

Eliminating Public Sector Fraud

The Counter Fraud Taskforce
Interim Report

Contents

Foreword by the Prime Minister	1
Foreword by Francis Maude MP	2
Executive summary	3
Introduction	5
Public sector fraud – more than just benefit cheats and tax evaders	7
Pilots delivering immediate savings	8
Key findings by the Taskforce	10
Implementing a collaborative approach	12
Proposals going forward	13
Priority 1: Collaboration	13
Priority 2: Assessment of risk and measurement of losses	13
Priority 3: A focus on prevention	14
Priority 4: A zero tolerance approach	15
Next steps for the Taskforce	16
Annex 1: National Fraud Authority Annual Fraud Indicator 2011	17
Annex 2: Summary of pilots	18

Foreword by the Prime Minister

Every year in the UK, fraud costs public services an estimated £21 billion. This represents a terrible misuse of money – money that should be spent on schools, hospitals and frontline staff.

Last summer, I announced a crackdown on the £1.5 billion being lost to benefit and tax credit fraud each year. I am pleased with the progress we have made in implementing the reforms that will start tackling this legacy, though there is clearly much still to be done. We must now go further and tackle the problem affecting the whole of the public sector. It is deeply unfair to allow opportunist fraudsters and organised criminals to steal money that should be used for frontline services, especially at a time when we have had to ask many in the public sector to make difficult decisions to bring the economy back on track. Our responsibility is to tackle public sector fraud and to stop it now.

Last autumn, I asked Francis Maude to tackle all types of fraud affecting the entire public sector. I am encouraged by the progress made by the Taskforce he has established. We must deliver the collaborative approach called for across government to stop fraud and ensure that there is a common defence against it across the whole of the public sector.



A handwritten signature in blue ink that reads "David Cameron".

Foreword by Francis Maude MP

Minister for the Cabinet Office and Paymaster General

Since establishing the Counter Fraud Taskforce in October 2010, I have been alarmed at the prevalence of fraud we have discovered across government. It has numerous guises such as overpayments to suppliers, fraudulently claiming benefits or false applications for public grants. HM Revenue and Customs (HMRC) estimates that there is at least £15 billion each year not paid to the Exchequer due to tax evasion. The National Fraud Authority estimates that £2.4 billion is lost to procurement fraud and £515 million is lost to grant fraud each year. The Department for Work and Pensions loses more than £1 billion each year to benefit fraud. Local government loses £2.1 billion each year to fraud. That means 3 pence of every pound spent by the Government goes to people who should not have it.

This is simply not good enough. No business in the world would put up with this scale of fraudulent activity, but its continuance is symptomatic of the situation whereby, for far too long, no one has concentrated on how to run the machinery of government properly. In the work of the Efficiency and Reform Group – co-chaired by myself and the Chief Secretary to the Treasury, Danny Alexander – we have tried to remedy this. We have renegotiated government contracts; cut spending on consultancy, advertising, property and ICT; and established the Major Projects Authority to centrally manage high-value government projects. We have also now started to address the important issue of tackling fraud.

The Taskforce has overseen eight pilot projects which have shown immediate and startling results. We have seen HMRC prevent £10.63 million of payments to potentially fraudulent tax credit applicants, and detect and stop payments of £1.5 million to existing tax credit recipients falsely claiming to be living alone. The Department for Transport has detected £0.5 million in overpayments to suppliers in just three months. On these pilots alone, we can save £1.5 billion over the next two to four years.

Over the next six months, the Taskforce will translate these recommendations into a concrete implementation plan for roll-out across Whitehall and the wider public sector. It will also start investigations into how to reduce the level of error (both by officials and by the public) and how to drastically improve how much and how quickly government collects debt.

We no longer accept that fraud is inevitable. Fraud can be defeated, but only if we adopt an all-pervasive, sustained, zero tolerance culture. It is time to end the 'pay first, check later' status quo and start putting £21 billion of taxpayers' money to better use.



Francis Maude.

Executive summary

The Taskforce on Fraud, Error and Debt was established in late 2010 to create a high-level, cross-Whitehall group to address the enormous level of unacceptable losses. The focus of its first report is combating fraud. The Taskforce brought together fraud professionals from both the private and public sector. It oversaw eight pilots that tested new approaches to tackling fraud, including the more efficient use of credit reference agency information, the deployment of data analytics, and the use of insights from behavioural science to improve how fraud is combated.

