20doc.pdf
[3] Paragraph 36, Regulatory Impact Assessment, Serious Crime Bill.
http://webarchive.nationalarchives.gov.uk/20100418065544/http://www.homeoffice.gov.uk/documents/Serious-Crime-Bill-RIA2835.pdf?view=Binary

operational benefits for intelligence and enforcement activity from arrangements with the enforcement orientated SAFOs which public authorities should explore.

6. The Information Sharing Task Force has set up a number of working groups to look at options for improving public and private sector access to data for fraud prevention purposes. As part of this work we will be looking at options for using a data sharing arrangement under section 68 to facilitate information hubs or platforms hosted by a SAFO which could offer private sector access to public sector data in a secure environment. The SAFOs who are members of the Task Force are all closely involved in taking this work forward. We will also look for other opportunities to build upon the findings of this informal survey as part of our ongoing work.

INTRODUCTION

7. In September 2009 the National Fraud Authority (NFA) established an Information Sharing Task Force of some 25 public and private sector organisations[4] supported by a project team to identify, analyse and work together to remove significant barriers to the exchange of information between the public and private sectors for fraud prevention. In its first 6 months the Task Force and project team identified six discrete obstacles that often prevent data sharing (cultural, competitive, financial, legal, procedural and technical) and over 180 specific data sharing issues and opportunities have been added to an 'Opportunities Register' – a list of the challenges that need to be tackled.

8. One of these opportunities tasked us with looking at the use being made of the new data sharing provision in section 68 of the Serious Crime Act 2007. The "gateway" in section 68 enables public authorities to disclose information for the purposes of preventing fraud under arrangements made with a specified anti-fraud organisation (SAFO). The Home Office specified 6 organisations in October 2008[5]; CIFAS, Experian Limited, Insurance Fraud Investigators Group (IFIG), N Hunter Limited (National Hunter), the Insurance Fraud Bureau (IFB) and the Telecommunications United Kingdom Fraud Forum Limited (TUFF).

9. Four of the six SAFOs (CIFAS, Experian, IFB and National Hunter) sit on the Information Sharing Task Force and reported concerns about the level of use of the gateway. Two large public authorities, the Department of Work and Pensions (DWP) and Her Majesty's Revenue and Customs (HMRC) also sit on the Task Force and hold data which is of interest to many of the SAFOs. They had both been approached by CIFAS, who believed that membership of CIFAS would result in savings to the public sector, but had declined the invitation to join. We undertook to look at the position by holding individual meetings with the six SAFOs and the key data holders who sat on the Task Force to try and get a picture of what was actually happening on the ground.

[4] Current members are: Aviva, British Telecom, Call Credit, Charity Commission, CIFAS, City of London Police, Detica, DWP, Equifax, Experian, HMRC, HSBC, Identity and Passport Service, Information Commissioner's Office, Insurance Fraud Bureau, Lloyds Banking Group, Ministry of Justice, National Anti-Fraud Network, National Fraud Initiative (Audit Commission), National Hunter, RBS, SOCA, Synectics Solutions and UK Cards Association/ Financial Fraud Action UK.

[5] The Serious Crime Act 2007(Specified anti-fraud organisations) Order 2008 (S.I. 2008/2353). http://www.opsi.gov.uk/si/si2008/uksi_20082353_en_1

BACKGROUND

10. The story behind the enactment of the gateway in section 68 of the Serious Crime Act 2007 can be linked to rising concerns about the extent of fraud and the response to fraud in the United Kingdom. The economic and social costs of fraud have been the subject of increasing concern and scrutiny in the last decade. Concern about the impact of serious organised crime and identity crime were also on the agenda and led to the publication of a Home Office Green paper "New Powers Against Organised and Financial Crime"[6]. Recognising that those who defraud the public sector are also likely to target the private sector, the paper contained proposals for legislation that would enable public sector membership of CIFAS, a private sector anti-fraud organisation, and was informed by other government work looking at data sharing under the aegis of the Home Office Identity Fraud Steering Committee (IFSC)[7] which suggested that one of the most efficient ways of reducing identity fraud is for public sector organisations to build on existing private sector data-sharing schemes, such as those operated by Credit Reference Agencies (CRAs) and CIFAS.

