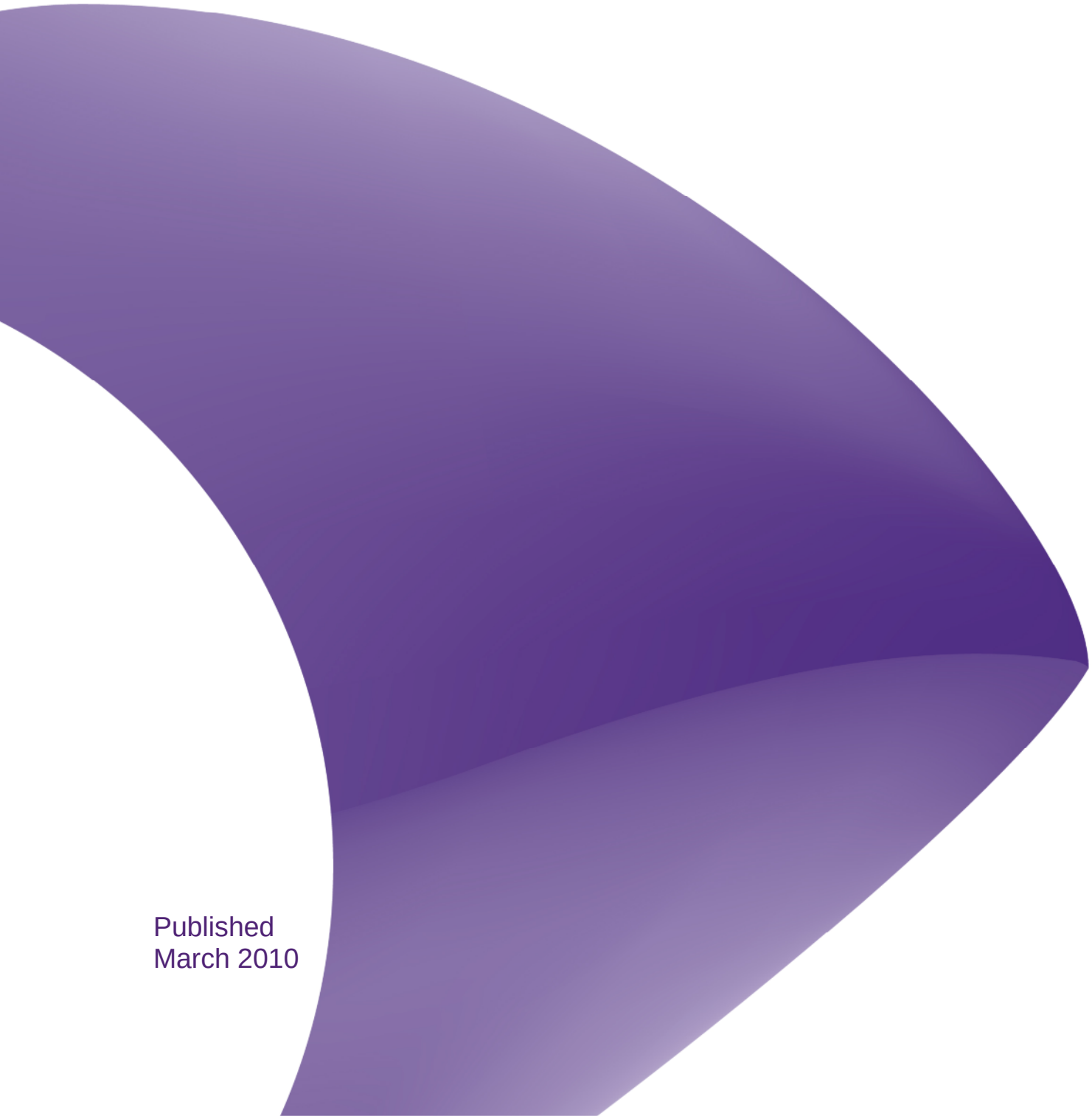
National Fraud Authority

A fresh approach to combating fraud in the public sector

The Report of the Smarter Government Public Sector Fraud Taskforce



Published
March 2010

FOREWORD

Fraud against Government is a crime that directly or indirectly victimises every person in the UK. An essential pre-condition to tackling fraud is recognising that it is more widespread than currently published figures indicate and represents a significant loss to Government income. By its very nature, fraud is committed by people who find that the value of the criminal gain is greater than the risk of detection. This situation must change. The necessary changes can be achieved by building on existing good work and implementing the recommendations of this report, which captures best practices from public and private sector organisations that have successfully tackled this type of crime.

Intelligence-led approaches to data sharing and analytical profiling, stronger identity authentication, designing fraud out of new online systems and raising internal and external awareness of the topic are all elements of this report's recommendations. Such measures will be essential to prevent fraud in a cost efficient way and, with effective implementation, will substantially reduce the opportunity to commit fraud against the public sector. I would urge the Government to act decisively to implement the recommendations in this report and I believe that the National Fraud Authority is well placed to coordinate and drive their delivery.

It has been a great privilege to be part of this extremely important project, completed in just a few short weeks by the excellent team at the National Fraud Authority, most ably led by Dr Bernard Herdan and Stephen Harrison. I have also appreciated the contributions made by taskforce members from the Departments and by the public/private sector senior oversight group that has guided and facilitated this work.

Dr James M. Hart CBE QPM
Independent Chairman - Smarter Government Public Sector Fraud Taskforce

CONTENTS

1. EXECUTIVE SUMMARY

1.1 The public sector fraud taskforce was established within the context of the 'Smarter Government' initiative as a cross-Government team led by the National Fraud Authority (NFA). The taskforce was asked to identify and make recommendations on ways to reduce fraud against the public sector, drawing particularly from best practice within the private sector. This report has been produced in a short period of time drawing on extensive existing experience as well as meetings and discussions with private sector organisations that provide systems, data and techniques to combat fraud or make use of such services within their organisations. Particular focus was placed on lessons we could learn from the finance and insurance sectors, where the fraud threat is greatest and correspondingly, where more investment has been made in counter-fraud solutions.

1.2 We have estimated that the total scale of fraud against the public sector amounts to some £25 billion per year. This comprises £18 billion of losses in tax through fraud and £7 billion of fraud against public sector expenditure, including social security benefits. This estimate is higher than previously published numbers as we have sought to provide figures for areas where levels of fraud are essentially unknown but in which, given comparison with elsewhere, there must be significant levels of fraud.

1.3 There is a significant contrast between the private and public sectors' approach to fraud. The private sector's main focus is on fraud prevention, whereas the public sector places proportionally more effort on detection, investigation and prosecution of fraud which has already been committed. Private sector examples show how use of data sharing, access to a wide range of databases and use of data analytics can prevent fraud occurring, either by deciding to refuse the provision of a service or product or by flagging high risk cases for investigation before a transaction is completed.

1.4 The private sector is also more advanced in risk profiling customers. It has a strong handle on the scale and nature of fraud it encounters and is able to react quickly to vulnerabilities exposed by new fraud threats. In common with the public sector, private organisations struggle with adequate identity verification – a growing issue with the increase in online services. They also suffer significantly from insider staff fraud. The private sector has emphasised to us that there has been no one solution or 'magic bullet' to these challenges. Rather, there is a need to invest as new areas of fraud attack open up and allow time to realise the benefits of each new investment.

1.5 We have also found a number of areas of good practice within the public sector. These include use of data matching and analytic techniques at the Department for Work and Pensions (DWP) and HM Revenue and Customs (HMRC), some effective use of similar techniques in a number of local authorities and valuable fraud prevention and detection work in the National Health Service (NHS) and Identity and Passport Service (IPS). We have found excellent practice in particular local authorities that has not been replicated elsewhere, revealing scope to increase fraud prevention. We have also found work in some Departments which would be applicable to others. We have generally concluded that there is marked reluctance in the public sector to share data, either because of real or imagined legal obstacles or simply a lack of enthusiasm.

1.6 Based on our work we have developed a series of recommendations. The public sector needs to develop a more comprehensive understanding of fraud losses and the causes of such losses across the whole of the sector. We recommend that sharing of data should be substantially increased and that public sector organisations should join with private organisations in putting their fraud data in to the National Fraud Intelligence Bureau (NFIB), which will benefit both sectors. We recommend that the NFA-led work to tackle blockages in information sharing is given increased impetus, again with benefits for the public and private sectors. We believe that the National Identity Crime Taskforce should be energised and that work on ID authentication, which would provide access to public sector records for identity verification purposes, should be speeded up.

1.7 As more Government services go online, it is essential that fraud prevention is built into online processes and systems and we have a number of recommendations on this. We recommend that a number of cross-cutting projects should be developed to tackle fraud issues, such as procurement fraud and staff fraud, which are common to the whole of the public sector. We have made recommendations on incentives to encourage Departments to reduce fraud.

1.8 Our comprehensive list of recommendations should be seen as a package. If all of these recommendations are adopted, we have concluded that between £4.8 billion and £6.7 billion could be saved over the next three years and in excess of £2.5 billion to £3.4 billion per annum thereafter. These are gross figures which do not take account of the cost of implementing new counter fraud measures. If these are taken into account, the net saving figures would be £4.7 billion to £6.3 billion over the next three years and £2.4 billion to £3.3 billion per annum thereafter. We have based our estimates of the cost of implementing new counter fraud measures on a typical private sector return on investment of at least ten to one. We also emphasise the need to maintain current levels of public sector counter-fraud expenditure to combat the continuously rising fraud threat.

1.9 In conclusion, we recommend that Ministers empower a co-ordinating body, such as the NFA, to drive forward a programme of reforms adopting the numerous recommendations in this report. It should operate within an agreed governance arrangement, closely integrated with other programmes, such as the Digital Delivery agenda, to ensure that fraud prevention measures are built in to initiatives such as putting Government services online. We also underline the need to change the culture in the public sector to make people far more aware of fraud risks and the need to pursue appropriate counter measures. A process should be put in place to track the delivery of this programme with six-monthly checkpoints and clear accountability for delivery.

1.10 This report is structured so that all the key messages are contained in this summary and in the next section providing the taskforce recommendations (Pages 7 to 13). The rest of the report provides the context and detailed basis for our conclusions and recommendations, enriched by relevant case studies.

2. SUMMARY OF THE TASKFORCE RECOMMENDATIONS

2.1 This section of the report summarises our recommendations. These recommendations are also embedded in the text of the main report, where further detail and context is provided.

2.2 Our recommendations must be taken as a package. As many private sector organisations told us, there is no 'magic bullet' solution to reduce and prevent fraud. A range of approaches and techniques is required.

2.3 If the public sector makes concerted progress on these recommendations, we will have made our country a more hostile place for fraudsters. We will also have made real financial savings within the public sector that will contribute to reductions in public expenditure and the funding of frontline services.