In January 2011, the Cabinet Office set up a network of Counter Fraud Champions (CFCs) drawn from every department to help strengthen the fight against fraud in the public sector and support the work of the Taskforce.

The attack on fraud forms one of the cornerstones of the Government's efficiency and reform agenda. After the formation of the Coalition in May 2010, the Minister for the Cabinet Office established the Efficiency and Reform Group (ERG), in order to support departments' efforts to reduce waste and spending in a coordinated approach. The ERG's focus includes procurement, ICT, property and suppliers, alongside fraud. All have a critical role to play in driving efficiency, with fraud potentially being one of the biggest contributors to removing wasteful government expenditure during this parliament and beyond, helping departments deliver the savings set out in the Spending Review.

Tackling public sector fraud alone is a huge challenge, with around £21 billion being lost each year. With public services and welfare facing cuts to reduce the deficit this situation can simply no longer be tolerated. The Government has already published a comprehensive strategy for tackling fraud and error in the benefits and tax credits system¹ and HMRC has strategies in place to target those who fail to pay their fair share of tax. But we need to go further. This report signifies a step change in how seriously the Government is now taking fraud. Fraud can be defeated, but only if we adopt an all-pervasive zero tolerance culture, ending the 'pay first, check later' culture, and take a coordinated approach to addressing the problem across Government.

Fraud affects all departments and, while fraud against the tax and benefits systems accounts for the most considerable losses, there are significant losses relating to other forms of expenditure such as procurement and grant fraud. There are also huge opportunities to reduce fraud through better coordination across Whitehall, between Whitehall and the rest of the public sector, and indeed between the public and private sectors.

¹ *Tackling Fraud and Error in the Benefit and Tax Credits Systems*, DWP and HMRC, October 2010

In this interim report the Taskforce has agreed four priorities for tackling public sector fraud:

- **Collaboration** – silos must be removed; all parts of the public sector must work together by: sharing intelligence on fraudsters; developing cross-cutting capabilities; initiating joint projects using data analytics; and ensuring we jointly procure data analytics to drive down costs.
- **Assessment of risk and measurement of losses** – fraud risk must be assessed before projects and programmes are under way. Losses should also be recorded and reported via the quarterly data summary.
- **Prevention** – investment and resource should go into prevention, not just detection and punishment. When vulnerabilities are detected as part of risk assessment, they should be designed out.
- **Zero tolerance** – there is no acceptable level of fraud.

Taken together, these priorities will enable the Government not only to prevent fraud but also to detect, deter, correct and punish offenders. In this way the Government's response can mirror the nature of the challenge: fraudsters attack the public sector across the board and exploit government processes at their weakest points; to combat this threat will require unprecedented cross-government collaboration.

The Taskforce has made a good start in initiating a more concerted and joined-up approach to tackling fraud and has already identified a number of proposals for action to deliver against these goals. But this is only a start. Greater energy, collaboration and an approach that prioritises preventing fraud is needed. This challenge will begin to be addressed over the next six months as the Taskforce moves to translating these proposals into final recommendations with a clear implementation plan.

Introduction

The National Fraud Authority (NFA) estimates that fraud alone costs the public sector around £21 billion a year. That is 55% of the nation's total fraud loss. The bulk of the fraud loss is due to fraud against the tax and benefits systems but the Government is also losing significant sums to procurement fraud and grant fraud. Local government is also under significant threat. Figure 1 shows the full breakdown of public sector fraud.