11. A cross-sector data-sharing sub-group was set up to investigate data-sharing options for reducing the incidence of impersonation of the deceased fraud and to clarify any legal impediments to data-sharing between the public and private sector. A pilot was set up to match confirmed fraud data from the Driver and Vehicle Licensing Agency (DVLA), Identity and Passport Service (IPS), DWP and HMRC with the CIFAS database. 31%[8] of the addresses provided resulted in a match against an existing record on the CIFAS database, providing support for the Green paper proposition that the same fraudsters were attacking both the public and the private sector. The sub-group also highlighted that legislation would be necessary in order to permit some parts of the public sector to share sensitive personal data with private sector organisations.

[6] New Powers against Organised and Financial Crime, July 2006, Cm 6875.
http://www.official-documents.gov.uk/document/cm68/6875/6875.pdf
[7] http://www.identitytheft.org.uk/committee.asp
[8] Paragraph 34, Regulatory Impact Assessment, Serious Crime Bill.
http://webarchive.nationalarchives.gov.uk/20100418065544/http://www.homeoffice.gov.uk/documents/Serious-Crime-Bill-RIA2835.pdf?view=Binary

THE DATA SHARING PROVISIONS

12. The outcome of the data-matching pilot provided evidence to support the case for public sector membership of CIFAS set out in the Green paper. But the Green paper recommendations went wider, recognising that a legislative solution should not be confined to a membership model and, in consequence, section 68 of the Serious Crime Act 2007 provides a number of options to public authorities who want to disclose information through the gateway.

13. Section 68(1) provides that a public authority may disclose information as a member of a specified anti-fraud organisation (SAFO) or otherwise in accordance with any arrangements made by such an organisation. The wording is capable of supporting a wide range of permutations and arrangements other than membership. Subsection 68(2) makes clear that the information disclosed may be of any kind and, significantly, may be disclosed to the SAFO, any members of it or any other person to whom disclosure is permitted by the arrangements concerned. The section makes it explicit that disclosure does not breach any obligation of confidence owed by the public authority disclosing the information or any other restriction on the disclosure of information (however imposed) but nothing in the section authorises any disclosure of information which contravenes the Data Protection Act 1998 (DPA) or is prohibited by Part 1 of the Regulation of Investigatory Powers Act 2000 (RIPA).

14. An anti-fraud organisation is defined as any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes, specified means specified by an order made by the Secretary of State and “public authority" means any public authority within the meaning of section 6 of the Human Rights Act 1998 (HRA).

15. Section 69 (1) makes it an offence to further disclose revenue and customs information which reveals the identity of the person to whom it relates.

16. Section 70 sets out the penalties for an offence under section 69 and provides that a prosecution may only be commenced following consent of the Director of Public Prosecutions. The Green paper recognised the importance of ensuring that arrangements made were DPA compliant and section 71 makes provision for the preparation of a Code of Practice by the Secretary of State.

17. The Code of Practice[9] laid before Parliament in October 2008 provides high level guidance to public authorities and sets out some broad principles and considerations for participants in data sharing arrangements under section 68. It is intended to complement good data sharing policy and practice already in existence in public authorities. It is also notable that information sharing arrangements made under section 68 are subject to audit by the Information Commissioner's Office (ICO). This follows an undertaking given by the Home Office during the passage of the Bill.

18. Section 72 inserts a new paragraph in Schedule 3 to the Data Protection Act 1998 to allow processing of sensitive personal data through an anti-fraud organisation. The processing must be necessary for the purposes of preventing fraud. The provisions are set out in full as enacted in **Appendix 1**.

[9] Data Sharing for the Prevention of Fraud, Code of Practice for public authorities disclosing information to a specified anti-fraud organisation under sections 68 to 72 of the Serious Crime Act 2007. http://www.whatdotheyknow.com/request/2971/response/7150/attach/3/12761_290510%20Data%20Sharing.pdf

THE SPECIFIED ANTI-FRAUD ORGANISATIONS

19. The data sharing provisions in sections 68-72 and the Order specifying the 6 anti-fraud organisations came into force on the 1st October 2008. Six organisations were specified; CIFAS, Experian Limited, Insurance Fraud Investigators Group (IFIG), N Hunter Limited (National Hunter), the Insurance Fraud Bureau (IFB) and the Telecommunications United Kingdom Fraud Forum Limited (TUFF).

CIFAS

20. CIFAS[10] is a not for profit data sharing scheme with in the region of 260 members spread across the banking, credit cards, asset finance, retail credit, mail order, insurance, savings and investments, telecommunications, factoring, and share dealing sectors in the United Kingdom. Members can post details of a fraud on the CIFAS database where there is sufficient evidence to press criminal charges. The annual CIFAS membership fee is based on a number of factors including the turnover of the organisation and ranges from £5,000 - £6,000 for smaller organisations to £166,000 for the largest organisations.