Recommendation	**Page**
1. We recommend that a more comprehensive estimate of public sector fraud should be produced on an annual basis. This estimate should be broken down not just by organisation but by major cross-cutting types of fraud such as procurement fraud, staff fraud and fraudulent grant allocations.	21
2. We recommend that steps are taken to ensure that those Departments which have made better progress on understanding their fraud risks should share their good practice more widely.	22
3. We recommend that the NFA and HM Treasury hold discussions with the National Audit Office (NAO) and the Audit Commission to establish a consistent method for producing a comprehensive analysis of fraud losses and exposure to fraud risks faced by the public sector organisations they audit.	22

Recommendation		Page
4.	Build in consideration of fraud risks early enough, at the policy development stage. We recommend that: • The NFA works with the Cabinet Office to develop and communicate guidance and training material for policy makers, explaining the benefits of assessing fraud risks at the policy development stage. This can make use of real cases and could form part of a 'fraud impact assessment' process • Office of Government Commerce (OGC) guidance at both the 'starting gate' and subsequent stages should make specific references to 'designing out fraud' by identifying and mitigating fraud risks • The NFA works with the OGC Gateway team to contact the senior responsible officers of all existing programmes that will be putting public services online in the next 24 months to check that they are satisfied that their programmes have properly considered fraud risks and counter measures	24
5.	All public sector organisations should consider rebalancing their counter-fraud work. They should place greater emphasis on the prevention of fraud, prior to providing a service or making a payment, compared to the resource they place against detection, investigation and prosecution after a fraud has occurred. They should also consider making more use of profiling techniques and being more intelligence-led.	25
6.	Public sector organisations need to learn more from the private sector approach to restraining and seizing assets promptly and thus improve public sector asset recovery performance. The study commissioned by the newly established Counter Fraud Strategy Forum is a useful initial step.	26
7.	Public sector organisations should consider making more use of real-time credit reference and other data checks when designing new systems. They have the potential both to prevent fraud and offer a better service for legitimate customers.	27

Recommendation		Page
8.	We welcome the decision of the UK Border Agency to become the first public sector member of CIFAS. We recommend that the benefits are shared as widely across the public sector as possible and that other Departments should be much more open to the benefits of CIFAS as an additional key element in their counter fraud strategy.	31
9.	Public sector organisations should recognise that information sharing with the private sector is a 'two-way street' which yields mutual benefit. Public sector organisations should endeavour to meet lawful and proportionate requests, especially where the private sector is willing to cover costs incurred by the public sector.	32
10.	IPS should find solutions to be able to extend the availability of the Passport Validation Service to aid the cross Government and private sector fight against fraud.	33
11.	The Driver and Vehicle Licensing Agency (DVLA) should work with public and private sector organisations to widen the provision of driving licence checks available to them on a robust consent basis with agreement from the Information Commissioner's Office (ICO). This should improve customer service and convenience, while providing greater security over their own data and identity. It would support identity verification and fraud prevention for accredited organisations.	34

Recommendation		Page
12.	We recommend that: • Work continues to develop more effective and efficient methods of verifying Government identity credentials and that this work takes account of the needs of both the public and private sectors • The public sector should evaluate the use of online identity verification techniques (offered by, for example, the credit reference agencies), as well as online links to relevant Government databases. This will become increasingly important as more services go online • The work of the National Identity Crime Taskforce should be energised to yield a range of interventions to combat ID fraud for the benefit of both public and private sectors. It should work more closely with the range of ID assurance initiatives which are underway in the public sector	36
13.	In the light of any Safeguarding Identity Strategy Group (SISG) recommendations, early action should be taken to implement agreed changes. There should be a particular focus on prevention of any fraud in the public and private sectors which may be facilitated by change of name.	37
14.	The Access to Public Services initiative (AtPS) should include a work strand which focuses on ensuring that fraud prevention is built into this important new shared service.	38
15.	To combat staff fraud, we recommend developing a staff engagement workstream and conducting early consultation with frontline staff to help scope the work. This work should also look at the experience of organisations which have used externally-run 'whistle blowing' services, providing staff who report fraud with greater reassurance.	41

Recommendation		Page
16.	We recommend that perverse counter-fraud incentives (and areas where there is a lack of an incentive) across the public sector are documented. A project should be established to find ways to build incentives which will be much more effective and better understood by staff.	42
17.	We recommend that any targets which focus on numbers of completed enforcement actions be reviewed and replaced, if possible, by targets that place greater emphasis on fraud prevention.	42
18.	The public sector should work actively within the NFA Information Sharing Taskforce to overcome blockages to information sharing already identified as impeding the fight against fraud. In some areas, Ministers will need to support legislative change to make this possible.	48
19.	We recommend that HMRC, DWP, local authorities and NHS sharing of fraud intelligence with the National Fraud Intelligence Bureau (NFIB) is progressed as a matter of urgency, and that a clear mandate is given to all Departments by Ministers to share their fraud intelligence with the NFIB. The NFIB needs to become clearer about the products, services and data it will provide back to data contributors and to law enforcement authorities other than the police.	48
20.	We recommend conducting a study of the various fraud intelligence systems in the public sector. This should include an analysis of what intelligence is currently shared across the public and private sectors, how it is analysed, and how the results of this analysis are fed back into fraud investigations and the design of new fraud prevention measures.	49
21.	We recommend that DWP and HMRC share information on non-criminal sanctions against fraudsters with other parties (preferably via the NFIB), subject to recommendation 19 above.	49
22.	We recommend that the use of data analytical techniques using anonymous matching is explored further for public sector applications.	50

Recommendation		Page
23.	It is recommended that all local authorities implement solutions to prevent ‘council tax single person discount’ fraud, by making use of credit reference agency and other open source data.	54
24.	We recommend the reduction in fraud threat to the public and private sectors posed by criminal use of accommodation addresses. The solutions to achieve this should be delivered by the NFA-led ‘accommodation addresses’ project.	56
25.	Depending on the result of the assessment, we recommend that DWP implements its proposed new Customer Centric end-to-end solution.	57
26.	We would encourage the Department for Communities and Local Government (DCLG) and local authorities to pursue their pilots on prevention of housing tenancy fraud. The conclusions and best practice identified should be built into operational implementation solutions as soon as possible.	60
27.	We note the additional work that the Student Loans Company (SLC) has undertaken to verify identity and income is to be evaluated. Depending on the results, we would advocate implementation and sharing of this best practice elsewhere in the public sector.	61
28.	We recommend that DWP evaluate the following pilots and/or initiatives and share their experience with relevant Government Departments and other public services: • Voice risk analysis technology • Predictive/innovative analytics • Housing benefit risk assurance tool	63

Recommendation		Page
29.	Those public sector organisations which have the largest proportion of expenditure on procurement and which make greatest use of contractors to provide outsourced services and products, should be involved in a scoping project to agree ways to reduce and prevent procurement/contractor fraud.	68
30.	We recommend that the public sector organisations who have the largest proportion of expenditure on staff should be involved in a scoping project to reduce and prevent staff/insider fraud.	68
31.	We recommend that, if resources allow, consideration should also be given to a regional pilot to determine the benefits of closer working across all counter fraud agencies in a specific location. Such a project may be more effective when there has been further progress on agreements to share intelligence via the NFIB.	69
32.	We recommend a study to determine the feasibility of establishing framework contracts with credit reference agencies to make it simpler and more cost effective for smaller public sector organisations to make use of these services.	69
33.	The current spending round comes to an end in the next financial year. We therefore recommend that HM Treasury encourages Government Departments to identify resources that could be made available for this coming financial year only, which can fund participation in the cross-cutting projects described in this report.	70

3. INTRODUCTION

3.1 In December 2009, the Government published a White Paper – 'Putting the Frontline First – Smarter Government'. It set out plans for strengthening the role of citizens and civic society, recasting the relationships between the centre and the frontline and between the citizen and the state, and streamlining Government.

3.2 One of the actions in the White Paper was to establish a taskforce to identify and make recommendations on ways to reduce fraud against the public sector, drawing particularly on best practice in the private sector including its use of data analysis techniques.

3.3 The taskforce was required to report to Ministers in time for Budget 2010.

3.4 In January 2010, the National Fraud Authority (NFA) was given the role of assembling and leading the taskforce, reporting to a senior oversight group and an independent chair. The members of the taskforce and oversight group are listed at Annex A.

3.5 We chose to focus its attention on those public sector organisations which had the greatest areas of declared fraud loss - HMRC and DWP - and those other areas of potentially large losses such as the NHS and local authorities. This is not to say that the level of fraud in other parts of the public sector is not also a concern. The recommendations on better measurement of the size and nature of fraud apply across the public sector. We also believe that many organisations across the whole public sector will benefit from collaborative, cross-cutting work in areas such as procurement fraud, staff fraud, identity fraud and information sharing.

3.6 We have focused on areas of fraud which result in financial losses. There are other types of fraud where the loss is not immediately measurable in financial terms but still has important social and policy consequences. An example of this is employment, benefits and social housing claimed by those residing illegally in the UK.

3.7 We decided to concentrate on banking and insurance organisations in the private sector because they have well-established approaches to estimating and countering fraud, both as individual companies and as industry groups; where they cooperate despite being commercial competitors. In the private sector they are also most subject to attack by fraudsters and, like many public services, they have large customer bases. They have also faced similar challenges in getting a single view of a customer and moving traditional services online. We sought information from these companies on their broader approach to fraud as well as their experience in deploying data matching and analytical software.

3.8 We also approached a number of companies who were known to members of the taskforce and our private sector contacts as counter-fraud service providers. Our brief was not to evaluate particular products, but to learn how they have been deployed and what return organisations had achieved in terms of fraud reduction. Our contact with private and public sector users of these services has helped us produce realistic assessments of where they could be deployed to best effect.

3.9 A list of the organisations contacted during this study is provided at Annex B.

4. THE SCALE AND NATURE OF PUBLIC SECTOR FRAUD

4.1 The most recent figures of the scale and breakdown of public sector fraud were published by the NFA in January 2010. The NFA's Annual Fraud Indicator was based mainly on 2008 figures which also included fraud against the private sector, individuals and charities. A substantial fraction of fraud is committed by organised crime groups and proceeds are used to fund other serious crimes such as drugs, illegal immigration, people trafficking and terrorism. The NFA is working on an analysis of the relationship between fraud and serious organised crime.

4.2 The high level breakdown of fraud between sectors of the UK economy is illustrated in Figure 1 below.

Figure 1 - Breakdown of fraud loss in the UK (2008)[1]

[1] Due to rounding, the components of figure one may not sum to their respective totals

4.3 The estimate of public sector fraud in 2008 was £17.6 billion. The great proportion by value of the £17.6 billion figure drew on comprehensive estimates prepared by HM Revenue and Customs (HMRC) and the Department for Work and Pensions (DWP) which were already in the public domain. The measurement processes used by these Departments have been subjected to rigorous scrutiny over a number of years by the Departments themselves and also by independent bodies such as the National Audit Office (NAO). However no other public sector organisation has such a comprehensive approach to measuring and estimating fraud. Indeed, a number of Departments and Agencies have not been able to provide any credible estimates for the fraud to which they are undoubtedly subject. The £17.6 billion figure was constrained to include only those numbers provided by Departments. It is therefore an under-estimate of the size of the problem. Table 1 (see over) provides the breakdown of the £17.6 billion figure. The figures have been rounded for presentation.

4.4 We have a high degree of confidence in the estimates provided by HMRC, DWP, TV Licensing, DVLA and NHS Patient Charge Evasion figures, which have been subjected to rigorous internal scrutiny by the Departments themselves and by external bodies such as the NAO. We have a lower degree of confidence in the other figures provided as they are based on:

- Incidents of recorded and investigated fraud. By their nature, frauds are difficult to detect. Unless organisations have a rigorous approach to both fraud recording and estimation they will not get a comprehensive picture of the scale and nature of the problem;
- Extrapolation of recorded frauds in a particular geographical or business area. The baseline figure for the extrapolation may be low, and the extrapolation itself may be conservative. For example, we have been told that the national estimate of housing tenancy fraud in England may be four times as high as the figure used to compile the £17.6 billion total.

Table 1 - Breakdown of NFA Annual Fraud Indicator estimate of public sector fraud (2008)

Area of Fraud	Estimated Loss (2008)	Breakdown
Tax	£15.2 billion 86% of public sector fraud loss	Includes HMRC's estimate of the tax gap that is attributable to fraudulent behaviour, tax credits fraud and vehicle excise duty evasion.
Benefits	£1.1 billion 6% of public sector fraud loss	Includes benefit fraud estimates for all areas of benefit spending.
Local Government	£684 million 4% of public sector fraud loss	Includes estimates of housing tenancy fraud, council tax single person discount fraud and an NFA estimate of other types of local authority fraud based on the findings of a survey of reported fraud across 24 London local authorities.
TV Licence Fee	£195 million 1% of public sector fraud loss	Figure relates to TV licence fee evasion losses as provided by the BBC.
NHS	£263 million 1% of public sector fraud loss	Includes data from NHS Counter Fraud Service, Audit Scotland and NHS Counter Fraud Unit Northern Ireland. Includes patient charges fraud, NHS contractor fraud, NHS bursary fraud and procurement fraud.
Pensions	£64 million <1% of public sector fraud loss	Includes fraud within Central Government, Local Government and NHS pension schemes.
Other Central Government	£161 million 1% of public sector fraud loss	Includes MoD procurement fraud, student loans fraud, National Savings and Investments fraud and fraud losses reported to HM Treasury.

4.5 The limitations of the £17.6 billion total were set out when it was published and there is a programme of work underway to develop better estimates on an annual basis. Because of the gaps in the £17.6 billion figure, we concluded that for this report it was important to provide an estimate of how much additional fraud losses there might be in the public sector. Otherwise there would be a risk that fraud prevention and reduction strategies will be distorted and might focus overly on areas of fraud which just happen to be better measured, rather than those causing most harm. Organisations which have placed insufficient emphasis on estimating fraud will naturally place less emphasis on combating it.

This is particularly concerning at a time of tightening public finances. There is also the risk that organisations might not focus sufficiently on types of fraud which are common problems across the public sector, such as procurement fraud and staff fraud.