Figure 1: Annual Fraud Indicator 2011: public sector fraud loss estimates

Area	Total fraud loss	Fraud type	Fraud loss
Tax	£15 billion	Tax fraud	£15 billion
		Vehicle excise fraud	£46 million
Central government	£2.6 billion	Procurement fraud	£1.5 billion
		Grant fraud	£472 million
		Television licence fee evasion	£196 million
		Payroll and recruitment fraud	£177 million
		NHS patient charges fraud	£165 million
		Student finance fraud	£31 million
		Pension fraud	£7 million
		National Savings and Investments fraud	£0.39 million
Local government	£2.1 billion	Housing tenancy fraud	£900 million
		Procurement fraud	£855 million
		Payroll and recruitment fraud	£152 million
		Council tax fraud	£90 million
		Blue Badge Scheme abuse	£46 million
		Grant fraud	£43 million
		Pension fraud	£8 million
Benefits and tax credits	£1.5 billion	Benefits fraud	£1 billion
		Tax credits fraud	£460 million

The theft of taxpayers' money on such a huge scale has a direct impact on reducing the resources that can be spent on frontline services. Every pound stolen from government means that there is less to spend on health, education, policing and defence. Reducing fraud is also a matter of fairness: every false benefit claim reduces the amount available to those deserving of government support and every false tax return means that more money needs to be raised from the honest citizen. Much of the money defrauded from government ends up in the pockets of organised criminals to fund other illicit and harmful activities.

In the current economic environment, losses due to fraud are even more unacceptable. As the public sector is forced to cut back spending, tackling fraud offers an efficient way to achieve the Government's number one priority of reducing the deficit.

Public sector fraud – more than just benefit cheats and tax evaders

Tax fraud is the highest area of public sector fraud loss and includes around £7 billion from tax evasion and about £3 billion of tax lost as a result of the hidden economy, as well as around £5 billion from criminal attacks. HMRC collects over 90% of all tax that is theoretically due, but the Government has recycled £900 million of HMRC's Spending Review savings into tackling tax avoidance, evasion and criminal attacks to reduce the gap to 7%. This will bring in up to £7 billion per annum by 2014/15 in additional tax revenues. Likewise, the Government has already published a comprehensive strategy for tackling fraud and error in the benefits and tax credits system, where fraud losses are £1.5 billion.

In its 2011 Annual Fraud Indicator, the NFA demonstrated the broader impact of fraud affecting the public sector. This report estimated that:

- **£2.4 billion is lost to procurement fraud each year.** Procurement fraud can take place during the contracting phase or after a contract has been awarded. Examples include collusion between suppliers to fix the price of goods or services provided to the public sector, through to false or duplicate invoicing to receive multiple payments on existing contracts.
- **£515 million is lost to grant fraud each year.** Grant fraud can range from applications from fictitious organisations or individuals for public funds, to multiple fraudulent applications to numerous grant distributors. It also extends to grants awarded that are not used for the purpose of the application.
- **£329 million is lost to payroll and recruitment fraud each year.** Payroll fraud can occur when unauthorised changes are made to payroll systems, such as the creation of false payees or amendments to salary payments or allowances. Recruitment fraud can occur when false information is provided in order to gain employment, for example lying about employment history and qualifications, or providing false identification documents demonstrating the right to work in the UK.
- **£165 million is lost to NHS patient charges fraud each year.** Patient charges fraud occurs when patients falsely seek exemption from paying NHS charges or falsely claim entitlement to free services. An example is where a patient falsely claims to be in receipt of Income Support in order to avoid paying the NHS prescription charge.

Pilots delivering immediate savings

The Taskforce has overseen a series of pilots aimed at driving out wasteful expenditure and identifying techniques that can be applied across the public sector. Details of these pilots are set out at Annex 2. Between them they are anticipated as saving around £1.5 billion over the next four years, and they have already made cashable savings by preventing or detecting fraud:

- **HMRC prevented losses of £10.63 million²** and expects to save £256 million over the next four years by rolling this procedure out across all new tax credit applications. HMRC invested £1 million, secured from government contract renegotiations with an IT supplier, in an innovative screening technique for tax credit applications. The tool analyses information provided by prospective claimants on their tax credit application form, compares this against internal and external data (e.g. credit reference agency data) and decides the likelihood of the application being fraudulent. HMRC piloted the exercise on approximately 4,000 new tax credit applications to test proof of concept and subsequently piloted the new process, preventing losses of £10.63 million between September 2010 and March 2011.
- **HMRC saved £1.5 million of losses and expects to save in the region of £700 million** over the next two years by undertaking the checks across tax credits. **The Department for Work and Pensions (DWP) expects to save £0.5 million of losses** from the pilot and £490 million over the next four years. HMRC and DWP commissioned credit reference agencies to verify the circumstances of 20,000 each of benefit and tax credit claimants, in order to identify those making claims that did not reflect their correct circumstances.
- **The Department for Transport (DfT) saved £0.5 million of losses from payments made to suppliers in one year.** With government spending £66 billion on procurement in 2009/10, applying these techniques across all departments could identify and recover **£264 million** on just one year of spending. DfT commissioned a data analytics company to undertake an audit on their group procure-to-pay systems, to detect and recover overpayments to suppliers. Analysis of one year of spend data has detected £0.5 million in overpayments by DfT, the Driving Standards Agency and DVLA. This is now being recovered by the company on a 'payment by results' basis, and they expect to identify and recover up to £8 million once the analysis is completed across the entire DfT family over six years of payments to suppliers. The Home Office undertook the same exercise and recovered £4 million in overpayments.