21. CIFAS told us that it lobbied for the creation of a gateway to overcome the legal impediments to membership encountered by some parts of the public sector which became apparent following the IFSC data matching exercise. CIFAS therefore strongly welcomed the introduction of section 68 of the Serious Crime Act 2007 and had high hopes following its subsequent designation as a SAFO by the Home Office. The hope was that, by establishing an explicit and clear legal gateway, public sector organisations would be keen to realise the potential financial benefits by sharing their information about frauds with organisations like CIFAS. The experience of CIFAS in exploring potential membership with many types of public sector organisations is that the legal gateway itself is unambiguous. Although it felt that awareness of the new powers was low, once the details of the gateway were explained most organisations could see the potential benefits that could result from membership of CIFAS.

22. CIFAS is currently engaged in some promising discussions with a range of local and national public sector organisations but the progress envisaged after the creation of the legal gateway has not materialised. This is particularly the case with respect to efforts by CIFAS to get interest in membership from the larger central government departments. CIFAS was pleased to confirm to us that the Legal Services Commission (LSC) is the first public sector organisation to make use of the provisions in section 68 SCA to join CIFAS, and will soon be in a position to start using fraud data from the CIFAS database

[10] http://www.cifas.org.uk/

and, in turn, sharing data about frauds committed against legal aid funds. Good progress has also been made in discussions with the UK Border Agency (UKBA) and work is underway to take this forward. Whilst CIFAS has concentrated most of its efforts on promoting membership it told us that it has been successful in obtaining and sharing confirmed fraud risk data from two public sector organisations.

EXPERIAN

23. Experian[11] is a global information services company which provides data and analytical tools to clients in the United Kingdom and internationally. As a Credit Reference Agency (CRA) it helps businesses to manage credit risk, prevent fraud, target marketing offers and automate decision making. Experian also provides services to individuals to check their credit report and credit score. The Experian consumer database holds information on 45 million UK customers and the Autocheck database holds live data on 31 million vehicles and over 90 million DVLA registration records. Experian has been working with the public sector for over 20 years and its client list includes major government departments, over 70 per cent of UK local authorities, regional development agencies, strategic health authorities, primary care trusts, acute trusts, police forces and fire and rescue services.

24. Following publication of the Home Office Green Paper, Experian lobbied strongly for a legislative solution wider than the proposed membership model which was primarily aimed at CIFAS. However, when we spoke to Experian in February 2010, although there had been discussions with some public authorities, it had not secured any data sharing arrangements under section 68.

25. When we met again in May 2010 it was clear that matters had moved on. Experian told us that discussions were underway with a Local Authority in London about data matching with Experian to counter social housing tenancy fraud. Experian is hopeful that progress will be made on this work and it sees the gateway in section 68 as providing key assurance that the disclosure of information to Experian by local authorities can be made lawfully. Experian believes that public/private data matching between a group of, firstly, London based authorities could be the first stepping stone towards the transformation of data sharing against fraud in the public sector at large. Experian told us that it is actively researching development with similar potential across many other areas of the public sector.

[11] http://www.experian.co.uk/

TELECOMMUNICATIONS UK FRAUD FORUM (TUFF)

26. TUFF[12] was established in 2000 and is a "not for profit" organisation which acts as a forum for the exchange of information and the promotion of a united effort against telecommunications fraud. Members come from a variety of backgrounds but are primarily telecommunication fraud professionals and fraud analysts. TUFF acts as a central point to enable information on telecommunications fraud to be shared across the industry and as an industry point of contact for law enforcement and other agencies for matters concerning telecommunication fraud. Members exchange information using the protocols established under the UK National Intelligence Model (sometimes referred to as the 5x5x5 system) used by police and other law enforcement bodies.

27. TUFF told us that it views its status as a SAFO as a "badge of honour" and has highlighted it on the front page of the TUFF website. There had been no disclosures of information to TUFF under section 68 and it was not actively pursuing any. TUFF acknowledged that the gateway would enable fraud investigators in some central Departments, HMRC for example, to join to share intelligence with TUFF members but this has not been pursued by TUFF.

INSURANCE FRAUD INVESTIGATORS GROUP (IFIG)

28. IFIG[13] is a non-profit making organisation created to tackle the growing problem of insurance fraud in the UK. There are currently over 250 members from the insurance industry and others such as lawyers, loss adjusters and independent insurance fraud investigators. Applications from persons other than insurers must be sponsored by an insurer. This wider private sector membership base distinguishes it from the IFB as does the wide membership from law enforcement such as police financial intelligence and regional intelligence units, the Financial Services Authority (FSA), UKBA, Fire Service investigation units and local authority intelligence units. Other members include the Solicitors Regulatory Authority (SRA), the British Bankers Association (BBA) and CIFAS. IFIG has also had recent discussions on membership with the Serious Organised Crime Agency (SOCA).