4.6 We therefore took a different approach, using a 'top down' method of estimating fraud as follows:

- Looking at specific areas of public finances, where we were confident that sound measurement exercises of fraud losses had been made
- Estimating a typical percentage loss based on the loss percentages identified in (i) above. This was not a simple averaging exercise. For example we excluded outlying figures where unusually high percentage losses had been found
- Treating expenditure fraud losses differently to revenue fraud losses. Revenue ('tax') fraud typically shows a higher percentage loss rate than types of expenditure fraud, such as benefit fraud.

4.7 Based on this approach, the estimate of public sector fraud which we have produced for the purposes of this report is £25 billion. The high level breakdown of this calculation is summarised in Table 2 below. More detail on the calculation method is included at Annex C.

Table 2 - Estimated public sector fraud loss 2010/11

	Expenditure / Revenue *(£ billions)*	Applied Fraud Rate *(Percent)*	Estimated Fraud Loss *(£ billions)*
Total Managed Expenditure 2010/11			
Total Managed Expenditure (excludes Work and Pensions AME[2])	£548.5	1.1%	£6.0
Work and Pensions AME	£153.2	-	£1.1
Total Managed Expenditure	£701.7	-	£7.1
Net Taxes and NI Contributions 2010/11			
HM Revenue and Customs	£423.1	-	£15.0
Non-HM Revenue and Customs[3]	£75.7[4]	3.3%	£2.6
Total Net Taxes and NI Contributions	£498.8	-	£17.6
Total Estimated Public Sector Fraud Loss 2010/11			**£24.7**

4.8 This £25 billion figure reflects the 'top down' estimate, whereas the £17.6 billion figure is derived more from a 'bottom up' method of estimating fraud. If particular fraud types are not recorded or estimated accurately they will inevitably be under-recorded in a 'bottom up' calculation. It would therefore be expected that a 'top down' estimate would be higher.

[2] AME: Annually Managed Expenditure
[3] Includes council tax, business rates, vehicle excise duty etc.
[4] In calculating this fraud loss estimate, this figure has been adjusted. See Annex C

4.9 Breaking down the £25 billion figure by Department or public service is problematic because it is based on overall percentages of average fraud rate and different factors apply in different parts of the public sector. However, we hope this figure will be used to encourage a better and more consistent approach to estimating levels of fraud across the public sector. This figure should also encourage more collective action against common types of fraud affecting many parts of the public sector crossing Departmental boundaries.

For example, procurement and staff costs account for 29% and 25% respectively of Total Managed Expenditure (TME) by the public sector. There are likely to be significant fraud losses in these areas, affecting a number of Departments and public services. Adopting common approaches could benefit them all and be easier to implement than by taking a Department-by-Department approach.

4.10 We also believe that similar cross-Departmental action should be taken on fraud in certain areas of 'grant awards'. We use the term loosely to encompass areas which together comprise around £15 billion[5] of expenditure per annum such as student loans and grants, international development grants, legal aid and EU Common Agricultural Policy Payments.

4.11 We have concluded that the current approach to estimating fraud in large parts of central Government, the local authority sector and in the NHS needs to be much improved. This requires not only a change in reporting and monitoring systems but also a cultural change, recognising that a better understanding of fraud risks and a willingness to tackle them will help focus more resources to frontline services. We say more about culture change requirements later in this report.

RECOMMENDATION 1

We recommend that a more comprehensive estimate of public sector fraud should be produced on an annual basis. This estimate should be broken down not just by organisation but by major cross-cutting types of fraud such as procurement fraud, staff fraud and fraudulent grant allocations.

[5] This figure does not take into account all grants paid out by the public sector.

RECOMMENDATION 2

We recommend that steps are taken to ensure that those Departments which have made better progress on understanding their fraud risks should share their good practice more widely.

4.12 The NFA could facilitate this work to limit the burden on those Departments which are the sources of good practice. As the author of the NFA Annual Fraud Indicator and as a body whose focus cuts across both the public and private sectors, the NFA can also help to ensure that good practice is also exchanged with the private sector.

4.13 The arrangements for central Government Departments to report levels of non-fiscal fraud are inadequate. The recent decision of HM Treasury to cease asking for annual returns will not help to improve the situation. It is unlikely that a request for an annual return by the NFA to each Department will be treated with the same degree of urgency as a request from HM Treasury. However, given than the annual reports to HM Treasury were not giving a sufficiently comprehensive picture in the first place, we believe that a more fundamental change in approach is required.

RECOMMENDATION 3

We recommend that the NFA and HM Treasury hold discussions with the National Audit Office (NAO) and the Audit Commission to establish a consistent method for producing a comprehensive analysis of fraud losses and exposure to fraud risks faced by the public sector organisations they audit.

5. WHAT WE HAVE LEARNED FROM THE PRIVATE SECTOR

5.1 This section summarises the lessons we learned from the private sector. There was a remarkable degree of unanimity in what they told us:

- Understand the problem, otherwise you will not target your counter fraud resources effectively
- Preventing fraud is more effective than detecting it after it has happened
- Fraud prevention checks do not necessarily mean a poorer customer experience, indeed the opposite can be the case
- Share data with organisations that face the same threats
- The private and public sectors face some common challenges and need to work together on identity fraud and staff fraud
- Consider incentive regimes when drawing up service contracts

Understand the problem otherwise you will not target your counter fraud resources effectively

5.2 Understanding both the size and nature of the fraud problem was vital for the private sector companies to whom we spoke. They expect an appreciable return on investment for their counter fraud projects, ranging from 10:1 up to 30:1. Knowledge of the size of the problem was important to help direct resources to the areas of greatest potential loss and therefore building a sound business case. The nature of particular types of fraud and fraud trends were also key concerns. For example, certain types of insurance fraud are committed as 'attacks' on the industry as a whole and an effective response requires collective sharing of information and intelligence across the industry.

5.3 Trends in attacks on e-enabled services were of particular concern, given the volume of business conducted online. The issue of e-Crime is a significant fraud enabler for both the public and private sectors. We were able to obtain some reassurance on how fraud risks to online services can be mitigated. We were also told of ways where online services can provide better fraud prevention techniques. The clear message from the private sector was to keep on top of these issues and spread good practice widely.

We made recommendations for improving public sector fraud measurement in Section 4.

Preventing fraud is more effective than detecting it after it has happened

5.4 The most striking difference between the private sector and public sector organisations we met was in their attitude to fraud prevention. The private sector focuses far more on preventing fraud and therefore preventing financial losses. We were told that fraud prevention was considered during the design of products and services, particularly when services were provided online. Fraud prevention checks were built into systems for processing products and service applications. We discuss some examples of these later in the report.

RECOMMENDATION 4

Build in consideration of fraud risks early enough, at the policy development stage. We recommend that:

- **The NFA works with the Cabinet Office to develop and communicate guidance and training material for policy makers, explaining the benefits of assessing fraud risks at the policy development stage. This can make use of real cases and could form part of a 'fraud impact assessment' process**
- **Office of Government Commerce (OGC) guidance at both the 'starting gate' and subsequent stages should make specific references to 'designing out fraud' by identifying and mitigating fraud risks**
- **The NFA works with the OGC Gateway team to contact the senior responsible officers of all existing programmes that will be putting public services online in the next 24 months to check that they are satisfied that their programmes have properly considered fraud risks and counter measures**

5.5 Private sector organisations' application processing systems allow them to profile the risk presented by customers. This is usually based on a combination of checks against internal data sources and external data sources such as credit reference agencies. A private sector organisation can decide that a particular individual poses such a potential risk that it will not do business with him or her, or will take account of that risk when providing services, for example setting the level of an insurance premium or rate of interest charged on a loan. Public sector organisations are much more constrained as to whether they can refuse a service. However they can design their systems to apply additional checks to higher risk applicants and in some circumstances they can legitimately refuse to do business with people whose claims or applications are unfounded, whose circumstances are falsely declared or whose identities are false. An increased focus on fraud prevention will also reduce burdens on the criminal justice system.

RECOMMENDATION 5

All public sector organisations should consider rebalancing their counter-fraud work. They should place greater emphasis on the prevention of fraud, prior to providing a service or making a payment, compared to the resource they place against detection, investigation and prosecution after a fraud has occurred. They should also consider making more use of profiling techniques and being more intelligence-led.

5.6 Where frauds are detected, feedback is gathered to learn lessons. Private sector organisations look to prevent further losses by analysis of the causes and make any appropriate changes to their systems. For example, they might look to gather additional information during the application stage to check against existing sources of data, identify new sources of data to check or look for trends, such as fraudulent applications coming from particular 'high risk' addresses.

5.7 When investigating a fraud, we were told the key benefit was the learning fed back into the organisation's prevention measures. The cost of investigation per se merely added to the loss which had already been incurred.

5.8 Private sector organisations adopt a different approach to the early restraint or seizure of assets of suspected fraudsters. They tend to be far more proactive than public sector organisations. While some fraudsters will not have significant assets to seize, this is not always the case. However in many cases fraudsters have disposed of their illegally obtained assets by the time they are convicted in court. Even the threat of a longer prison sentence may not be an effective incentive for them to reveal 'hidden' assets.

RECOMMENDATION 6

Public sector organisations need to learn more from the private sector approach to restraining and seizing assets promptly and thus improve public sector asset recovery performance. The study commissioned by the newly established Counter Fraud Strategy Forum is a useful initial step.

Fraud prevention checks do not necessarily mean a poorer customer experience, indeed the opposite can be the case

5.9 Private sector organisations pointed out to us that checks on customers can usually be done in real time. It is no longer the case that counter fraud checks significantly delay the application process. Indeed lower risk customers can experience a much quicker service as they are 'fast tracked'. Even some higher risk customers can still receive a prompt service, as it is often still possible to carry out some additional checks online or via the telephone. We have examples in the following case study.

Mobile telecommunications provider – electronic proof of identity

A mobile telecommunications provider was experiencing a reduction in sales because potential customers did not have the correct level of physical identity documents available to open an account both online and at high street stores.

Electronic confirmation of identity was provided by a credit reference agency. This involved potential customers being asked particular questions to confirm their identity and open a contract. The questions were asked even when customers could present physical documents. This had an impact on fraudsters who were providing false identity documents to open accounts. When they were asked to answer questions to confirm their identity, they refused and left the store or exited the application process. Conversely, legitimate customers who did not have ID on them when visiting the shop were still able to sign up for the service as they could answer all of the questions correctly.

The service has had a significant impact on fraud prevention at the same time as improving sales. In a three month period, 250,000 applicants had their identity checked. The company saw a 50% reduction in fraud and an 8% increase in sales.

RECOMMENDATION 7

Public sector organisations should consider making more use of real-time credit reference and other data checks when designing new systems. They have the potential both to prevent fraud and offer a better service for legitimate customers.

Share data with organisations that face the same threats

5.10 The banking and insurance industries are particularly noteworthy in their approach to sharing data about fraud and there are other examples of cross-company data sharing in other sectors. Data sharing includes suspected fraud as well as confirmed fraud, which helps to provide a richer intelligence picture. Data is shared at an industry level, via shared services which are funded on a subscription basis. Individual companies also employ similar tools and techniques and recognise the need to invest in the skills of analysts to interpret the results of data matching; helping the organisations avoid being overwhelmed with alerts of potential frauds.

5.11 There is no 'magic bullet' to combating fraud. All the companies we contacted rely on a mix of tools and techniques. They cannot rely on just one approach and they need to keep their counter measures under review as fraudsters continually adapt their attacks.

Finance industry - Fraud Intelligence Sharing System (FISS)

FISS allows financial institutions to identify and prevent fraud against their organisations by sharing confirmed, suspected and attempted payment fraud information in a secure environment. At the same time, it provides a direct feed into the NFIB.

To ensure compliance with the requirements of the Information Commissioner, FISS is hosted on a secure site with strict access controls. Members must agree to the FISS Legal Agreement, Security Code of Conduct and Security Policy, which stipulates due diligence when acting on other members' data. There are requirements for annual member 'self-certification' regarding compliance with security codes and policies. This includes completion of a questionnaire and certification of responses to the UK Payments Council.

All banks using the service have recognised benefits in the prevention of fraud, with one financial institution reporting £4m savings over the last quarter.

Insurance industry – Insurance Fraud Bureau (IFB)

The UK insurance industry is divided into two categories: general insurance (motor, property, accident and health) and long-term insurance (life and pensions). Long-term insurance accounts for the majority of the insurance market, with total net premiums of £131 billion, compared to just £33.8 billion for the general insurance market. The Association of British Insurers (ABI) publishes an annual 'savings' figure relating to general insurance fraud and provides fraud losses for both detected and undetected insurance fraud. Based on information provided by the ABI, insurance fraud is estimated to have cost the industry £2.08 billion during 2008. These fraud losses apply only to the general insurance market. Undetected fraud in the long-term insurance market is believed to be exceptionally low.