² Savings referred to are derived from the pilot exercise, calculated by officials and are not assured figures.

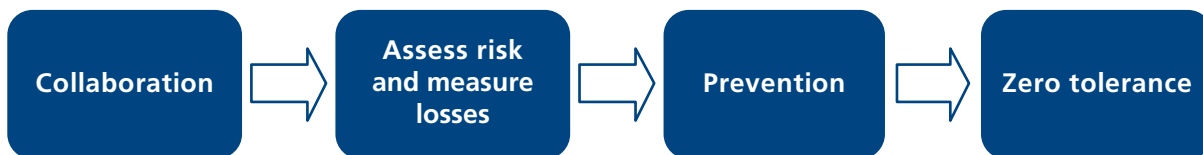
- **HMRC prompted 1,575 people to pay their tax on time using behavioural techniques.**

HMRC estimates a 5% improvement would lead to **£125 million** reaching public coffers earlier, with HMRC having to deal with 50,000 fewer debts. HMRC sent text messages to 31,500 people who were late paying tax by more than £1,000 in 2009/10. The exercise prompted a 5% improvement in behaviour, increasing tax yield by £180,000 and making additional savings in debt management and related costs. Currently, around 1 million people are late paying their tax each year.

Key findings by the Taskforce

The Taskforce has identified that fraud is a common threat across government and requires a common defence in order to prevent, detect, deter, correct and punish fraud. Four priorities will help to deliver against these strategic objectives (Figure 2):

Figure 2: Priorities for action



- **Collaboration** – silos must be removed; all parts of the public sector must work together by: sharing intelligence on fraudsters; developing cross-cutting capabilities; initiating joint projects using data analytics; and ensuring we jointly procure data analytics to drive down costs.
- **Assessment of risk and measurement of losses** – fraud risk must be assessed before projects and programmes are under way. Losses should also be recorded and reported via the quarterly data summary.
- **Prevention** – investment and resource should go into prevention, not just detection and punishment. When vulnerabilities are detected as part of risk assessment, they should be designed out.
- **Zero tolerance** – there is no acceptable level of fraud.

The sharing of intelligence on known frauds and fraudsters is the basis of a common

defence. Fraudsters make multiple attacks across government departments and across the public and private sectors. The reciprocal sharing of intelligence needs to be at the heart of a common response. Insurance companies successfully worked together to establish the Insurance Fraud Bureau, which links up fraud intelligence to prevent fraudsters replicating their attacks across the insurance sector. Public sector organisations need to do likewise.

Combating fraud will be difficult without a clear understanding of the scale and type of the problem. The Taskforce is firmly of the view that departments need to measure fraud loss, and properly assess their fraud risk. All departments need to determine the extent of their fraud losses so that there is a pan-government understanding of the threat; departments then need to understand their fraud risk in the context of the overall public sector fraud threat to determine the appropriate response.

Prevention, not detection or punishment, is the most efficient way to reduce fraud loss and when vulnerabilities are detected they need to be designed out. Prevention requires embracing the power of data analytics and deploying them, especially to prevent fraud at the application stage for government grants, benefits and services. The HMRC pilot demonstrated that a fraud firewall can go hand in hand with better service delivery by replacing cumbersome manual checks with something fit for purpose in the digital age. It is crucial that the Government puts in place the right incentives to encourage counter-fraud investments so that the organisations tackling fraud reap the benefits. It is also vital that departments design out vulnerabilities from new systems and processes as part of the underlying focus on prevention.