29. IFIG operates an online Fraud Forum and receives and disseminates e-alerts on confirmed and suspected fraud (at 128 SSL Security) across its membership community. The alert facility is modelled on the National Intelligence Model 5x5x5 system and compliance with that model is policed by IFIG. Membership is based on reciprocity and an understanding that members will post alerts in addition to benefitting from those posted by others. It is possible to filter postings to restrict access to certain categories of member.

[12] http://www.tuff.co.uk/home.asp
[13] http://www.ifig.org/

30. On confirmation of IFIG's specification for the purposes of section 68, IFIG Chairman Peter Upton said:

    "We are delighted to be awarded this status by the Home Office and look forward to building on our relationships with the public sector. We know fraudsters involve themselves in many aspects of criminality and we are very keen to disrupt them by working closely with other organisations.

    IFIG now has over 250 company members covering the vast majority of the insurance industry and insurance fraud investigators. We already have close links with many law enforcement agencies and the additional relationships with other public bodies is a great opportunity to work together."[14]

31. When we met in March 2010 IFIG told us that there had been no uptake of membership from public authorities who would need to use the section 68 gateway to join IFIG nor had it identified or actively pursued this with any prospective members. The position had not changed when we contacted IFIG again in June 2010. However, IFIG believes that its SAFO status has helped its credibility in negotiations with prospective members from the public sector and has given it greater credibility with police and fire service investigators.

INSURANCE FRAUD BUREAU (IFB)

32. IFB[15] was formed in 2006 to provide a cost effective, tactical solution for the detection and prevention of organised, cross industry insurance fraud to complement the wider Association of British Insurers (ABI) and industry fraud strategy. It is non-profit making. IFB's work on investigations is supported by close relationships with police and other law enforcement agencies. It acts as a co-ordinating point for investigations into potential frauds between insurers, to establish if insurance claims are likely to be fraudulent and require further investigation. IFB can access a number of databases, for example the Motor Insurance database and uses data matching and analytical techniques to identify potential fraud. Supplementary data is sourced directly from participating insurers to build a detailed intelligence picture.

33. IFB told us that the range of organisations specified by the Home Office is curious. They are all quite different with their own distinct aims and contrasting membership pools. IFB has been successful in securing a memorandum of understanding (MoU) with the Ministry of Justice to share data under section 68 on 'cash for crash' staged accidents. The IFB and the Ministry of Justice Claims Management Regulation Unit

[14] http://www.ifig.org/
[15] http://www.insurancefraudbureau.org/

identified that they had a mutual interest in sharing information to assist each organisation undertake their respective roles. Since the Information Sharing Agreement was signed in March 2009, they have held regular intelligence sharing meetings, created and utilised an intelligence sharing framework and jointly co-operated in multi task force approaches to a number of law enforcement operations.

34. IFB would like to secure similar arrangements with HMRC, DWP and DVLA and are engaged in ongoing discussions with all three but, as yet, has no concrete results to report.

N HUNTER Limited (National Hunter)

35. The National Hunter[16] system is an anti-fraud data sharing system for use by members of the financial services industry. It was founded in 1993 and there are now approximately 90 member organisations sharing application information for the purposes of fraud prevention. Members submit details of applications that they receive for products such as mortgages, credit cards and loans which are checked against existing applications using a predefined set of rules. Any applications that warrant investigation are referred for further checks and may be declined by the lender where fraud is suspected. Additionally, information on anomalies flagged is shared amongst members for the purposes of fraud prevention. National Hunter also receives intelligence reports from members, the SRA and the FSA. It shares intelligence with law enforcement on a case by case basis with permission from the organisation who posted the information.

36. National Hunter told us that section 68 was brought to its attention by the FSA and it immediately saw the potential benefit of specification as an anti-fraud organisation to its members. It believed that specification as a SAFO would offer "comfort" to public authorities and encourage them to disclose data. When we met in February 2010, National Hunter had not actively pursued any opportunities for sharing under section 68 with any public authority but it is hopeful that this may change in light of the work being taken forward by the Information Sharing Task Force on section 68 which is discussed further below. It has also recently made contact with HMRC to take forward a discussion of the potential for information sharing on a case by case basis.