The Insurance Fraud Bureau (IFB) was launched in 2006. It provides a cost effective, tactical solution for detecting and preventing organised, cross industry fraud, supporting the wider ABI industry fraud strategy. The IFB collates and combines data available from industry databases and uses data matching and analytical techniques to develop cross-industry intelligence and identify potentially fraudulent networks. Supplementary data is sourced directly from participating insurers, as required, to build a detailed intelligence-based understanding of activity. The IFB leads and coordinates the industry response to the identification of criminal fraud networks and works closely with the police and law enforcement agencies. The IFB estimates the insurance industry's exposure to fraudulent organised motor claims is £350 million per annum. Insurance fraud adds an average of £44 to individual policyholders' premiums each year.

Mobile telecommunications providers – 'no intention to pay'

All major mobile telecommunications providers were experiencing losses from customers who had no intention of paying their mobile phone bills.

A credit reference agency provided a solution for all providers to share their data on customers who had failed to pay mobile phone bills, were suspected of having committed fraud or were believed to have no intention to pay their bills.

The credit reference agency provided a data matching service which each telecommunications provider could access. Having invested approximately £300,000 each in the service, each provider has estimated fraud savings at approximately £2m. This reflects a return on investment of 6:1.

CIFAS and UK Border Agency – public/private sector data sharing

CIFAS is the UK's Fraud Prevention Service with over 260 members spread across banking, credit cards, asset finance, retail credit, mail order, insurance, savings and investments, telecommunications, factoring and share dealing. Members share information about identified frauds in the fight to prevent further fraud.

CIFAS is the world's first 'not-for-profit' fraud prevention data sharing scheme. With 350,000 records added each year, in 2009 alone CIFAS members stated they had saved a combined total of over £857m from using its services. Following specification by the Home Office under the Serious Crime Act 2007, public sector organisations are able to join CIFAS and share information reciprocally to prevent fraud. As well as sharing information with the private sector, public sector organisations may share fraud information with one another through CIFAS.

The UK Border Agency (UKBA) will shortly become the first public sector body to join CIFAS. UKBA will provide CIFAS with information on people thought to be residing illegally in the UK, for example those whose visas have expired. CIFAS members will be alerted if such a person applies for one of their products or services. UKBA will benefit as this will help to create a more hostile environment for illegal immigration as well as providing valuable information on the whereabouts of people who should no longer be in the country.

RECOMMENDATION 8

We welcome the decision of the UK Border Agency to become the first public sector member of CIFAS. We recommend that the benefits are shared as widely across the public sector as possible and that other Departments should be much more open to the benefits of CIFAS as an additional key element in their counter fraud strategy.

5.12 We make a number of specific recommendations on information sharing in Section 6. While not strictly part of our brief, we felt that we should make the following recommendation in addition to those in Section 6.

RECOMMENDATION 9

Public sector organisations should recognise that information sharing with the private sector is a 'two-way street' which yields mutual benefit. Public sector organisations should endeavour to meet lawful and proportionate requests, especially where the private sector is willing to cover costs incurred by the public sector.

The private and public sectors face some common challenges and need to work together on identity fraud and staff fraud

Identity Fraud

5.13 Traditional methods of proving identity by checking a physical identity document often defeat the object of improving online customer service. Increasingly sophisticated services, using information held by credit reference agencies, provide a high degree of assurance of identity. These not only give a risk score against some initial information provided by the customer, but also prompt additional questions only the individual concerned should be able to answer (for example more details about the number and provider of credit cards an individual holds). These questions can be answered online or via a call centre so the customer can still get a quick service. Private sector organisations have told us that they would welcome online checks of Government issued documents commonly used as proof of identity to be available. There are a number of such initiatives which we have summarised below. We welcome moves to coordinate these measures on identity authentication and assurance for the purposes of access to public services under the Digital Delivery initiative and the close working between these and the wider measures to safeguard identity led by the Home Office.

Identity and Passport Service - Passport Validation Service (PVS)

PVS allows public and private sector customers to check the validity of the passports presented as a proof of identity. This service began several years ago to support business efforts to prevent money laundering and is now widely used. Financial services organisations and Government Departments have benefited significantly from PVS. Around sixty organisations use this service – twenty are Government Departments or Agencies, including the DVLA, Security Industry Authority and the Student Loans Company. Forty are from the private sector, principally financial services.

The service has prevented many fraudulent transactions since its inception and the saving to business has been millions of pounds. It is now a business-critical tool for many organisations where UK passports are presented as proof of identity.

National Identity Service

In November 2009, the Identity and Passport Service began to issue identity cards on a voluntary basis to British citizens aged 16 and over, resident or working in Greater Manchester. In addition, identity cards were offered to British and EEA nationals working at Manchester and London City airports. The service has been extended to people in the North West region, those aged 16-24 in London and those who register an interest on the IPS website.

Manchester Airport introduced a number of benefits for airside workers who hold an identity card and believe they can introduce these benefits because of the added identity assurance the card gives them. Airside workers who hold an identity card now benefit from a streamlined service to get an airside pass. IPS supported these improvements by introducing the following identity services at the airport:

- A biometric reader to verify the information on an identity card from a person's fingerprint; and
- A Card Validation Service to verify the biographic details shown on an identity card against the National Identity Register

Businesses and airside workers are now seeing benefits from the introduction of identity cards and both airports intend to introduce further improvements.

5.14 We have been told that the ability to verify passport data in real time – particularly in support of online access to public services – would be of considerable interest to a number of public and private sector organisations. IPS has made some progress in developing such a way of using PVS, though this is currently limited to a small number of organisations.

RECOMMENDATION 10

IPS should find solutions to be able to extend the availability of the Passport Validation Service to aid the cross Government and private sector fight against fraud.

DVLA - Driver Validation Service (DVS)

DVLA already provides instant access to drivers' information for a number of organisations to allow them to fulfil their statutory responsibilities, including the Police, Courts, Fixed Penalty Offices, Vehicle and Operator Services Agency (VOSA) and the Driving Standards Agency (DSA). For example, in the Police case, DVS provides an interface between the Police National Computer and the drivers' register which only allows authenticated users to submit enquiries on drivers' records via the Government Secure Intranet. North Wales Police successfully piloted a variant which provides DVS through handheld devices, facilitating access to drivers' details including photograph and signature at the roadside. This allows immediate identification and helps the police to enforce against unlicensed and disqualified drivers, while negating the need for motorists to produce their driving licence at a police station. In one survey undertaken by Northamptonshire Police, some 60% of those stopped provided false details and this facility saves Police time and improves effectiveness of intervention significantly. An initial pilot, operating on an individual consent basis, has also proved successful when deployed for car hire, car leasing and car insurance companies.

5.15 DVLA has not yet been able to extend the provision of the DVS to a range of other public and private organisations who have told us this would be hugely beneficial to help with identity verification and fraud prevention.

RECOMMENDATION 11

The Driver and Vehicle Licensing Agency (DVLA) should work with public and private sector organisations to widen the provision of driving licence checks available to them on a robust consent basis with agreement from the Information Commissioner's Office (ICO). This should improve customer service and convenience, while providing greater security over their own data and identity. It would support identity verification and fraud prevention for accredited organisations.

Department for Children Schools and Families (DCSF) – Employee Authentication Services (EAS)

DCSF's EAS offers a means for Local Government employees and trusted partners to access shared information on Government services and databases. EAS ensures that the correct person is accessing appropriate information by using 'two-factor' authentication to verify the identity of a user. It requires a user to have two components to validate their identity when logging onto a system – a PIN and a token or card. EAS is endorsed and security accredited as a core Government shared asset, meaning that individuals can use EAS to access multiple applications and databases across Government through a single authentication process and token. As more shared Government databases switch to 'two-factor' authentication as a minimum security standard, EAS will help decrease the burden on the end user by reducing the number of tokens that they are expected to carry and manage in order to access sensitive information.

National Identity Crime Taskforce

To combat the increasing threat of identity-enabled crime the Home Office asked the NFA to chair an Identity Crime Task Force. This seeks to co-ordinate the work of three pre-existing groups: the Association of Chief Police Officers (ACPO) Identity Crimes Working Group, the Serious Organised Crime Agency (SOCA) Programme of Activity 17 and the Identity Fraud Communications and Awareness Group (IFCAG).

The chairs of each of these groups plus the IPS, the City of London Police (CoLP) and HMRC are collaborating to implement a 28 point action plan to combat identity crimes. Work is underway to address the creation of false documents, the use of specialist printing equipment by criminals, to stop fraudsters obtaining genuine identity credentials, to tackle websites that sell false identities and produce guidance on handling bulk data arising from disruptive operations.

5.16 The National Identity Crime Taskforce has made significant progress and has commissioned the first ever strategic assessment of identity crime, but much more still needs to be done. The threat assessment will provide the best ever picture of this threat, but all of this work needs to be driven forward with even greater urgency, using national multi-agency governance in order to get to grips with a growing problem.

RECOMMENDATION 12

We recommend that:

- **Work continues to develop more effective and efficient methods of verifying Government identity credentials and that this work takes account of the needs of both the public and private sectors**
- **The public sector should evaluate the use of online identity verification techniques (offered by, for example, the credit reference agencies), as well as online links to relevant Government databases. This will become increasingly important as more services go online**
- **The work of the National Identity Crime Taskforce should be energised to yield a range of interventions to combat ID fraud for the benefit of both public and private sectors. It should work more closely with the range of ID assurance initiatives which are underway in the public sector**

ACPO Identity Crime Working Group (ICWG) - Name Changing

The ACPO Identity Crime Working Group (ICWG) initiated work to understand the issue of name changing, including:

- The use of name changing by those involved in economic crime, organised crime, sexual offences and international terrorism,
- The use of name changing to help facilitate criminal activity and evade detection,
- The relative simplicity of the name changing process, lack of a central database, little regulation and limited evidence of data sharing making it an attractive proposition for criminals,
- The fact that name changing was not confined to criminals' use of lawful avenues to change their name for criminal intent, but also criminals' use of fraudulently obtained genuine documents and further name changes to confuse authorities and evade detection.

Further analysis of the problem is being steered by the Safeguarding Identity Strategy Group (SISG) – the overarching senior official leadership group for Government policy and strategy on identity. The group, chaired by the Permanent Secretary of the Home Office, is considering the need for a more consistent approach to dealing with change of name requests within Government, the benefits that this may bring in relation to the efficient delivery of public services, and whether additional action is required.

RECOMMENDATION 13

In the light of any Safeguarding Identity Strategy Group (SISG) recommendations, early action should be taken to implement agreed changes. There should be a particular focus on prevention of any fraud in the public and private sectors which may be facilitated by change of name.

The 'Access to Public Services' (AtPS) initiative

The AtPS initiative aims to provide a shared service across Government, allowing users of Government services to identify themselves simply and definitively and access those services online. This process is sometimes called Remote Authentication. It provides a high degree of convenience for users of the services and is a key enabler of 'channel shift' for the service providers, helping to move interaction online and away from face-to-face or telephone transactions.

The mobilisation phase of AtPS concluded in December 2009. The clear conclusion from that work was that such a service was feasible, had wide applicability across Government and had a viable delivery mechanism, centred on the Government Gateway.

A team in DWP has been set up with the aim to deliver a 'proof of concept' of AtPS by May 2010. The team is working closely with colleagues in DirectGov, IPS, HMRC and other Government Departments to deliver this. The key objectives of the proof of concept are:

- To deliver a prototype for remote access to online public services
- To develop a plan for moving the proof of concept, if successful, to a production version
- To deliver a supporting strategy for the use of credentials, initially within DWP
- To devise a commercial model for AtPS

RECOMMENDATION 14

The Access to Public Services initiative (AtPS) should include a work strand which focuses on ensuring that fraud prevention is built into this important new shared service.

Staff Fraud

5.17 Developing preventative measures against fraud committed or facilitated by staff is a continuing challenge for both public and private sector organisations. Traditional methods of pre-employment checks still have value but can now be supplemented by other checks. CIFAS has developed a service which allows members to record the details of individuals dismissed for fraud. The service can then be checked to identify 'serial fraudsters' who move from employer to employer.

5.18 Some employees turn to fraud as a result of changes in their personal financial circumstances. Services are being used which can provide alerts based on pre-defined triggers, for example excessive cash withdrawals on credit cards. Some private sector companies combine these checks with other steps, such as monitoring more closely an individual's use of corporate IT systems.