To underpin a new approach to tackling fraud, there is a need to establish a zero tolerance culture across the public service, where every public servant recognises the threat from fraud and understands their role in tackling the threat. There is a need to put an end to the 'pay first, check later' culture and ensure that there is swift and sure justice for those who defraud the public sector. This will signify a step change in how seriously the Government is taking fraud.

Implementing a collaborative approach

Departments need to adopt a collaborative approach where good practice and intelligence are shared freely in order to combat fraud.

Departments such as HMRC and DWP have led the way, developing considerable expertise in preventing, detecting and investigating fraud – but this expertise needs to be shared more widely. The newly established CFC network needs to become the forum for sharing knowledge about fraud and fraudsters, and successful techniques used to prevent, detect and investigate fraud.

Local authorities also need to adopt a common approach to tackle the specific fraud threats they face collectively. Work is already under way to develop a local government strategy guided by a ten-point plan developed by the NFA for the Department for Communities and Local Government.

Proposals going forward

While progress is being made in each of these four areas, the Taskforce recommends that the Government continues to drive reforms that will deliver further savings. Based on the assessment by the Taskforce, the results of the pilots, and other activities undertaken under the Taskforce remit, there are a number of proposals we have already identified within the four priorities. The Taskforce will continue to explore other potential reforms in the coming months.

Priority 1: COLLABORATION

The cross-government and public/private sector sharing of fraud intelligence and alerts is needed to prevent related fraud attacks. To this end, we propose to:

- utilise the capability of the National Fraud Intelligence Bureau (NFIB) to network fraud data to provide every public sector organisation with the intelligence needed to maintain the integrity of their operations and defend themselves against common fraud threats;
- agree a roadmap for intelligence sharing between the NFIB, HMRC, DWP, and other departments and local authorities;
- organise the distribution of alerts concerning new fraud types which have impacted on one part of the public sector and threaten others;
- consider the development of a watch list of people who have committed insider-enabled fraud against the public sector;
- share information between procuring departments on companies which routinely

overcharge public sector organisations to ensure future invoices are rigorously checked;

- share information on compromised and false identities;
- identify problems with existing legal gateways and data sharing agreements, and address the data security implications of sharing data;
- ensure that every department:
 - puts in place solutions to prevent fraud during contract award
 - undertakes a recovery audit on its payment systems;
- look into how to consolidate and streamline the way grants are distributed with a view to making the application of fraud prevention measures more efficient and effective; and
- evaluate and deliver mechanisms for matching grant application data in order to spot duplicate applications and inconsistencies, such as 'Grantgov' in the USA.

Priority 2: ASSESSMENT OF RISK AND MEASUREMENT OF LOSSES

The assessment of risk, the measurement of losses and an understanding of the nature of fraud are the cornerstones of an effective strategy. We propose to:

- assess the fraud risks across benefits and revenues, treasury management, payroll, grants and procurement, making full use of the suite of HM Treasury guidance on 'Managing Risk of Financial Loss';

- recognise explicitly the risks posed by fraud in the work of Audit Committees and in Statements on Internal Control (Governance Statements from 2011–12);
- report on the full scale of detected and undetected losses through fraud in the Quarterly Data Summaries;
- adopt common and consistent estimates for spend metrics in business plans and Quarterly Data Summaries;
- arrange for an independent assessment of the accuracy of reported and estimated losses to provide confidence in the investment decisions subsequently taken to tackle fraud;
- understand how fraud is perpetrated, what creates fraud risk, and who conducts fraud and why; and distinguish fraud attacks by different types of perpetrator (e.g. opportunistic individuals versus organised criminals); and
- develop fraud mitigation plans for each department tailored to individual fraud risks.
- utilise ‘payment by results’ and industrialise solutions across the public sector;
- deploy the National Fraud Initiative more widely as a near real-time tool to enable data matching between departments, and between central and local government;
- establish a system of peer review that brings together a panel of experts from across relevant departments/agencies/private sector organisations to provide a robust and independent view of the fraud risk for current business, systems in development and proposals for new systems and processes;
- extend the process of peer review to the ERG Starting Gate, Gateway Review and work of the Major Projects Authority to provide explicit external oversight of the level of fraud and error risk at key points in each new major project and programme;
- develop the application of behavioural insights to combat public sector fraud;
- ensure that robust counter-fraud protocols are designed into the online delivery of public services;
- put in place the right incentives to encourage counter-fraud investment (where justified by a projected strong return on investment) and do away with perverse incentives that hinder organisations from making such investments; and
- ensure that those departments which make savings are able to re-invest the savings made in frontline services.