[16] http://www.nhunter.co.uk/

THE PUBLIC AUTHORITIES

37. We met with officials from HMRC and DWP to hear their perspective on the gateway in section 68.

38. HMRC told us that it was not involved in the formulation of policy for the legislative proposals which resulted in the enactment of section 68. However, it was successful in securing the restrictions on onward disclosure of Revenue and Customs information and the offence of wrongful disclosure in sections 69 and 70 of the 2007 Act. These were important to HMRC as it is HMRC policy that all confidential information supplied to a third party, such as information revealing a person's identity or from which identity could be deduced, should be subject to a restriction on onward disclosure and that wrongful disclosure should be the subject of a specific criminal offence. When we saw HMRC in February 2010 it told us that CIFAS had been the only SAFO that had approached HMRC with any proposals to disclose information under section 68.

39. HMRC has received several approaches from CIFAS to consider becoming a member of CIFAS. HMRC told us that each request was reviewed in terms of its potential benefits, legal and policy considerations and operational impacts but the case for HMRC membership had not been persuasive. HMRC acknowledged that the 2006 cross-sector data-matching pilot produced some interesting results but it suggested that further detailed analysis of these results would need to be done to establish the potential benefit of CIFAS data to both HMRC and wider government. HMRC also pointed out that it was not necessary for it to become a member of CIFAS in order to disclose HMRC information to them under section 68. Nor was it necessary for HMRC to join CIFAS to obtain information from them. HMRC told us that it is always happy to consider data sharing requests from both public and private sector organisations on an individual case by case basis.

40. HMRC gave us a number of examples of situations where it has disclosed information to SAFOs. But the disclosures were made using HMRC's main statutory gateway in section 18(2) of the Commissioners for Revenue and Customs Act 2005[17] (CRCA) and not by way of section 68. For example, it disclosed information to the IFB in December 2009. This gateway was appropriate because the disclosure occurred in the context of an HMRC criminal investigation and was made in furtherance of HMRC business needs. HMRC emphasised that it will consider any request made to it by a SAFO and will determine whether there is a gateway through which the information may be disclosed, including section 68. As is the case for any request for information it is important for the requester to explain why they need the information and HMRC would expect that to be made plain to assist

[17] Commissioners for Revenue and Customs Act 2005 (c.11).http://www.opsi.gov.uk/acts/acts2005/ukpga_20050011_en_2#pb4-l1g18

in determining whether and how it might assist. Sometimes disclosure of the information will not only be of benefit to the requester but also to HMRC and, in those circumstances, HMRC may be able to use one of its own gateways, such as section 18(2) CRCA, and would therefore not need to go on to consider alternatives such as section 68.

41. DWP told us that CIFAS approached it on a number of occasions, most recently in January 2010, inviting it to consider CIFAS membership. DWP has considered the matter at meetings with CIFAS but has concluded that there is no case for membership or clear benefit to DWP from use of CIFAS data. DWP emphasised that it remains open to and will give due consideration to requests from any SAFO who has a data sharing proposal to put to DWP. There have been discussions with IFB and a workshop is planned to see how DWP might help them.

CONCLUSIONS

42. We concluded our informal survey of data sharing under section 68 by meeting the current Home Office policy lead on the gateway and the policy lead at the time the Serious Crime Bill was in preparation. The initial idea for a gateway came from the 2006 Green Paper[18]. The Home Office was lobbied by CIFAS and had a number of meetings with Departments to see if individual fixes were possible. There was little enthusiasm for individual Departmental fixes to the legal vires to share data with the private sector and that resulted in the "open sesame" approach adopted for the gateway in terms of the public authorities that could make use of it.

43. Following Royal Assent the Home Office sent out a note inviting applications for specification as an anti-fraud organisation from regular fraud contacts and wrote to Departments to advise them that the gateway was in place. The Home Office does not see it as part of its remit to monitor use of the gateway or to encourage SAFOs to make cases to public authorities for data sharing. At the time of the passage of the Serious Crime Bill it felt confident that public authorities would look favourably at the opportunities for joining and entering into arrangements with SAFOs that the gateway can facilitate. It held a meeting with the six SAFOs in 2009 and it was clear that all were disappointed at the lack of progress. The Home Office also told us that it had no current plans to extend the list of SAFOs, albeit it was aware of interest from a number of organisations.