Pre-employment checking - CIFAS staff fraud database

A survey by CIFAS, the UK's Fraud Prevention Service, in December 2004 revealed that there are, on average, 1,500 dismissals a year from 127 organisations as a result of employee fraud. The largest companies dismiss over 100 staff each year. Total UK losses from staff fraud are estimated to be in excess of £40m per annum.

The CIFAS staff fraud database helps employers pre-vet employees to ensure they have no record or history of fraud. Members share information on individuals who were dismissed for fraudulent activity so other members, who are prospective employers of these individuals, can make a more informed decision on employment.

By February 2010, CIFAS had 123 organisations using the service and 620 individuals were recorded on the database. The cases submitted to the database doubled between 2009 and 2010 and this is increasing at 4% per month. The current 'match' rate for members using the service is 2.5%.

5.19 We make recommendations on a staff fraud project both here and in Section 6 of this report.

Credit reference agency – post-employment checking

A credit reference agency offers a service providing daily alerts to enable employers to screen employees on an ongoing basis. The alerts advise when an individual has missed payments (where shared data is permitted for use) or is showing other signs of debt stress, such as registration of county court judgments. This service allows organisations to quickly become aware of when existing employees are facing financial difficulty, move to support them (possibly improving work performance) and reduce the potential for them to commit fraud. There is a wide set of alerts from changes to how accounts are used through to bankruptcy, which allows employers to make risk-based decisions about when problems are sufficiently advanced to merit taking action.

5.20 The vast majority of staff are honest and diligent and have an important role to play in helping to prevent and detect fraud. They are often most familiar with how systems can be exploited by fraudsters and therefore how they might be protected. There may be concerns among staff if wider use is made of financial alerts to flag potential insider fraud risks (see paragraph 5.18), and staff may not be aware of where they can report their suspicions of insider fraud. We therefore recommend that the public sector consider use of externally managed whistle-blowing services such as that provided to many financial institutions by Crimestoppers.

5.21 More broadly we recommend the development of a major civil service and local authority communications campaign to foster an anti-fraud culture. This would seek to win hearts and minds and convince staff of the scale of the fraud problem, the need to fight it and why fraud matters for them, for their organisation and for the public at large. Staff will need to be convinced of this in order that they are ready to accept closer supervision and personal vetting, which could be seen by some as intrusive. Staff also need to accept that they can all play a part in eradicating fraud from their organisation to the ultimate benefit of staff, customers and the population.

RECOMMENDATION 15

To combat staff fraud, we recommend developing a staff engagement workstream and conducting early consultation with frontline staff to help scope the work. This work should also look at the experience of organisations which have used externally-run 'whistle blowing' services, providing staff who report fraud with greater reassurance

Consider incentive regimes when drawing up service contracts

5.22 We were told of the incentive regime which operates between the BBC and a company contracted to collect Television Licence Fee revenue. The company is rewarded in line with increased licence fee revenue. The Television Licence Fee is a rather 'self-contained' tax and the level of collection is less prone to factors which affect other taxes and benefits which are subject to fraud. That said, in certain areas there may be particular opportunities to consider incentive models that take account of external factors, so that an agreed understanding can be reached on whether a supplier's actions have contributed to reductions in fraud loss or revenue increase.

5.23 The specific issue of incentives for the Television Licence Fee led us to consider the wider issue of incentives. We have been told where there are or may be perverse incentives in the public sector to detect and prevent fraud:

- Additional anti-fraud resources are counted against DWP's costs (its Departmental Expenditure Limit), but savings in fraud are realised by the Exchequer as reductions in Annually Managed Expenditure (AME). The Department therefore sees no financial return on its investment in counter fraud measures.
- Business Rates are collected locally and then transferred to the National Non Domestic Rate (NNDR) Pool. This is later distributed to local authorities based upon a fixed amount related to the population. There is currently no incentive for local authorities to investigate NNDR Fraud as they receive no specific financial benefit. The benefit goes to the 'pool' and thence to other authorities. The amount collected for the NNDR in 2008-09 was £18.7 billion.
- The perverse incentive that a local authority discovering a housing benefit fraud 'shares' a financial penalty with DWP. If it does not look for the fraud, it bears no financial loss.

RECOMMENDATION 16

We recommend that perverse counter-fraud incentives (and areas where there is a lack of an incentive) across the public sector are documented. A project should be established to find ways to build incentives which will be much more effective and better understood by staff.

5.24 We have been told that some enforcement targets, for example, achieving a specific number of sanctions against benefit fraudsters, may counteract placing greater emphasis on fraud prevention. Rebalancing public sector efforts to put more emphasis on prevention and disruption will help avoid the risk of increasing burdens on the criminal justice system.

RECOMMENDATION 17

We recommend that any targets which focus on numbers of completed enforcement actions be reviewed and replaced, if possible, by targets that place greater emphasis on fraud prevention.

5.25 In the time available to complete this report we have not been able to compare and contrast relative expenditure on counter-fraud activities in the public and private sectors. This should be considered for the future.

6. IMPROVING PUBLIC SECTOR FRAUD PREVENTION

6.1 There are a number of examples of good practice in detecting, preventing and reducing fraud the public sector. Use is made of some of the techniques and approaches discussed in the previous section. Systems and projects are at different levels of maturity and this section discusses those:

- Which have been implemented or are in the process of being rolled out. These should be sustained and where appropriate the approaches should be spread more widely across the public sector;
- Which have been piloted and appear suitable for wider implementation and could therefore start to make a contribution to additional fraud savings. In the time available we have not been able to verify what the private sector companies told us about the actual or projected benefits in all cases;
- Which have been scoped or piloted but where further work is needed to evaluate the benefits.

Successful approaches to data matching and sharing

6.2 A number of public sector organisations make use of data sharing and matching across their various databases and with other organisations. As with many large private sector organisations, information on customers has been spread across a number of legacy systems which were built with limited capability to share data. Information on customers who may be defrauding the organisation has therefore been spread across 'silos'. The following three examples show the approaches currently being adopted by DWP, HMRC and the Audit Commission.

DWP data matching – 'Centric'

DWP recognised the importance of data matching over 15 years ago as a means of identifying conflicting evidence between information provided on benefit claims and held on other data sources. Consequently, the Department already has in place a well developed data matching service that helps it identify over £100m in overpayments annually. While improvements have been made in cross-benefit interfaces, conflicting evidence can be presented in different applications. With the introduction of new measures, such as tax credits and housing benefit, new areas continue to emerge where cross-checking is required. The data matching service has grown beyond DWP's own data and now includes data from other public sector organisations including local authorities, HMRC, the Office of National Statistics (ONS) and the Home Office. This has allowed a far wider range of data matching to take place. It can identify customers who fail to declare the full extent of their savings or that they have started to work. DWP's data matching capability is currently being enhanced to provide customer-centric data matching. This enables all information held on a customer to be simultaneously matched with all other sources to provide a holistic view of known inconsistencies.

HMRC data matching – 'Connect'

HMRC has developed a data analytics tool known as 'Connect'. Connect is an IT tool which enables HMRC to identify potential tax fraud and broader criminal networks with greater speed and efficiency, while enabling compliant customers to be processed faster and more effectively. Connect is able to uncover the hidden relationships in HMRC's rich reserves of data, as well as linking data from third parties in order to detect tax fraud.

Connect has the capacity to search around a billion records at the touch of a button and links almost thirty databases, including HMRC's multiple databases and the external databases that HMRC traditionally use.

Connect has allowed HMRC to make significant improvements in how it targets its response to fraud. In the period up to 2008/09, implementation costs were in the region of £18.6m, while the increased yield due to the system stood at £572m. Specific savings include:

- VAT – Connect has uncovered £330m of fraudulent claims since June 2008, preventing £151m from being claimed and protecting a further £118m in direct taxes
- Tax credits – Connect has identified organised criminal attacks and prevented revenue loss of around £3.5m a year
- 2007 Offshore Disclosure Facility (ODF) - In 2008, Connect was used to risk assess bank records of 200,000 businesses and individuals, identifying a significant non-compliance yield of tens of millions of pounds.

Local authority data matching – the Audit Commission's 'National Fraud Initiative' (NFI)

Local authorities have embedded data matching techniques via the Audit Commission's NFI. This exercise takes place on a two-year cycle and matches electronic data within and between the Commission's audited bodies to prevent and detect fraud. This includes police authorities, local probation boards and fire and rescue authorities as well as local councils. To date, an estimated £600m in fraud and overpayments has been identified from the initiative.

The data matched for local authorities comprises: payroll, pensions, creditors, housing benefit claims, council tax benefit claims, housing, electoral register, students, residential care homes, transport passes and permits, insurance and licences (traders and taxis). In 2008/09, the initiative identified 2,700 matches per participating body. This included 17,701 housing benefit overpayments, 1,999 pensions to deceased persons stopped; 14,295 council tax single person discounts stopped, 276 employees dismissed/resigned, and 15,184 disabled blue badges cancelled. Across all participants, the value of detected fraud so far in 2008/09 is £140m.

A large metropolitan council has been using a data warehouse for some years and has developed extensive matching and mining processes which are compliant with the Data Protection Act 1998. The datasets used are similar to those used in the NFI however, the Council has extended the project beyond fraud, to include error and to produce efficiency savings. It has undertaken matching exercises with neighbouring boroughs and also conducted payroll cleansing exercises with HMRC. This resulted in identifying employees working under false identities for further investigation.

Some local authorities use the NFI data to undertake other matches. One local authority matched the 'temporary accommodation' datasets against the in-house Housing Common Register. Using two housing investigators for one month they investigated 120 cases and removed 77 customers from the waiting list, 12 of which were able to bid for properties using the points system. The cost of a council house is estimated at £75,000 and the cost of temporary accommodation is estimated at £11,000 per year.

Local authorities also participate in the Housing Benefit Matching Service which matches DWP and HMRC data.

6.3 We were encouraged by the NFI's desire to enhance their data matching to support preventative checks made upfront before grant of benefits or payments, rather than in retrospect (possibly many months after the event). We hope progress will be made quickly in this area.

Joint working between DWP and local authorities – using credit reference agency data

DWP and nine local authorities identified £212,000 savings by matching housing benefit/council tax benefit records against data held by credit reference agencies. The pilot highlighted previously unreported fraud in the following areas:

- Non-residence
- Undeclared non-dependents
- Landlord/tenant relationships
- Possible sub-letting and
- Living together

Following the successful pilot, a national rollout is planned for Spring 2010 which should yield benefits of £40 million over the next three years.

6.4 The NFIB is designed to gather and analyse data on hundreds of thousands of cases of reported fraud to spot patterns in fraudulent behaviour. It is managed by the City of London Police as part of its role as the national lead police force on fraud. The NFIB database is intended to be populated from a large number of public and private sector organisations, representing industry, commerce and Government.

6.5 The NFIB employs analysts from law enforcement and private sector backgrounds to sift through the raw intelligence, searching for distinct patterns of fraudulent activity and behaviour. It uses some of the latest data matching and analytical tools. Currently, reports are dispatched to police forces to help support criminal investigations and improve the local intelligence picture. Thus far, almost all the fraud data in the NFIB is coming from the private sector though there is some public sector content from the Office of Fair Trading (OFT) and the Serious and Organised Crime Agency (SOCA).

Scope to increase data matching and sharing in the public sector

6.6 Public sector agencies lag behind a number of private sector industry groups in their capability and willingness to share intelligence about the people and organisations that are or may be defrauding them. While the larger Departments have data matching and intelligence systems for their own purposes, there is little evidence of routine, systematic sharing of intelligence which we have seen on the scale adopted by the banking and insurance industries. In this report we have chosen not to repeat the well-rehearsed arguments about legislative constraints to information sharing. If such constraints are real, the will should be found to overcome them where information sharing is clearly in the public interest. Cultural inhibitions to information sharing should be challenged at the highest level in Departments.

RECOMMENDATION 18

The public sector should work actively within the NFA Information Sharing Taskforce to overcome blockages to information sharing already identified as impeding the fight against fraud. In some areas, Ministers will need to support legislative change to make this possible.

6.7 The major victims of public sector fraud (HMRC, DWP, local authorities and the NHS) should, as a minimum, be sharing intelligence with the NFIB which already brings together some private sector sources. We are aware that DWP and HMRC are already in dialogue with NFIB, but this has not reached a conclusion.