Priority 3: A FOCUS ON PREVENTION

Upfront prevention and detection of fraud through the development and deployment of real-time data analytics is needed, as well as the ability to design vulnerabilities out of systems. To achieve this, we propose to:

- replace the public sector ‘pay first, check later’ culture by a renewed emphasis on prevention through the greater deployment of data analytics and preventative checks against relevant data assets;

Priority 4: A ZERO TOLERANCE APPROACH

We need an all-pervasive culture of zero tolerance to fraud, led from the top. To this end, we propose to:

- deliver a cross-government programme to raise awareness of fraud;
- establish a repository of fraud-related information and supporting material;
- promote a single e-learning tool to provide consistent training and awareness of fraud;
- encourage all departments to utilise the Changing Organisational Cultures toolkit as a basis for wider behavioural change;
- establish an expert panel to support departments changing culture;
- grasp the opportunity of centralising HR to introduce counter-fraud requirements and staff incentives;
- require the development and delivery of job-specific fraud training modules, e.g. for procurement specialists;
- take the battle to change culture to the public in order to change the perception that fraud against the Government is acceptable;
- signal a step change in how seriously the Government is now taking fraud against the public sector by taking swift and effective enforcement action against fraudsters; and
- take disruption activity in order to stem continuing losses and make greater use of early restraint of assets and civil litigation.

Next steps for the Taskforce

The next steps for the Taskforce are to give further consideration to the specific actions that will best deliver against the four priorities. This will require further options analysis and the development of final recommendations, and an implementation plan within six months, as well as cross-government collaboration and energy to drive delivery. The Taskforce will also look to extend the lessons learned in central government to local government.

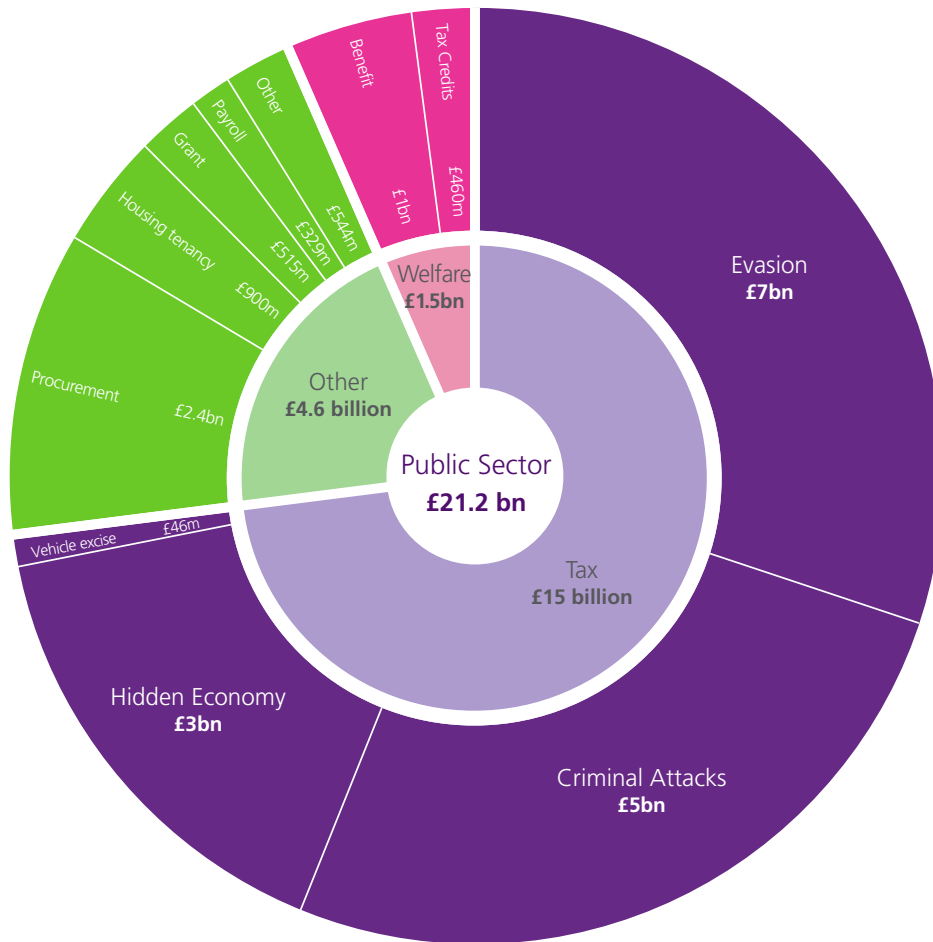
The Taskforce will now also turn its attention to how further savings can be made by taking a cross-government approach to reducing error and debt by, among our other priorities, applying a preventative approach, using data analytics and seeking opportunities for the sharing of best practice.