44. Section 68 is a very wide gateway and should be viewed as a legal facilitator which provides a framework for lawful sharing for fraud prevention by public authorities who would otherwise have no lawful means of disclosing data to private sector organisations. The width of the gateway offers opportunities for a range of options which, it is suggested, should suit the requirements of most organisations. So, why has uptake of the opportunity for data sharing been slow? Our conclusion is that it is a combination of a lack of awareness of the gateway and what it can facilitate and, perhaps more significantly, a degree of hesitation on part of public authorities. This is not surprising given the history of recent data losses in the public sector and the private sector[19] and there is, we suggest, a resulting and understandable nervousness about sharing sensitive personal information outside the usual parameters.

45. Some private sector organisations believe that these recent events have made the public sector less inclined to share data even when they may lawfully do so, especially post the Poynter Review[20] (which

[18] See note 6 to paragraph 10 for reference.
[19] Data Sharing Review Report, Thomas, R. and Walport, M., 11 July 2008 http://www.justice.gov.uk/docs/data-sharing-review-report.pdf
[20] Review of information security at HM Revenue and Customs. Poynter, K., June 2008. http://www.hm-treasury.gov.uk/media/0/1/poynter_review250608.pdf

reported on and made recommendations following the HMRC data loss). We were also told that reciprocity does not work well between the private and public sectors. We do not believe that a lack of reciprocity is at the root of the problem. Both HMRC and DWP made clear to us that they were willing to share data where there was a case for doing so and where they were lawfully able to do so. Often, the challenge for the public sector is the absence of a legal gateway to share data or statutory restrictions on who they can share with and, increasingly, the absence of a specific statutory gateway will prevent the disclosure of sensitive personal information. It is exactly this sort of problem that the creation of the gateway in section 68 was intended to get round.

46. The DPA requires personal information to be processed fairly, lawfully and in a way not incompatible with the purposes for which it was collected. Data sharing under section 68 should only be undertaken to the extent that it is necessary and proportionate for fraud prevention. It will, therefore, always be important for SAFOs to be in a position to present a business case to public authorities in support of any data sharing proposal setting out why the data is required. Even with an excellent business case to share data, the key to any arrangement will be a relationship based on mutual trust. SAFOs should recognise that the concept of sharing data in a commercial environment, albeit for the purposes of fraud prevention, can create nervousness in the public sector, particularly about the security and control of onward use of data after it has been shared.

LOOKING FORWARD

47. Our informal survey of use of the gateway suggests that there has been a slow start to data sharing under section 68 but there is good evidence of ongoing discussions and work on product development that should produce results for both the public sector and private sector in their fraud prevention capabilities. It is important to appreciate that any good data sharing arrangement, whether under section 68 or otherwise, will take time to develop and agree.

48. Some of the current SAFOs see specification as a "badge of honour" and, whilst this may be a laudable outcome we believe that the Home Office should ensure that any future SAFOs set out how they intend to make use of their status for fraud prevention purposes.

49. There is a need for public sector organisations to recognise that there should be a greater emphasis on preventing fraud before it happens instead of detecting fraud after the event. The report of the Smarter Government Public Sector Fraud Taskforce[21] made a number of recommendations in this area and NFA is currently drawing up an action plan to take this forward. Recommendations in the report included encouraging the public sector to take up opportunities for data sharing and data matching with the private sector. Data sharing under section 68 is one way of doing this.

50. The 2006 cross-sector data-sharing pilot lends support to the case for data-sharing and CIFAS points to it in support of its position that public sector membership would result in fraud savings. An estimate in the Regulatory Impact Assessment[22] to the Serious Crime Act 2007 put the savings at between £137m and £273m per annum on an assumption that the Departments that participated in the pilot joined. However, CIFAS has not been successful in encouraging Departments to join. To date, CIFAS has focused the majority of its efforts on the benefits of membership to the public sector and less on other arrangements under section 68 to make public sector data available to their members.

51. It is important not to focus exclusively on the big outcomes that could result from data sharing under section 68. The information sharing arrangement with the Ministry of Justice secured by IFB is a good example of use of the gateway to improve operational outcomes. We believe that there is potential for operational benefits for intelligence and enforcement activity from arrangements with the enforcement orientated SAFOs such as IFB, IFIG and TUFF which public authorities should explore.