RECOMMENDATION 19

We recommend that HMRC, DWP, local authorities and NHS sharing of fraud intelligence with the National Fraud Intelligence Bureau (NFIB) is progressed as a matter of urgency, and that a clear mandate is given to all Departments by Ministers to share their fraud intelligence with the NFIB. The NFIB needs to become clearer about the products, services and data it will provide back to data contributors and to law enforcement authorities other than the police.

6.8 There should be no legal obstacles to this arrangement, which will help to ensure that best value for money is obtained from the expenditure already incurred by and committed to the NFIB.

6.9 We are also aware that intelligence on fraud is distributed among a number of different systems. Our recommendation to ensure that intelligence is shared with the NFIB should help to improve this situation. However we believe that a study of what the current situation is, including the new developments for managing the response to serious organised crime could identify some 'quick wins' in parallel with building a strategic solution based on the NFIB.

RECOMMENDATION 20

We recommend conducting a study of the various fraud intelligence systems in the public sector. This should include an analysis of what intelligence is currently shared across the public and private sectors, how it is analysed, and how the results of this analysis are fed back into fraud investigations and the design of new fraud prevention measures.

6.10 Any gaps, overlaps or other deficiencies should be identified and a programme of work agreed to resolve them. This should also consider options for plugging gaps where no intelligence systems are in place. Use of existing facilities as 'shared services' should be the default option for consideration.

6.11 We have identified a specific concern over sharing data on fraudsters who accept administrative penalties, such as cautions and civil penalties as an alternative to court. Such people are fraudsters and information about them should be shared with other counter-fraud organisations.

RECOMMENDATION 21

We recommend that DWP and HMRC share information on non-criminal sanctions against fraudsters with other parties (preferably via the NFIB), subject to recommendation 19 above.

6.12 We recognise that sharing more intelligence about confirmed and suspected fraudsters could raise privacy concerns. We were told that data analytical techniques which employ anonymous matching can realise the benefits of data matching without requiring individuals' details to be held on one system. It also does not require individuals' data to be disclosed between different organisations' systems.

RECOMMENDATION 22

We recommend that the use of data analytical techniques using anonymous matching is explored further for public sector applications.

Successful approaches to prevention

Prevention via lessons learned - DWP's latent failure model

The latent failure model examines the nature of selected recent benefit frauds, how they succeeded and what could be done to prevent a recurrence.

A recent organised attack on the National Insurance number application process was discovered in February 2009, which then led to claims for crisis loans and tax credits. New intelligence-led procedures were introduced which, between August 2009 and February 2010, resulted in around 8,000 suspicious applications being refused.

Student Loans Company (SLC) – improved screening of applications

SLC continues to improve its systems to detect and prevent fraud. For example, it has established electronic links with IPS to establish the identity and status of applicants. SLC is also developing electronic links with HMRC for the verification of household income, the principal parameter used to determine eligibility to means-tested grants and loans. These developments also reduce the burden on applicants to produce documentary evidence.

HMRC - Missing Trader Intra-Community (MTIC) fraud using carbon credits

In its simplest form, MTIC fraud involves obtaining a VAT registration to acquire goods or services VAT-free from other EU Member States. The fraudsters then sell on the goods at VAT-inclusive prices and disappear without paying the VAT to HMRC.

Earlier this year, HMRC intelligence and operational activity identified a real and increasing risk of the UK becoming a major target for a type of this fraud in connection with trading of emissions allowances (carbon credits). In response, legislation was introduced to zero-rate the supply of emissions allowances within the UK with effect from 31 July 2009. This early action was taken to prevent substantial potential losses to the Exchequer and to ensure that fraudulent trading did not undermine the legitimate market. HMRC estimates that significant losses were prevented by this action. Losses from carbon credit-related MTIC in France, prior to similar legislative change, were estimated to be €1.8 billion.

HMRC - tax credit and repayment fraud

Organised fraud within tax credits typically involves external fraudsters using stolen identities to make claims, in some cases 'hijacking' existing claims. HMRC has put restrictions on the availability of claim forms and withdrawn the facility to claim over the internet. In order to strengthen their customer identity verification and authentication capability, HMRC has also introduced an Identity Authentication Service (IDAS) for its tax credit customers.

This system uses a combination of internal and external data sources to assure the customer's identity. Work is ongoing to identify how HMRC can strengthen identity verification and authentication processes across customer segments and for other regimes.

IPS – credit reference agency checks

The IPS 'authentication by interview' initiative requires all first-time passport applicants to attend a personal interview before a passport is issued. First-time applicants present a higher risk of fraud than those renewing their passports. Before the interview, questions are chosen from information derived from credit reference agency data checks. These are much harder for a fraudulent applicant to answer. As a result of these checks, 1,001 passports have not been issued in the 2009 calendar year. Fraudulently obtained genuine passports are of much higher value to fraudsters, as they pass tests designed to identify forged or tampered passports and will also be confirmed by the Passport Validation Service as genuinely issued.

Successful approaches to tackling staff fraud

6.13 The following is an example of action taken by DWP to investigate staff fraud.

DWP – staff investigations

DWP's Risk Assurance Division (RAD) undertake investigations into suspicions of fraud, dishonesty or other serious wrongdoing by any staff working for, or on behalf of DWP. While only a minority of its employees commit such offences, the Department takes fraud and impropriety seriously. It has mechanisms in place to actively detect, prevent and deter staff fraud. Where impropriety is proven, staff are subject to disciplinary action. Where criminal offences are identified, the policy is to prosecute where appropriate.

Allegations of fraud or abuse by staff are referred to RAD by a number of sources including managers, staff and customers. The Department also operates a whistleblowers hotline for staff to raise concerns.

RAD Investigations has a prevention, deterrence and detection unit that undertakes various proactive exercises (for example data matching and mining) to identify staff fraud and abuse. The team undertakes proactive work aimed at detecting inconsistencies as flags for potential fraud and error. They gather information from a variety of sources, including reports from Government Departments, enforcement agencies and information from previous cases.

Some proactive exercises are run regularly to identify potential abuse in areas where historic data suggests there may be ongoing abuse. Other exercises, such as matching staff details against benefit data, are run at intervals where changing circumstances indicate there may be fresh exposure to staff fraud, for example nationwide recruitment exercises. The team also work with various parts of DWP to help address identified weaknesses in controls.

Successful pilots – possible candidates for rollout

6.14 Private sector organisations gave us information about pilots they have conducted with the public sector, or on their own initiative with a view to marketing new solutions and systems in the public sector. Two local authorities succeeded in separate initiatives in reducing fraudulent claims for council tax single person discount.

Local authorities – council tax single person discount

A Local authority in England commissioned a service to identify potentially fraudulent claimants of council tax single person discount (SPD). The software supplier used a four stage verification approach:

- Basic identity checks – undertaken against the full and edited electoral registers and credit reference agency data
- Address verification – checked against council tax records and the Local Land and Property Gazetteer
- Occupancy checks – checked against deceased and 'gone-away' registers along with a 'national false positives' screen to identify additional property occupants
- Additional person verification – credit reference agency checks against landline, mobile telephone, and banking activity registered to the address

Of the 37,000 residents claiming SPD, 6,753 were identified as potential fraud or error. Action was taken on 1,490 of these claimants and the local authority was able to collect an additional £544,000 in council tax. Another local authority in Scotland undertook a similar exercise which resulted in the collection of additional council tax of £1.2m in 2006/07 and £1.25m in 2007/08.

If the above results are indicative of SPD fraud across other local authorities in England, the number of claimants flagged using this approach could exceed 300,000, representing a potential reduction in council tax subsidies of around £90m each year.

An additional 1,800 SPD claimants also in receipt of housing benefit in this local authority were flagged as possible fraud or error, but were not pursued as part of the exercise. If these figures were extrapolated to the rest of England, an estimated 100,000 further people could also be wrongly claiming SPD and housing benefit. Action taken against these could result in further savings of £32 million.

RECOMMENDATION 23

It is recommended that all local authorities implement solutions to prevent 'council tax single person discount' fraud, by making use of credit reference agency and other open source data.

6.15 We were told of other projects and studies which have shown promise for reducing fraud via data sharing. The benefits cases for these are less developed. We therefore mention them to illustrate potential benefits:

- Council tax fraud resulting from 'unknown addresses'. This is where a property has been converted for multi-occupancy without the local authority's knowledge. A data matching trial indicated that matching property details with data from utility companies identified potential fraud.
- Council tax fraud can also be perpetrated by false claims that a property is unoccupied. Data matching can reveal economic activity at a property to indicate that this is not the case and there is a resident liable for council tax.
- The unlawful sub-letting of social housing. Data matching can reveal that the original tenants have moved by showing evidence of economic activity in their names at other addresses.

Promising future developments – awaiting full evaluation

6.16 Beyond the above range of examples, we have been told about a number of very promising new developments which should be further investigated with a view to future implementation.

NFA, City of London Police, DWP and HMRC collaboration on 'accommodation addresses'

Mail forwarding addresses, post office boxes and serviced and virtual offices are all abused by criminals to put distance between themselves and the frauds they commit. The NFA, in collaboration with the City of London Police (CoLP), is leading a multi-agency project to reduce the threat posed by the criminal abuse of these 'accommodation addresses'. The partners in the project, which include the DWP and HMRC, are seeking to construct a single and comprehensive list of such addresses that can be used to make better risk based decisions on awarding benefits or paying claims. Restrictions on data sharing may pose problems to creating this list, but it is anticipated that the relevant data owners will seek gateways to share this valuable information.

Once suspect addresses have been identified, CoLP will take forward tactical operations to disrupt fraudsters and will be looking for collaboration from other law enforcement agencies to resource this work.

RECOMMENDATION 24

We recommend the reduction in fraud threat to the public and private sectors posed by criminal use of accommodation addresses. The solutions to achieve this should be delivered by the NFA-led 'accommodation addresses' project.

DWP – 'Customer Centric' prototype

The DWP's Customer Centric prototype is a proof of concept activity, which went live in October 2008. It aims to redevelop fraud and error matching from a product-based service to a customer-based service.

Key business aims include the:

- Creation and population of a Centric 'data mart'
- Coding of fraud and error rules
- Application of an agreed scoring methodology to referrals
- Provision of a decision support facility for users to manage referral selection
- Provision of a view back facility to give users access to the latest data held for a customer
- Ability to detect all incorrectness at once instead of issuing multiple referrals

The Department will assess any business improvement achieved and the impact upon DWP business processes. It will be used to inform plans to develop the proposed end-to-end solution.

RECOMMENDATION 25

Depending on the result of the assessment, we recommend that DWP implements its proposed new Customer Centric end-to-end solution.

DWP and local authorities – 'voice risk analysis' pilot

Voice risk analysis (VRA) is a risk assurance process employing a combination of three elements: voice stress analysis, intelligent scripting and call handlers specially trained in conversation management and behavioural analysis to enable the detection of truthful statements. VRA is already in use in the private sector, for example in better assessing the risk associated with insurance claims.

The Department made a public commitment to test a VRA process in its 2005 strategy document 'Reducing fraud in the benefit system: achievements and ambitions'. A first stage of an evaluation programme for VRA took place between May 2007 and July 2008 and covered new claims to income support and jobseeker's allowance in Jobcentre Plus and six trials on reviews of existing claims in local authorities. The results across the sites were mixed, however, they were encouraging enough to justify a second phase of extended pilots in local authorities that were designed to provide a broader evidence base.

24 local authorities took part in the extended trial and if it proves successful, the anticipated benefits include:

- Improved risk scoring of new and existing claims for housing benefit, allowing call handlers to apply an appropriate level of verification to claims as they are passed through the system
- Improved identification of high risk cases for further investigation, which will enable better prevention and detection of fraud.
- Improved customer service and efficiency savings, by identifying the low risk claims (approximately 90% of the caseload) which can be 'fast tracked' by receiving a lower level of scrutiny.

Final evaluation of the pilot is planned for spring 2010 when estimates of potential savings may by possible.

DWP new and existing benefit claimants – predictive/innovative analytics

DWP has delivered a proof of concept project which uses live DWP data held in a secure environment. Three companies have been invited to demonstrate what their software can do to identify more potential fraud and error in the data than is found with current methods. As a proof of concept project, the evaluation will not lead to the selection of particular products or approaches.

The anticipated benefits are:

- Improved identification of fraud and error in existing benefit claims, enabling them to be corrected, improve the rate of benefits for underpaid customers and improve the sanction rate for DWP's fraud investigation service;
- Improved identification of potential fraud and error in new claims, enabling those claims to be further investigated before being paid, thus preventing fraud;
- Providing the opportunity for substantial efficiency savings from faster claims processing and also more effective post claims activity;
- Improved customer experience by speeding up the claims process and helping people to receive the right level of benefit.

The three suppliers which participated in the proof of concept offered different approaches. One focused on data preparation to create a single view of a customer across the various benefit systems and used prediction models to score the entire data set for the risk of fraud and error. Another demonstrated the scale and speed of execution that is now possible across large volumes of data, tracking changes of circumstances over an 18 month period of pension credit and job seekers allowance customers. The third supplier focused on better identification of customers who were living together or who were deceased. Evaluation of the results is underway.

Department for Communities and Local Government (DCLG) and local authorities – housing tenancy fraud

The Audit Commission found that housing tenancy fraudsters (people obtaining social housing to which they are not entitled) could be occupying at least 50,000 council and housing association properties worth more than £2bn. Queues for homes have increased by more than 50%.

In 2009, DCLG announced funding of up to £50,000 per local authority to undertake proactive work that would identify unlawful sub-letting, reducing homelessness costs and freeing up accommodation. 148 local authorities have taken up the pilot and the results will be published later this year.

RECOMMENDATION 26

We would encourage the Department for Communities and Local Government (DCLG) and local authorities to pursue their pilots on prevention of housing tenancy fraud. The conclusions and best practice identified should be built into operational implementation solutions as soon as possible.

Student Loans Company (SLC) – prevention by identity and income verification

In October 2009, the SLC carried out checks to help verify the identity and status of applicants who had not supplied details of their UK passport, and separate checks to verify the household income of sponsors.

The results of the pilot are being analysed and early indications suggest these additional checks are a useful complement to the SLC's existing processes.

RECOMMENDATION 27

We note the additional work that the Student Loans Company (SLC) has undertaken to verify identity and income is to be evaluated. Depending on the results, we would advocate implementation and sharing of this best practice elsewhere in the public sector.

DWP and local authorities – real-time verification of applications for housing benefit

Local authorities have piloted a risk assurance tool that risk scores new claims for housing benefit in real time. This potentially allows low risk claims to be fast tracked, while targeting high risk claims that are more likely to contain fraud and error. The initial pilots have indicated that risk assurance tools can deliver efficiency and administration savings of up to £1.5m per annum. These tools also have potential to prevent fraud and error and further live trials are being planned.

The efficiency pilots aimed to:

- Test the existing DWP risk score alongside the risk assurance tool used in the pilot to develop a better overall product
- Allow local authorities to experiment with customised campaigns in a way that is not possible with the current Housing Benefit Matching Service's 'one size fits all' approach
- Test and establish the practicalities of delivering new-claim risk ratings to an assessor's PC desktop in real time
- Synchronise with voice risk analysis (see page 58)

The main conclusions from the pilots have been:

- The risk model correctly differentiated between high, medium and low risk claims within the pilots. On average, 57% of claims were identified as low risk and 23% as high risk
- Risk and claimant information was delivered to the assessor within two seconds at the time of claim
- Processing times for low risk claims were reduced by 37% on average
- Overall claim processing times were reduced by 32% at Glasgow and 12% at Lambeth. Lambeth elected to focus some released resources on visiting all high risk claimants prior to authorising or refusing payment
- Around 1.5% of National Insurance numbers were successfully matched with claims in other local authorities, using a claimant register covering 15% of local authorities spread throughout the UK. This suggests that 10% would match against a full register.

RECOMMENDATION 28

We recommend that DWP evaluate the following pilots and/or initiatives and share their experience with relevant Government Departments and other public services:

- **Voice risk analysis technology**
- **Predictive/innovative analytics**
- **Housing benefit risk assurance tool**

Legal Services Commission (LSC) – tackling legal aid application fraud

People who are in receipt of certain state benefits are automatically entitled to legal aid. The LSC has been working with the DWP to ensure that those granted legal aid on this basis are properly entitled to benefits and thus to legal aid. LSC and DWP are in the process of setting up a joint working procedure which will hopefully culminate in future joint prosecutions, where people have defrauded both organisations. This work will ensure that fraud across multiple agencies is dealt with consistently and will deter future fraudsters through publication of their successes.

Other counter fraud work within the LSC includes a focus on the measurement of fraud. For example the organisation is investigating the screening of legal aid applications which will sit alongside the existing fraud work undertaken after legal aid has been granted. The LSC is also bringing forward measures to notify the opponent when legal aid is applied for in a private law family case in order to verify that the applicant is financially eligible for funding.

In 2010, the LSC secured their first conviction for legal aid application fraud. The LSC has also been working to tackle fraud from within their supplier base, with £1.1m recovered in this area last year.

6.17 This section has demonstrated the wide range of counter fraud activity which is being undertaken by public sector organisations. It has not been possible to cover many other areas of activity of which we have been made aware. What became particularly apparent in our discussions with private sector suppliers is that the same problem is often being addressed by different means in different parts of the country. While it is important not to stifle innovative ideas and approaches, better spreading of good practice would avoid duplication and help local organisations become better customers of the various services on offer.

7. POTENTIAL FRAUD SAVINGS

7.1 We have produced an estimate of savings which would be possible if the good practice examples discussed in this report were implemented more widely. We have estimated additional savings over and above those which could be attributed to HMRC and DWP, which already have better established counter fraud strategies than other parts of the public sector.

7.2 Due to the maturity of the counter-fraud approaches of HMRC and DWP, we have treated these Departments separately in our calculations. We have used figures agreed with HMRC which reflect dialogue which has already taken place with HM Treasury in reducing the tax gap. In the case of DWP, we have agreed the basis of a calculation which assumes that they will meet challenging targets already set for benefit fraud reduction in 2010/11 and that they will continue with a similar level of performance over the following two years.

7.3 We then determined the proportion of the £25 billion estimate of public sector fraud, which falls outside of the scope of HMRC and DWP. This figure is formed from an expenditure fraud estimate and a 'non-HMRC' tax fraud estimate (including, for example, council tax and business rates). To these figures, we applied some of the more reliable figures provided by public and private sector organisations on the percentage of fraud losses reduced by deploying examples of the good practice discussed in this report. We have concluded that 10-20% is a realistic and achievable range.

7.4 Savings higher than this 10-20% range can be achieved particularly in areas where there has been little or no counter-fraud work to date. A 60% reduction was quoted in one area of NHS fraud after effective action had been taken. However where counter-fraud work is already well established and some reductions in fraud have already been made, it will be more difficult to achieve further higher percentage savings.

Table 3 shows the annual reduction in fraud losses that we estimate could be achieved by 2012/13.

Table 3 - Reduction in Fraud Losses by 2012/13

Area of Reduction	Estimated Fraud Loss 2010/11 (£billions)	10% Reduction (£ billions)	20% Reduction (£ billions)
Expenditure (excluding DWP reductions)	£6.0	£0.60	£1.21
Taxes (excluding HMRC reductions)	£2.6	£0.26	£0.52
DWP	£1.1	£0.11	£0.21
HMRC	£15.0	£1.50[6]	
Total Fraud Reduction	**£24.7**	**£2.47**	**£3.43**

7.5 We needed to take into account that new counter-fraud interventions can take time to implement, especially if they involve changes to systems or working practices. They also require some up-front investment. We have drawn on public and private sector data to estimate implementation costs. We have used a conservative estimate of a ratio of cost to savings of 1:10. We have been told of projects that have achieved a ratio as high as 1:30.

7.6 The details of our calculations are shown in Annex D. They take into account both implementation cost and the speed of roll out. We have made calculations based on a 10% and 20% savings estimate. Both show that a progressively greater amount of fraud savings are achieved each year as new systems and approaches roll out.

7.7 We have not taken into account that there may be a displacement effect as fraudsters redirect their attacks to different areas, in response to stronger prevention and detection methods.

[6] Due to the complexity of tax fraud and the difficulties in countering this type of fraud, a more conservative estimate of a 10% reduction has been applied across both the 10% and 20% savings estimate.

7.8 The estimated aggregate total gross[7] saving in fraud losses over the next three financial years is:

- £4.8 billion and £6.7 billion which we believe is realistic and achievable.
- Excluding the contribution of HMRC and DWP, the estimate of additional three year public sector fraud savings, is £1.6 billion to £3.2 billion.
- The year three figures represent 'steady state' and should be replicated in future years. They amount to £2.5 billion to £3.4 billion per annum in total, or £0.9 billion to £1.7 billion per annum, excluding the HMRC and DWP figures. This is provided there is continued investment in counter-fraud measures.

7.9 As with the 'top-down' estimate produced for overall public sector fraud losses discussed in section 2, we have chosen not to attribute these additional savings to particular Departments or public services. However, we believe it is reasonable to assume that a significant proportion of these savings could be achieved by cross-cutting work on frauds which affect a number of Departments. Procurement and staff costs account for 29% and 25% respectively of Total Managed Expenditure (TME) by the public sector. If we assume that fraud losses are approximately in proportion to expenditure, a considerable amount of estimated additional fraud savings could be targeted by projects in these two areas alone.

7.10 We believe that the following organisations comprise a significant share of procurement and staff expenditure in the public sector. They are:

- Department for Business Innovation and Skills
- Department for Children, Schools and Families
- Department for Work and Pensions
- HM Revenue and Customs
- Local authorities
- Ministry of Defence
- National Health Service and Department of Health
- Department for Transport

[7] These are gross costs which do not take account of the cost of implementing new counter fraud measures. If these are taken into account, the net saving figures would be £4.7 billion to £6.3 billion over the next three years and £2.4 billion to £3.3 billion per annum thereafter.

7.11 Public sector organisations are particularly vulnerable to procurement fraud and to fraud perpetrated by contractors delivering outsourced services and products. This may include procurement frauds perpetrated by staff working in collaboration with contractors as well as contractors fraudulently invoicing for work not done or exaggerating the cost of what has been done. It also includes fraud committed by self employed staff working within the public sector, including the NHS.

RECOMMENDATION 29

Those public sector organisations which have the largest proportion of expenditure on procurement and which make greatest use of contractors to provide outsourced services and products, should be involved in a scoping project to agree ways to reduce and prevent procurement/contractor fraud.

7.12 As mentioned earlier in this report, the private sector would seem to have a stronger focus than the public sector on staff/insider fraud. The public sector should consider employing a similar approach to that operated by CIFAS, building a database of employees dismissed for committing fraud against the public sector, which could then be checked when taking employment decisions. The public sector should also consider taking the private sector lead and evaluating the benefits of services which produce alerts based on employees' changes of circumstances. Other aspects of staff fraud, including payroll and expenses fraud are also of concern.

RECOMMENDATION 30

We recommend that the public sector organisations who have the largest proportion of expenditure on staff should be involved in a scoping project to reduce and prevent staff/insider fraud.

7.13 We have noted some good examples of case working at a local level, for example by DWP and local authority housing benefit teams. At present local authorities can find themselves responding to a number of nationally inspired initiatives. If resources allow, we see benefit in taking a local holistic approach to reducing fraud against all the services in a locality – whether they are locally or centrally administered. Such activity should be informed by a joined-up local fraud intelligence picture and it may therefore be better to wait until further progress has been made on agreement to share such intelligence with the NFIB.

RECOMMENDATION 31

We recommend that, if resources allow, consideration should also be given to a regional pilot to determine the benefits of closer working across all counter fraud agencies in a specific location. Such a project may be more effective when there has been further progress on agreements to share intelligence via the NFIB.

7.14 We have also noted that investment may be needed in new facilities such as services provided by credit reference agencies. We have been told by service providers that the public sector market is fragmented. They would welcome exploring options for making it more straightforward for public sector organisations, especially smaller ones, to make use of their services and draw on framework contracts or shared services.

RECOMMENDATION 32

We recommend a study to determine the feasibility of establishing framework contracts with credit reference agencies to make it simpler and more cost effective for smaller public sector organisations to make use of these services.

7.15 Some of the recommendations in this report encourage making more extensive use of existing 'shared services' such as the NFIB. However we are concerned that there may be reluctance to fund some of the projects and activities we have suggested. This would be short-sighted.

RECOMMENDATION 33

The current spending round comes to an end in the next financial year. We therefore recommend that HM Treasury encourages Government Departments to identify resources that could be made available for this coming financial year only, which can fund participation in the cross-cutting projects described in this report.

8. DELIVERING CONCERTED ACTION

8.1 Public sector organisations face common fraud threats. As we have said elsewhere, the recommendations in this report are a package. A cross-Government collaborative response is needed, underpinned by a clear will and commitment to engage and share more information about fraud within the public sector and with the private sector.

8.2 The NFA stands ready to coordinate this work but it needs to be funded and empowered to do so with a clear mandate, appropriate governance arrangements and Ministerial oversight of the programme.

8.3 These governance arrangements should be closely integrated with other programmes, for example in the Digital Delivery agenda, to ensure that fraud prevention measures are integrated into online Government services and that other work on identity verification and data sharing is consistent with the counter-fraud agenda.

8.4 We have sought to spell out the actions needed to deliver against each of the recommendations. In some cases the outcome can be quickly realised while in others it will take time and discussion to identify the outcomes.

8.5 We recommend that there should be six-monthly checkpoints to ensure work is proceeding with the appropriate pace.

ANNEX A: MEMBERSHIP OF THE SENIOR OVERSIGHT GROUP AND TASKFORCE

Senior Oversight Group

Dr James M. Hart CBE QPM	Independent Chair
Dr Bernard Herdan	National Fraud Authority
Nick Starling	Association of British Insurers
Andrew Campbell	Department for Communities and Local Government
John Oliver	Department for Work and Pensions
David Barr	Department for Work and Pensions
Bob Alexander	Department of Health
Mike Eland	HM Revenue and Customs
Mel Groves	Jobcentre Plus
Paul Smee	UK Payments Council

Taskforce Members

Stephen Harrison	National Fraud Authority
Sanjay Mackintosh	National Fraud Authority
Amie Jefferies	National Fraud Authority
Peter Ratcliffe	National Fraud Authority
Gbemisola Dipeolu	National Fraud Authority
Jyoti Kataria	National Fraud Authority
Alexandra Moore	National Fraud Authority
Clare Bradley	National Fraud Authority
Garvin Bowen	Department for Work and Pensions
John Fitzpatrick	Department for Work and Pensions
Ken Green	Department for Work and Pensions
Rachael Tiffen	Enfield Borough Council
David Margree	HM Revenue and Customs
Penny Thorne	HM Revenue and Customs
Emma Page	NHS Counter Fraud Service
Martin Wiles	NHS Counter Fraud Service

ANNEX B: ORGANISATIONS CONTACTED DURING THE STUDY

Aviva
Barclays
Birmingham City Council
Callcredit
Capita
CDMS - Transactis
CIFAS
City of London Police
Data Discoveries Managed Analytics
Department of Business Innovation & Skills
Detica
Driver & Vehicle Licensing Agency (DVLA)
Equifax
Experian
GB Group
HBOS
HSBC
IBM
Insurance Fraud Bureau (IFB)
Identity & Passport Service (IPS)
Legal Services Commission
Ministry of Defence (MoD)
Office of Government Commerce (OGC)
PriceWaterhouseCoopers
Royal Bank of Scotland
Royal Bank of Scotland Insurance
Royal Borough of Kensington & Chelsea
SAS
Serious Organised Crime Agency (SOCA)
Student Loans Company
Synectics Solutions
UK Payments Council

ANNEX C: METHODOLOGY FOR CALCULATING PUBLIC SECTOR FRAUD LOSS ESTIMATE

C1. A 'top-down' approach has been used to produce an estimate of public sector fraud loss for the purpose of this report. Table 4 provides a summary of this fraud loss estimate.

Table 4 – Estimated public sector fraud loss 2010/11

	Expenditure / Revenue *(£ billions)*	**Applied Fraud Rate** *(Percent)*	**Estimated Fraud Loss** *(£ billions)*
Total Managed Expenditure 2010/11			
Total Managed Expenditure (excluding DWP AME[8])	£548.5	1.1%	£6.0
Work and Pensions AME	£153.2	-	£1.1
Total Managed Expenditure	£701.7	-	£7.1
Net Taxes and NI Contributions 2010/11			
HM Revenue and Customs	£423.1	-	£15.0[9]
Non-HM Revenue and Customs	£75.7	3.3%	£2.6
Total Net Taxes and NI Contributions	£498.8	-	£17.6
Total Estimated Public Sector Fraud Loss 2010/11			**£24.7**

[8] Annually Managed Expenditure
[9] The estimated fraud loss figure for HMRC is a figure already agreed with HM Treasury and therefore not part of a fresh calculation for this report.

C2. This estimate has been calculated by applying an estimated fraud rate to the planned Total Managed Expenditure (TME) and expected tax and national insurance contributions for 2010/11. Revenue ('tax') fraud typically shows a higher percentage loss rate than types of expenditure fraud such as benefit fraud. Therefore separate fraud rates for expenditure and tax have been calculated by:

(i) Looking at specific areas of public finances where we were confident that sound measurement exercises of fraud losses had been made;

(ii) Estimating a typical percentage loss based on the loss percentages identified in (i) above. This was not a simple averaging exercise. For example we excluded outlying figures where unusually high percentage losses had been found.

Calculating fraud loss within Total Managed Expenditure

C3. Robust fraud estimates covering 13 areas of expenditure were reviewed in order to calculate an average fraud loss rate. The total identified fraud loss across these areas was £1.3 billion compared to expenditure of £115.8 billion. This equates to an average fraud loss rate of 1.1% of expenditure.

C4. The planned TME for 2010/11 is £701.7 billion[10]. Reliable estimates for benefit fraud have already been published by DWP and so it was not necessary to calculate a top-down estimate of benefit fraud. DWP's Annually Managed Expenditure (AME) was separated from TME for 2010/11 to ensure benefit fraud was not counted twice in this fraud loss estimate.

Expenditure fraud estimate (excluding benefit fraud)

C5. Planned AME spend for 2010/11 for DWP is £153.2 billion[11]. This AME spend has been deducted from 2010/11 TME. No further adjustments were made to the remaining TME of £548.5 billion. An estimated fraud loss of £6,034 million has been calculated by applying a fraud rate of 1.1% to £548.5 billion.

[10] HM Treasury - Public expenditure statistical analyses 2009. Table 1.1, page 26
[11] HM Treasury - Public expenditure statistical analyses 2009. Table 1.5, page 29

Expenditure fraud estimate (benefit fraud only)

C6. Benefit fraud is one of the few areas of Government spending where reliable fraud estimates exist. The most recent figures published by the DWP show that benefit fraud losses in 2008/09 were £1.1 billion, accounting for 0.8% of all benefit spend in 2008/09. For the purpose of this fraud estimate, it has been assumed that benefit fraud losses will remain the same in 2010/11.

Calculating fraud loss within tax and NI contributions

C7. HMRC, DVLA, the BBC and the Audit Commission all produce estimates in relation to lost revenue resulting from the fraudulent evasion of tax and duties. Based on the most recent fraud estimates provided by these organisations, tax fraud accounted for lost revenue of £15.3 billion. This equates to around 3.3% of total revenue across these four areas. Fraud estimates produced by the NHS in relation to patient charge evasion were excluded from this fraud rate calculation as the percentage of lost revenue was significantly higher than other fraud estimates.

C8. Income from tax and national insurance contributions is estimated at £498.8[12] billion for 2010/11. This figure takes into account tax receipts processed by HMRC as well as tax collected outside of HMRC. Estimates of tax fraud falling within the remit of HMRC have been treated separately for this estimate of fraud.

Tax fraud estimate (excluding HMRC)

C9. Because there are some taxes and duties processed outside of HMRC (for example council tax, business rates, vehicle excise duties etc) a separate fraud estimate has been calculated for these taxes. These additional taxes have been projected to generate income of £75.7 billion in 2010/11. This projected figure of £75.7 billion has been adjusted to £78.3 billion to take into account revenue that would otherwise have been collected, had payment of taxes and duties not been avoided fraudulently. Applying an estimated revenue fraud rate of 3.3% to £78.3 billion equates to a fraud loss of £2.6 billion.

[12] HM Treasury - 2009 Pre-Budget report: the economy and public finances – supplementary material. Table 2.9, page 40.

Tax fraud estimate (HMRC)

C10. The size of the UK tax gap is estimated to be around £40 billion in 2007/08. If it is assumed that the categories of 'evasion', 'hidden economy' and 'criminal attacks' equate to fraud, then the fraudulent element of this tax gap can be estimated at £15 billion. For the purpose of this fraud estimate, fraud relating to tax and duties collected by HMRC is estimated at £15 billion as per HMRCs tax gap estimate published in December 2009. We have therefore used this figure as there was no need to make a fresh calculation.

ANNEX D: METHODOLOGY FOR CALCULATING PROJECTED SAVING FIGURES

D1. In identifying projected fraud savings, two estimates have been calculated assuming a 10% and 20% reduction in fraud losses. Because these reductions apply over a three year period it is necessary to calculate cumulative fraud savings to quantify the full financial impact of counter fraud interventions. Table 5 provides a breakdown of projected savings.

Expenditure and tax projected savings (excluding DWP and HMRC reductions)

D2. The figures presented in section A and B of Table 5 represent projected savings between 2010/11 to 2012/13 (excluding DWP and HMRC savings), taking into account both new and continued savings. In calculating the realisable savings between 2010/11 and 2012/13, it has been assumed that in year one, 25% of the reduction outlined in Table 3 (page 66) will be met, in year two, 50% will be met and by year three the full fraud reduction will be realised. The 'new savings' and 'continued savings' in section A and B do not take into account the cost of implementing and managing counter fraud interventions. Instead, this is accounted for in the 'net savings' total for section A and B which combines new and continued savings but deducts 10% in order to give a net realisable benefit.

DWP and HMRC projected savings

D3. A similar approach has been taken in calculating cumulative fraud savings to DWP and HMRC reductions in fraud (as shown in section C and D of Table 3). However to take into account more mature counter fraud processes within DWP and HMRC, reductions in fraud have been spread equally across the three years. Cumulative savings have been factored into the savings calculation in the same manner as for non-HMRC and DWP savings. Note that these figures do not take into account the cost of counter fraud interventions. It is assumed that a similar level of funding allocated to DWP and HMRC for counter fraud work will continue throughout this three year period.

Table 5 - Cumulative fraud savings 2010/12 to 2012/13 assuming 10% and 20% reduction in fraud losses

		10% Reduction				20% Reduction			
		Year One (2010/11) *(£ millions)*	**Year Two** (2011/12) *(£ millions)*	**Year Three** (2012/13) *(£ millions)*	**Total** *(£ millions)*	**Year One** (2010/11) *(£ millions)*	**Year Two** (2011/12) *(£ millions)*	**Year Three** (2012/13) *(£ millions)*	**Total** *(£ millions)*
Section A - Expenditure Savings Excluding DWP Savings	New Savings	£151	£226	£226	£603	£302	£453	£453	£1,207
	Continued Savings	£0	£151	£377	£528	£0	£302	£754	£1,056
	Total Savings	£151	£377	£603	£1,131	£302	£754	£1,207	£2,263
Section B - Tax Savings Excluding HMRC Savings	New Savings	£65	£97	£97	£258	£129	£194	£194	£517
	Continued Savings	£0	£65	£161	£226	£0	£129	£323	£452
	Total Savings	£65	£161	£258	£484	£129	£323	£517	£969
Section A and B - Total	Net Savings	£194	£485	£776	£1,454	£388	£969	£1,551	£2,908
	Gross Savings	£215	£539	£862	£1,616	£431	£1,077	£1,723	£3,231
Section C - DWP Savings*	New Savings	£35	£35	£35	£105	£70	£70	£70	£210
	Continued Savings	£0	£35	£70	£105	£0	£70	£140	£210
	Total Savings	£35	£70	£105	£210	£70	£140	£210	£420
Section D - HMRC Savings*	New Savings	£500	£500	£500	£1,500	£500	£500	£500	£1,500
	Continued Savings	£0	£500	£1,000	£1,500	£0	£500	£1,000	£1,500
	Total Savings	£500	£1,000	£1,500	£3,000	£500	£1,000	£1,500	£3,000
Section C and D - Total	Net Savings**	-	-	-	-	-	-	-	-
	Gross Savings	£535	£1,070	£1,605	£3,210	£570	£1,140	£1,710	£3,420
Total Savings	**Net Savings**	**£729**	**£1,555**	**£2,381**	**£4,664**	**£958**	**£2,109**	**£3,261**	**£6,328**
	Gross Savings	**£750**	**£1,609**	**£2,467**	**£4,826**	**£1,001**	**£2,217**	**£3,433**	**£6,651**

* These are estimates of potential savings, not target savings

** As net saving figures are not available for DWP and HMRC figures, the total net savings figure combines gross HMRC and DWP figures with net 'new' savings.

National Fraud Authority

National Fraud Authority
PO Box 64170
London
WC1A 9BP

www.attorneygeneral.gov.uk/nfa

T: 020 3356 1000