Annex 1

NFA Annual Fraud Indicator 2011 Public Sector Fraud



National Fraud Authority



Area	Total fraud loss	Fraud type	Fraud loss
Tax	£15 billion	Tax fraud	£15 billion
		Vehicle excise fraud	£46 million
Central government	£2.6 billion	Procurement fraud	£1.5 billion
		Grant fraud	£472 million
		Television licence fee evasion	£196 million
		Payroll and recruitment fraud	£177 million
		NHS patient charges fraud	£165 million
		Student finance fraud	£31 million
		Pension fraud	£7 million
		National Savings and Investments fraud	£0.39 million
		Local government	£2.1 billion
Procurement fraud	£855 million		
Payroll and recruitment fraud	£152 million		
Council tax fraud	£90 million		
Blue Badge Scheme abuse	£46 million		
Grant fraud	£43 million		
Benefits and tax credits	£1.5 billion	Pension fraud	£8 million
		Benefits fraud	£1 billion
		Tax credits fraud	£460 million

Annex 2

Summary of pilots

Pilot	Lead	Description	Outcome(s)	Way forward
Fraud and Error Assessment System Tool	HMRC	Together with an IT supplier, HMRC has piloted an innovative screening technique for tax credit applications and renewals to prevent losses to fraud and error. The technique analyses the information provided on the application form and profiles the application for its likelihood of being fraudulent.	HMRC invested £1m from contract renegotiations with the IT supplier and this yielded £10.63m in savings. The technique has been able to identify high-risk applicants and prevent payments being made to these, while fast tracking payments to low risk applicants.	The pilot has highlighted the potential for data analytics to prevent fraud , while improving the efficiency of processing tax credit applications and renewals. HMRC plans to roll the tool out more widely.
Undisclosed partners	HMRC/ DWP	HMRC and DWP commissioned credit reference agencies (CRAs) and data matching companies to verify the circumstances of 20,000 benefit and tax credit claimants each, and identify people falsely claiming to be living alone.	<p>For HMRC, CRAs identified 2,000 high-risk cases which were matched against internal HMRC data. 750 letters were issued to high-risk claimants and, from this, more than 300 claims were stopped or amended. This amounted to a gross saving of £1.5m with an expectation to save up to £10m once remaining cases are followed up.</p> <p>For DWP, two CRAs identified between 689 and 2,598 Income Support and Jobseeker's Allowance claimants as high risk. DWP matched this against internal data and expects to save £0.5m through stopping or amending relevant benefit claims.</p>	<p>Through a single contract, HMRC and DWP will industrialise the use of these checks across their data. In doing so, HMRC estimates it will save in the region of £700m over the next two years. DWP estimates it will save £490m over the next four years.</p> <p>The pilot has demonstrated the power of data analytics and data matching to prevent fraud.</p>

Pilot	Lead	Description	Outcome(s)	Way forward
'Nudge' behaviour	HMRC	Together with the Behavioural Insights Team in the Cabinet Office, HMRC used 'nudge' principles to influence people who were late paying tax last year. The aim was to stimulate a shift to paying the correct amount on time, or submitting returns on time. SMS messages were sent to around 31,500 people who were late paying tax of more than £1,000 in 2009/10 or who sent in their returns late.	The exercise prompted a 5% improvement in behaviour, covering an increase in tax yield as well as reductions in debt management and related costs. Currently, around 1 million people are late paying their tax each year. HMRC estimates that a 5% improvement would lead to £125m reaching public coffers earlier, with HMRC having to deal with 50,000 fewer debts.	The pilot has shown that behavioural techniques can have a positive impact on preventing fraud, error and debt . HMRC plans to use SMS campaigns more widely across different parts of the business. The Behavioural Insights Team will be undertaking further pilots in 2011 to test the impact of these techniques in other areas of fraud and error.
Cross-government fraud alerts system	NFA/DH	The pilot delivered a proof of concept for a system of fraud alerts to Government Counter Fraud Champions (CFCs). A single case of fraud against a departmental payment system was used as a test case. Details of the case were matched with data in the National Fraud Intelligence Bureau and an alert was issued to CFCs.	The pilot indicated that many government departments were aware of the fraud and had taken steps to tighten controls and prevent falling victim to the fraud. Good practice fraud prevention measures were identified in departments, but this had not necessarily been shared more widely.	The alerts system will be tested further and rolled out fully. CFCs have nominated Alert System Coordinators to handle and respond to future alerts. The pilot has highlighted the importance of sharing intelligence and data in order to protect from attack .
Procurement fraud, error and debt	DfT	DfT commissioned an analytics company to undertake a 'spend and recovery audit' on their group procure-to-pay systems. The aim was to identify overpayments to suppliers over the previous financial year. A similar exercise undertaken by the Home Office identified £4m in overpayments, with the supplier recovering overpayments on a payment by results basis.	Almost £0.5m in overpayments has been identified for recovery. This relates to payments made in the previous financial year by DfT, the Driving Standards Agency and DVLA. It is estimated that up to £8m could be identified for recovery once analysis is undertaken across the entire DfT family payment systems over a six-year period.	The pilot has presented a strong case for all government departments and public bodies to undertake a spend and recovery audit, particularly where this is offered on a 'payment by results' basis. It shows that using data analytics to detect fraud or error can be undertaken with little risk but maximum benefit. The Cabinet Office will take this forward as part of its recommendations to tackle procurement fraud in the public sector.

Pilot	Lead	Description	Outcome(s)	Way forward
Insider-enabled fraud	UKBA	The exercise focused on the UK Border Agency's (UKBA's) use of a data analytics package which detects links between UKBA staff and their involvement in breaches of immigration controls. The aim was to draw parallels between this work and the potential to identify corrupt staff involved in committing fraud.	The package has detected three cases of serious criminality and provided strong evidence for 70 internal investigations of UKBA staff. Two closed cases were reopened as a result of new evidence generated by the analysis.	The pilot has demonstrated a need for public bodies to protect themselves from attack by those working inside their organisation. The Taskforce will explore areas where these tools can be used more widely, alongside taking forward recommendations by the National Fraud Authority to tackle insider-enabled fraud in the public sector.
Grant fraud	Big Lottery Fund	The Big Lottery Fund matched 10,000 successful and rejected grant applications with the National Fraud Intelligence Bureau database. The aim was to detect links between grant applications and criminal activity, including organised crime.	Work is still continuing to assess the threat to lottery funding. 692 applications were highlighted as having links to data held in the National Fraud Intelligence Bureau. These are being analysed further.	The pilot has demonstrated that multiple applications are a threat in the grant awarding process which could be exploited by organised crime. The Taskforce will be taking this forward in line with the National Fraud Authority's recommendations to tackle grant fraud in the public sector.
Hotlines	HMRC	HMRC commissioned a data analytics company to undertake a text mining exercise on referrals to the Tax Evasion Hotline. Text mining analyses unstructured data and identifies hidden information which can generate better intelligence.	The exercise has improved the quality of data extracted from referrals to the hotline, which has generated greater actionable intelligence on which HMRC can improve seizures and increase tax yield.	The pilot has demonstrated the breadth of capability data analytics can provide to improve prevention and detection of fraud . HMRC plans to invest in text mining technology across other databases where unstructured data is held.