---

[21] A fresh approach to combating fraud in the public sector, The Report of the Smarter Government Public Sector Fraud Taskforce, March 2010.
http://www.attorneygeneral.gov.uk/nfa/WhatAreWeSaying/NewsRelease/Documents/A%20fresh%20approach%20to%20combating%20fraud%20in%20the%20public%20sector%20doc.pdf

[22] Paragraph 36, Regulatory Impact Assessment, Serious Crime Bill.
http://webarchive.nationalarchives.gov.uk/20100418065544/http://www.homeoffice.gov.uk/documents/Serious-Crime-Bill-RIA2835.pdf?view=Binary

52. The Information Sharing Task Force has set up a number of working groups to look at options for improving public and private sector access to data for fraud prevention purposes. As part of this work we will be looking at options for using a data sharing arrangement under section 68 to facilitate information hubs or platforms hosted by a SAFO which could offer private sector access to public sector data in a secure environment. The SAFOs who are members of the Task Force are all closely involved in taking this work forward. We will also look for other opportunities to build upon the findings of this informal survey as part of our ongoing work.

APPENDIX 1

SECTIONS 68-72
SERIOUS CRIME ACT 2007

PART 3

OTHER MEASURES TO PREVENT OR DISRUPT SERIOUS AND OTHER CRIME

CHAPTER 1

PREVENTION OF FRAUD

Sharing information with anti-fraud organisations

68 Disclosure of information to prevent fraud

(1) A public authority may, for the purposes of preventing fraud or a particular kind of fraud, disclose information as a member of a specified anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation.

(2) The information—

(a) may be information of any kind; and

(b) may be disclosed to the specified anti-fraud organisation, any members of it or any other person to whom disclosure is permitted by the arrangements concerned.

(3) Disclosure under this section does not breach—

(a) any obligation of confidence owed by the public authority disclosing the information; or

(b) any other restriction on the disclosure of information (however imposed).

(4) But nothing in this section authorises any disclosure of information which—

(a) contravenes the Data Protection Act 1998 (c. 29); or

(b) is prohibited by Part 1 of the Regulation of Investigatory Powers Act 2000 (c. 23).

(5) Nothing in this section authorises any disclosure by a relevant public authority of information whose subject-matter is a matter about which provision would be within the legislative competence of the Scottish Parliament if it were included in an Act of that Parliament.

(6) In subsection (5) “relevant public authority” means a public authority which has (whether alone or in addition to other functions) functions which are exercisable within devolved competence (within the meaning given by section 54 of the Scotland Act 1998 (c. 46)).

(7) This section does not limit the circumstances in which information may be disclosed apart from this section.

(8) In this section—

"an anti-fraud organisation" means any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes;

"information" includes documents;

"public authority" means any public authority within the meaning of section 6 of the Human Rights Act 1998 (c. 42) (acts of public authorities); and

"specified" means specified by an order made by the Secretary of State.

69 Offence for certain further disclosures of information

(1) A person ("B") commits an offence, subject as follows, if—

(a) B discloses protected information which has been disclosed by a public authority—

(i) as a result of the public authority being a member of a specified anti-fraud organisation; or

(ii) otherwise in accordance with any arrangements made by such an organisation;

(b) the information—

(i) has been so disclosed by the public authority to B; or

(ii) has come into B's possession as a result (whether directly or indirectly) of such a disclosure by the public authority to another person; and

(c) B knows or suspects, or has reasonable grounds for suspecting, that the information is information of the kind mentioned in paragraphs (a) and (b).

(2) Subsection (1) does not apply to a disclosure made by B—

(a) where B is acting (whether as an employee or otherwise) on behalf of the person to whom the information was disclosed by the public authority concerned and the disclosure by B is to another person acting (whether as an employee or otherwise) on behalf of that person;

(b) for the purposes of the detection, investigation or prosecution of an offence in the United Kingdom;

(c) with the consent of the public authority concerned; or

(d) in pursuance of a Community obligation or a duty imposed by an enactment; but it does apply to a disclosure made by B which does not fall within paragraphs (a) to (d) above but which (but for the offence) would have been permitted by a power conferred by an enactment.

(3) Subsection (1) does not apply to a disclosure made by B of information—

(a) which has been disclosed by a relevant public authority; and

(b) whose subject-matter is a matter about which provision would be within the legislative competence of the Scottish Parliament if it were included in an Act of that Parliament; and subsection (6) of section 68

applies for the purposes of this subsection as it applies for the purposes of subsection (5) of that section.

(4) It is a defence for a person charged with an offence under this section to prove that the person reasonably believed—

(a) that the disclosure was lawful; or

(b) that the information had already and lawfully been made available to the public.

(5) In this section "protected information" means—

(a) any revenue and customs information disclosed by Revenue and Customs and revealing the identity of the person to whom it relates; or

(b) any specified information disclosed by a specified public authority.

(6) For the purposes of this section—

(a) "revenue and customs information" means information about, acquired as a result of or held in connection with the exercise of a function of the Commissioners of Revenue and Customs or an officer of Revenue and Customs in respect of a person;

(b) revenue and customs information reveals a person's identity if—

(i) it specifies his identity; or

(ii) his identity can be deduced from it; and

(c) revenue and customs information relates to a person if he is the person in respect of whom the function mentioned in paragraph (a) is exercised.

(7) In this section—

"Commissioners of Revenue and Customs" means Commissioners for Her Majesty's Revenue and Customs;"

"enactment" has the same meaning as in section 14;

"public authority" has the same meaning as in section 68;

"Revenue and Customs" means—

(a) the Commissioners of Revenue and Customs;

(b) an officer of Revenue and Customs; or

(c) a person acting on behalf of the Commissioners or an officer of Revenue and Customs;

"specified anti-fraud organisation" means any person which is a specified anti-fraud organisation for the purposes of section 68;

"specified information" means information specified or described in an order made by the Secretary of State; and

"specified public authority" means a public authority specified or described in an order made by the Secretary of State.

70 Penalty and prosecution for offence under section 69

(1) A person who commits an offence under section 69 is liable—
  (a) on summary conviction, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;
  (b) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.

(2) A prosecution for an offence under section 69 may be begun in England and Wales only—
  (a) in the case of revenue and customs information disclosed by Revenue and Customs—
    (i) by the Director of Revenue and Customs Prosecutions; or
    (ii) with the consent of the Director of Public Prosecutions; and
  (b) in any other case, with the consent of the Director of Public Prosecutions.

(3) A prosecution for an offence under section 69 may be begun in Northern Ireland only—
  (a) in the case of revenue and customs information disclosed by Revenue and Customs—
    (i) by the Commissioners of Revenue and Customs; or
    (ii) with the consent of the Director of Public Prosecutions for Northern Ireland; and
  (b) in any other case, with the consent of the Director of Public Prosecutions for Northern Ireland.

(4) If an offence under section 69 committed by a body corporate or a partnership is proved to have been committed with the consent or connivance of—
  (a) an officer of the body corporate or (as the case may be) a partner or a senior officer of the partnership; or
  (b) a person who was purporting to act in any such capacity; he (as well as the body corporate or partnership) is guilty of the offence and liable to be proceeded against and punished accordingly.

(5) In the application of subsection (1)(a) in Northern Ireland, the reference to 12 months is to be read as a reference to 6 months.

(6) In this section—
  "body corporate" includes a limited liability partnership;
  "Commissioners of Revenue and Customs", "Revenue and Customs" and "revenue and customs information" have the same meaning as in section 69;
  "director", in relation to a body corporate whose affairs are managed by its members, means a member of the body corporate;
  "officer of a body corporate" means any director, manager, secretary or other similar officer of the body corporate; and
  "senior officer of a partnership" means any person who has the control or management of the business carried on by the partnership at the principal place where it is carried on.

71 Code of practice for disclosure of information to prevent fraud

(1) The Secretary of State must prepare, and keep under review, a code of practice with respect to the disclosure, for the purposes of preventing fraud or a particular kind of fraud, of information by public authorities as members of specified anti-fraud organisations or otherwise in accordance with any arrangements made by such organisations.

(2) Before preparing or altering the code, the Secretary of State must consult—

(a) any specified anti-fraud organisation;

(b) the Information Commissioner; and

(c) such other persons as the Secretary of State considers appropriate.

(3) A public authority must have regard to the code in (or in connection with) disclosing information, for the purposes of preventing fraud or a particular kind of fraud, as a member of a specified anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation.

(4) Nothing in this section applies in relation to any disclosure by a relevant public authority of information whose subject-matter is a matter about which Provision would be within the legislative competence of the Scottish Parliament if it were included in an Act of the Scottish Parliament.

(5) The Secretary of State must—

(a) lay a copy of the code, and of any alterations to it, before Parliament; and

(b) from time to time publish the code as for the time being in force.

(6) In this section—

"information" and "public authority" have the same meaning as in section 68;

"relevant public authority" has the meaning given by section 68(6); and

"specified anti-fraud organisation" means any person which is a specified anti-fraud organisation for the purposes of section 68.

72 Data protection rules

In Schedule 3 to the Data Protection Act 1998 (c. 29) (conditions for processing sensitive personal data), after paragraph 7, insert—

"7A (1) The processing—

(a) is either—

(i) the disclosure of sensitive personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation; or

(ii) any other processing by that person or another person of sensitive personal data so disclosed; and

(b) is necessary for the purposes of preventing fraud or a particular kind of fraud.

(2) In this paragraph "an anti-fraud organisation" means any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes."