

**Safeguarding
social security:
GETTING THE
INFORMATION
WE NEED**



- Safeguarding social security:
**GETTING THE INFORMATION
WE NEED**





Foreword	v
Chapter One: What is the problem?	1
Chapter Two: Using information to stop the fraud	7
Chapter Three: The information we need	9
Chapter Four: Safeguards	17
Chapter Five: Costs and impact on business	21
Chapter Six: The consultation process	25



We spend over £100 billion each year on the social security system. This money pays for pensions, help for people with an illness or disability, help for families and help for those who are out of work. It is a huge amount and is entirely funded by the people of this country.

We want to make sure that the right benefits go to the right people. We must also secure the system from the dishonest, weeding out fraud and error to prevent crime and make money lost through fraud available to help those who need it.

To provide a better service, we are moving more staff to the front line to help people get the benefit they are entitled to as well as making sure we pay the right amount to the right people. We are posting an additional 3,000 staff into local offices to deal directly with our customers as part of our restructuring so that we focus specifically on the needs of different client groups – people of working age, pensioners, and families with children.

To combat fraud and error, we are continuing to introduce tighter checks on claims to ensure that they are correct as well as working closely with other departments such as the Inland Revenue to ensure that fraudsters are caught and punished. Our strategy, launched in March 1999, involves better measurement, improved incentives, smarter security and commitment across the Department of Social Security. This is being achieved by a sustained effort across three fronts:

- **getting it right** – benefit payments should be correct from day one;
- **keeping it right** – ensuring payments are adjusted as circumstances change; and
- **putting it right** – detecting when payments go wrong and taking prompt action to correct them with appropriate penalties to prevent a recurrence.

To make sure our strategy works we are monitoring progress, evaluating the strength of our defences and adjusting them in the light of experience.

The Government has made it clear that it intends to take further powers to deal with fraud. For example, it will legislate to stop people receiving benefit when they have been convicted of two benefit offences.

This document is published in advance of new legislation. It focuses only on the information needed to help stop fraud.

Last autumn, the Chancellor of the Exchequer asked Lord Grabiner QC to conduct an investigation into the hidden economy and to produce a report. The report, entitled *The Informal Economy*, was published in March 2000. Lord Grabiner made a series of recommendations to combat tax and benefit fraud covering incentives to join the legitimate economy, prevention, detection, punishment, and publicity. The Government is committed to implementing his recommendations.

In his Summary of Recommendations, Lord Grabiner says “the Government should consider ways to use information from private sector sources as a cross-check on the details people provide to Departments (such as where they live and whether they have a bank account)”. In the chapter on ‘Detection: Intelligence Gathering’, he says “I recommend that the Government should examine how it can make use of information from private sector sources and put in place a Code of Practice and, if necessary, legislation”.

This document seeks your views on the sorts of new information that we should be able to obtain in order to prevent, detect and punish social security fraudsters. It describes the sorts of information we might wish to obtain, the organisations from which we might obtain it, and what we could do with that information. It explains the safeguards that we could put in place to ensure that people’s right to privacy was protected and to ensure that we fully complied with the Human Rights Act and Data Protection Act to which we are fully committed. It explains how we could seek to minimise the impact of obtaining information on businesses. On all this, it seeks your views. We very much hope that you will take the time to respond. Responses should be made by 21 October 2000 to the address given in Chapter Six.

Department of Social Security



The starting point

- 1.1 Social security fraud and error is estimated to cost the country between £2 billion and £4 billion a year. How has this happened? The system had the following principal flaws:
 - the amount of benefit fraud that we **detected** was our only measure of success. There was no incentive to **prevent** fraud from entering the system in the first place;
 - there was no measurement of fraud to understand the scale of the problem until 1995, which meant that there was no overall strategy for safeguarding the system;
 - inadequate investment in information technology (IT) meant that we couldn't draw together all the information that we held on a person's claims, to guard against fraud and to avoid error; and
 - there was a culture throughout the organisation that too often regarded security as a bolt on extra rather than an integral part of the everyday running of the social security system.

Steps already taken

- 1.2 We set out our strategy in *A new contract for welfare: SAFEGUARDING SOCIAL SECURITY* (Cm 4276, March 1999). For the first time, we have set out a plan to secure the system from the first claim to the final payment.
- 1.3 We have set a target for reducing the amount of fraud and error, rather than for merely detecting fraud that has already happened. We have already undertaken to cut the rate of fraud and error in Income Support (IS) and Jobseeker's Allowance (JSA) by 30 per cent by March 2007, with at least 10 per cent reduction by March 2002. We are now raising our targets with a view to reducing losses from fraud and error in IS and JSA by 25 per cent by March 2004 and by 50 per cent by March 2006.
- 1.4 Putting the system right and correcting its flaws will take time, but we are already seeing results:
 - tighter checks at the gateway to IS have halved the number of claims paid without enough supporting evidence, and will save over £1 billion during the course of this Parliament;
 - we have given computer terminals to almost all local authorities so that they can use electronic data from the Benefits Agency. This will save some £24 million each year;

- the cross-checking of Department of Social Security (DSS), local authority and other government records has already saved over £150 million. We will soon start cross-checking benefit and tax records to flush out benefit cheats in the construction industry;
- in 1999/2000, we prosecuted or sanctioned over 20,000 people, compared to just over 14,000 in 1998/99;
- we have given an extra £100 million to local authorities to help them make tougher identity checks on people claiming Housing Benefit (HB), before any payment is made;
- we have made arrangements with the Royal Mail to stop HB fraudsters redirecting their mail from false addresses; and
- for the first time, we have launched a hard-hitting television campaign, to get the public onside in the fight against fraud.

1.5 We have more initiatives in place that will bear fruit next year. These include:

- specialist identity checks nationally when people apply for social security – especially where they do not have National Insurance numbers. These have been successfully tested in South London where they have resulted in over 200 arrests; and
- stronger powers for our investigators to inspect employers' records to check on people who are working whilst claiming to be unemployed.

1.6 Other things that we are doing include:

- introducing tougher punishments, including withdrawing benefit from persistent offenders (**two strikes and you're out**);
- moving 3,000 staff from the centre to the front line;
- investing in new IT systems to make better use of information and to make the system more secure;
- paying benefits directly into bank accounts, so that by 2005 almost all benefits will be paid in this way. Not only will this cut fraud and losses involving order books and Girocheques, but each payment will cost around 1p, rather than 79p as at present; and
- setting up a National Intelligence Unit to produce a better targeted approach to finding the fraudsters.

The scale of the problem remaining

1.7 Much has been done to make the system more secure. But more remains to be done if we are to drive fraud out of the system. The rest of this chapter sets out the size of the problem in the three most vulnerable benefits: IS, JSA and HB where we lose almost £2.2 billion a year to fraud and error.

- 1.8 We begin with the main ways in which people may steal IS or JSA.

Undeclared earnings

- 1.9 The means-tested benefits are mainly aimed at those without work or those doing small amounts of part-time work. If someone works for 16 hours a week or more, they will no longer be entitled to either IS or JSA. The customer must also tell us about the earnings of a spouse or partner for whom they are claiming. If someone works for fewer than 16 hours a week and earns more than £5 a week (in some cases £15 a week) they must inform us, as this may affect the benefit that we pay them. The last Budget contained proposals to enable many of those claiming benefit and working to retain more of their earnings. From next April, the long-term unemployed, lone parents, people with a long-term illness or disability, carers and pensioners will be able to retain £20 of their weekly earnings.
- 1.10 Customers may therefore commit fraud by deliberately not telling us about the work that they do, or not telling us about all or part of the wages that they receive. For example, they may work cash-in-hand for an employer and deliberately not tell us about it.
- 1.11 This type of fraud may contribute to the hidden economy as it often involves collusive employers who knowingly employ people who are in receipt of benefits.

We estimate that this type of fraud costs £344 million each year

Undeclared income

- 1.12 In a similar way to earnings, we need to know about the amount of other income received by a customer or their dependants. With a few exceptions, any income from benefits, pensions or other sources is taken into account when we assess entitlement to benefit. Customers are obliged to inform us of any income that they receive when they claim or during the course of their claim.
- 1.13 For example, a customer may receive an income from an investment and not tell us.

We estimate that this type of fraud costs £36 million each year

Undeclared capital

- 1.14 The means-tested benefits are also intended to help people without significant amounts of savings or capital. By capital, we mean assets or property owned by the customer or their dependants. It does not include the customer's home. Currently, customers are allowed to have £3,000 in capital and savings before their benefit is affected.

- 1.15 Customers are obliged to inform us of any capital available to them. People who deliberately do not do so are committing fraud. For example, they do not tell us that they have a savings account with a bank or building society.

We estimate that this type of fraud costs £34 million each year

Family circumstances

- 1.16 When someone makes a claim for a means-tested benefit, we need to know about his or her family circumstances. This means, for example, that if someone is married, or living with someone as if they were married, we need to know so that we can assess their claim as a couple. This is regardless of whether they wish to claim for their partner or not. We need to do this because it would be unfair to pay a means-tested benefit to someone who may not work themselves but lives with someone who does. Any income or savings that one has must be treated as available to the other.
- 1.17 Fraud occurs when a customer deliberately tells us that they are single when they are not, and, more importantly, fails to declare the income or resources of their partner. We also need to know if the household includes a non-dependant. This might affect the amount of benefit paid if, for example, the claim includes a mortgage.
- 1.18 A common type of fraud is one where a person claims to have been left by their partner when in fact they are still living with them.

We estimate that this type of fraud costs over £200 million each year

Housing Benefit fraud

- 1.19 HB is calculated in a similar way to IS and JSA and is intended to help meet the accommodation costs of people on low incomes who rent their homes from a landlord. Many of the types of fraud committed on IS and JSA apply equally to HB while others, such as falsifying the amount of rent payable, are specific to HB.
- 1.20 Many local authorities make payment of HB directly to landlords. This means that the customer does not have to worry about making payment to the landlord himself. However, fraud may occur when the landlord fails to inform the local authority when the tenant moves out, or claims benefit for tenants who have never lived in their property. We give more information about this type of fraud in the next section, 'Residency fraud'.

We estimate that fraud in Housing Benefit costs £600 million each year

Residency fraud

- 1.21 This type of fraud may be committed by either a landlord or by the benefit claimant. It involves the claimant giving a false address or failing to declare that he or she has left an address. Either way, a false address suggests that a fraud has been committed. It is a 'cross-cutting' fraud in that it may involve any or all of the types of fraud previously mentioned. This type of fraud is not measured separately for this reason.

Identity fraud

- 1.22 Any benefit claim made using false identity is fraudulent. A claimant may adopt a completely false identity and, as a result, receive benefit to which they are not entitled. There are cases of multiple identity fraud in which a claimant has simultaneously adopted several identities. This type of fraud, like residency, is 'cross-cutting' in that it covers various other types of fraud. For this reason, it is not measured separately.

■ Example:

An organised gang adopted the identities of 171 people from the Irish Republic and used them to make a string of false claims in the UK. Members of the public brought this fraud to the attention of DSS investigators. The real owners of these identities were not implicated and, in fact, had no idea that their identities had been used in this way. The gang was investigated and prosecuted, with the ringleaders receiving prison sentences of between three and four-and-a-half years. The final overpayment was in excess of £2 million. **If the DSS had data sharing arrangements in place with the Irish social security authorities, this fraud could have been prevented.**

Using information to beat fraud

- 1.23 Too much money is lost to fraud and error. Most fraud occurs through people hiding information from us. The next chapter describes the action we are already taking to share information with other government departments to chase the fraudster.



Sources of information

- 2.1 Fraud is committed by people telling lies or concealing the facts. Cross-checking what claimants tell us against independent sources of information is crucial to catching out the fraudster.
- 2.2 The government already collects a substantial amount of information and cross-checking that information is extremely valuable in combating fraud. This chapter explains the sorts of cross-checking of information that we are already doing.

Checking information with other departments

- 2.3 The Department of Social Security (DSS) has already begun to share information with other government departments and local authorities to combat fraud and error. This is done on individual claims and by routinely checking certain records held by, for example, the Inland Revenue.

Checking individual claims

- 2.4 To enable individual claims to be checked we have installed computer terminals in 388 local authorities to provide Housing Benefit (HB) staff with access to DSS benefit systems. These will help prevent fraud and overpayments of HB and Council Tax Benefit (CTB).
- 2.5 The Personal Details Computer System (PDCS) and Customer Payment Computer System (CPCS) have both been operating since July 1997. When fully operational in 2001, the PDCS will provide a single source of claimants' personal details across all benefits, whilst the CPCS will provide a single up-to-date source of payment details across all benefits. These systems will cut fraud by revealing inconsistencies and helping to prevent the use of false identities.

Data matching our information

- 2.6 We are making use of modern computer capabilities to compare different sets of our own records, as well as to compare our own records with those of the Inland Revenue. HB records held by local authorities are also being compared with other relevant records. The purpose of these exercises (which we refer to as **data matching exercises**) is to identify inconsistencies between different sets of records that might indicate fraud and error. For example, if a person is claiming benefit on the basis that they are not in work then the Inland Revenue should not be receiving tax and National Insurance (NI) payments in respect of them. If a data match found that the Inland Revenue were receiving such payments in respect of such a claimant this would indicate fraud.

- 2.7 During 1998/99, we compared data held by DSS and by local authorities. 189,000 inconsistencies in the data were identified and referred for further investigation by either Benefits Agency or local authority staff. These led to over £149.5 million of benefit savings for the year.
- 2.8 Since the passing of the Social Security Administration (Fraud) Act 1997 we also have access to the Royal Mail database giving information about redirection of mail. This has enabled us to prevent claimants from using this facility to submit benefit claims from false addresses. This was made available to all local authorities from 1 February 1999 and so far over 270 authorities have signed up.

The need to do more

- 2.9 The problem with government information is that someone who lies to one government department may well lie to another to maintain a consistent story. A person may lie, for example, about his or her earnings both to claim benefit and to avoid paying tax. Similarly, an employer may say that he or she does not employ a person both to help that person claim benefit whilst working and to avoid paying NI in respect of him or her. Consequently, cross-checking our information with, for example, that held by the Inland Revenue does not always detect fraud. That is why we need to look wider to get information to help us beat the fraudster.



- 3.1 Whenever we process a claim for benefit, we have to strike a balance between the need to provide a fair and efficient service to customers and a need to guard against fraud. We want to provide a social security system that focuses upon people's needs and responds rapidly to them. However, that system also needs to include sufficient checks to ensure that claims are correct, and such checks can slow the system down. It is, therefore, important that when we have doubts about a person's claim we are able to resolve these as quickly as possible. If we can, we always try to resolve our questions with the claimant without involving a third party. However, there are times when obtaining information from someone other than the claimant is necessary when people refuse to co-operate or to tell the truth.
- 3.2 Fraud occurs because people lie about their circumstances, or deliberately fail to tell us about a relevant change. If we had more information about people's circumstances, we could more effectively safeguard the benefit system from fraud. We know that there are other sources of information which we do not yet have access to, but which might help us to combat fraud.

■ Example:

H was a self-employed block paver. The Benefit Fraud Investigation Service received an anonymous allegation that he was working and claiming benefit. Observations were conducted and evidence collected about his crime. As a result, his benefit was taken away. He was invited to attend an interview at the local benefit office. During the interview he admitted that he had had 12 jobs during the period he had received benefit.

At the interview H was asked to give his consent to obtain details of his bank accounts. It was only when the information from the bank accounts was examined that the full extent of the fraud became known. As a result, an overpayment of over £17,000 was identified. H was charged with five counts under the Theft Act 1968. He was sentenced at the Crown Court in January this year to 6 months' imprisonment.

- 3.3 It is, therefore, necessary for us to obtain information from sources outside government.

- 3.4 Although we can ask customers for permission to approach companies in the private sector that hold information about them, they can decline should they wish and a fraudster would do so in many instances. In the example cited above, had H declined, we would have stopped paying his benefit but we would have been unable to establish the full extent of the money already stolen. Had we had legislative powers to require a bank to give details of customer accounts, this fraud might have been discovered at an earlier stage. We would also not have had to risk the claimant's declining to give consent.
- 3.5 Information is available from a range of sources outside government. Examples are:
- a person's income and capital – for example, earnings, savings and income from insurance policies;
 - a person's identity;
 - where people live; and
 - whether a person lives alone.
- 3.6 Fraudsters will lie about all these things. It is, therefore, extremely important that we are able to cross-check our information with the people who hold the information we need, when we suspect that fraud is taking place. However, as explained below in paragraphs 3.10 to 3.15 we propose to seek such information only where there are grounds for suspecting that an individual claiming benefit is lying to us. We do not propose to ask for sensitive information where we have no suspicions of fraud.
- 3.7 Paragraphs 3.18 to 3.20 invite views on whether we should be able to obtain less sensitive information, such as the absence of electricity or water consumption at addresses to which we are sending benefit payments, in cases where there were no suspicions of benefit fraud.
- 3.8 Paragraphs 3.21 to 3.23 ask for views on whether we should be able to exchange information with insurance companies where we are both making payment for the same contingency, for example unemployment, and there are proper safeguards in place to prevent the misuse of any information exchanged.

The information we need

- 3.9 We need information at three key points in the life of a claim. These are highlighted in our fraud strategy *A new contract for welfare: SAFEGUARDING SOCIAL SECURITY* (Cm 4276, March 1999) and are:
- ensuring that claims are correct from the outset – **getting it right**;
 - regularly reviewing claims to ensure that they remain correct – **keeping it right**;
- and

- detecting and investigating fraud and error where they slip through our prevention network – **putting it right**.

Getting it right

- 3.10 The following are examples of how we could use additional information to ensure that claims were correct from the outset.

Example One: A person claims benefit on the basis that he has recently been made redundant and has no savings to live on. Although he worked for a large company known to pay salaries into bank accounts, he claims he no longer has a bank account. The benefits officer is suspicious that the claimant may still have an account which contains savings. The benefits officer contacts the bank and asks whether the claimant still has an account.

Example Two: A person claims for a large family from an address in a street that is known to consist of small flats only. The benefits officer suspects that the claimant may not be resident at that address. At the moment, we would need to conduct an investigation and send somebody round to the flat. He might try to fool us by saying that the flat was a mess because he had only just moved in and that his family were out. We would then have to conduct long-term surveillance, which would affect his neighbours. We would not have to do this, however, if we were able to check with the water supplier and confirm that the flat was not connected – a good sign he didn't live there.

Keeping it right

- 3.11 Although we are determined to ensure that claims are correct at the outset, we know that fraud and error does creep in. Seven out of every ten claims that are found to be incorrect were correct when they were first made. This makes it clear that regular reviews of claims are essential to prevent fraud and error. The following are examples of how private sector information might be used to help us ensure that our benefit claims remain correct.

Example Three: Cases are selected for spot checks on the basis of an analysis of the risks that they could be fraudulent. At the moment, the claimant would be either visited or interviewed. Details of bank or National Savings accounts could be requested. If we were able to contact the bank, we could verify the claim with greater efficiency, or prove it to be fraudulent.

Example Four: A claimant has declared that he is receiving income from an insurance company or pension provider. It is known that this is increased annually, and that this claimant has failed to inform us of changes in the past. At the moment, the only way we could find out about the annual increase would be to contact the claimant. If we were able to go directly to the provider, we could be certain that we had the correct information to assess how much benefit to pay.

Putting it right

- 3.12 No matter how careful we are about checking claims, the determined fraudster will always try to target the benefit system. We therefore need to strengthen our means of detecting fraudulent cases that have evaded our vigilance. The following are examples of how we might use information from the private sector to detect fraud which has already occurred.

Example Five: A fraud section has recently prosecuted a number of people claiming benefit whilst working in a self-employed capacity. A fraud investigator receives further allegations that claimants are working and searches the local papers for adverts for any services where the person is likely to be self-employed, for example a window cleaner. There are such adverts, but they quote only a telephone number – they show no business address. At the moment, there would be no way to further this type of investigation. If we were able to check with the telephone company to see to whom the advertised telephone numbers belonged, we could then check the names and addresses provided against benefit records to see whether any of them were claiming benefits.

Example Six: A person claims for a second time that their weekly Girocheque has been lost or stolen. On the previous occasion, having replaced the Giro immediately to prevent hardship, we subsequently established that they had cashed it and received the money. At the moment, we would interview the claimant, but if they did not admit to having cashed the second Giro, we would have to replace it again. If we were able to check with the local cheque cashing shop before replacing the Giro, we might be able to tell whether it had been cashed there and whether the person cashing the Giro was the claimant.

Example Seven: A fraud section receives information that a student at a local college is claiming benefit. A number of similar cases had been recently prosecuted. At the moment, we could ask the college for confirmation that this individual was currently studying with them, but it wouldn't be obliged to tell us. If fraud investigators were able to obtain records directly from UCAS, the Student Loans Company, or colleges and universities, they could match the details against departmental records.

Potential sources of information

- 3.13 The organisations that we think will have the information we need will include major financial institutions, utilities, colleges and universities. We do not propose to seek information from small businesses.
- 3.14 If we were to take powers to obtain this information from these organisations, we would be doing so because we needed the information to prevent and detect fraud. By refusing, they would (even unwittingly) be helping dishonest and unscrupulous criminals. For this reason, we think that any legislation we might take to obtain information from the private sector should enable us to insist that they provide the information.
- 3.15 **We would welcome views on whether we should require information from business in individual cases where we had suspicion that benefit was being stolen.**

Local authorities

- 3.16 Local authorities pay Housing Benefit (HB) and Council Tax Benefit (CTB) in a similar way to which we pay Income Support (IS) and JSA. Fraud is as much a problem for them as it is for us, and is also paid for by the taxpayer. If they are to be effective in the fight against HB fraud, they will need similar powers to those described above. We would extend provisions to share information to investigators working for local authorities.
- 3.17 **We would welcome views on whether we should extend such powers to local authority fraud investigators.**

Other circumstances in which information may be required

- 3.18 The Government is proposing further steps to check the validity of claims. The examples cited so far cover situations where suspicion has focused on an individual. However, there may be circumstances where further, more general, information may help the fight against fraud. Safeguards are essential as is discussed in Chapter Four.
- 3.19 We believe that there are types of information which are not sensitive for the majority of people but which could tell us whether people might have lied about their circumstances. Examples might be information about which addresses were not currently consuming electricity or water. If we compared this information against our records of addresses to which benefit payments were being sent, any matches would raise suspicions that the claimants concerned were not living at the addresses that they had given us. This is potentially a very valuable source of information to cut the level of non-residency fraud described in paragraph 1.21. And for those addresses where no benefit was in payment, the only information we would have was that electricity or water was not being consumed there – hardly a sensitive matter.

- 3.20 **We would welcome views as to whether there was a case for extending our proposals concerning *specific* information requirements where we had suspicions of fraud to cover similar types of *general* information the possession of which would not be an unwarranted intrusion into the private lives of the majority of people.**
- 3.21 Another potential source of information would be details of people claiming similar benefits from the insurance sector as are available from the social security system. An insurance company, for example, may be paying unemployment insurance to someone who is claiming Jobseeker's Allowance (JSA). There is nothing wrong with this, provided the claimant has told us about the insurance payments. However, there are two types of fraud which may occur. Firstly, we may not have been told about the insurance payments. Secondly, the insurance company may not have been told if their customer had returned to work, although we may know that the person concerned had stopped registering with us as unemployed.
- 3.22 There may be a case for mutual exchange of information between us and insurance companies to prevent these kinds of fraud. This would certainly be so if there was strong support for the Government's helping to prevent insurance companies being defrauded. We know that this will be a sensitive subject which requires strong safeguards to protect the rights of the citizen. We would ensure that any legislation was compatible with the Data Protection Act. We would also have to be satisfied that any information we gave was kept securely, and that the recipient could justify its use. In other words, the scale of the information required must be justified by the scale of the problem.
- 3.23 **We would welcome views on whether we should be able to exchange information with the insurance sector in the narrowly circumscribed circumstances described above, that is where we are both making payment for the same contingency and there is both sufficient justification for the exchange and adequate safeguards to prevent misuse of the information exchanged.**

Information from other countries

- 3.24 Means-tested benefits should not be paid to people who are receiving similar benefits from another country. They are also not available to people who are working in another country. In some cases, benefits should not be paid to people living in another country, although there are exceptions to this, including contributory benefits like Retirement Pension. Other countries have similar rules.
- 3.25 For these reasons, we would like to be able to provide information to other countries about people claiming benefit here, and to obtain information from other countries about people living, working and claiming benefit there. In some circumstances we can already do this, under European law and under social security agreements that the UK has with some other countries. But this is not

enough to let us exchange all the information we need to prevent fraud. The fraud cited in Chapter One, where an organised gang used identities from the Irish Republic to claim in the UK, could have been prevented had there been a regular exchange of information between the two Governments.

- 3.26 Clearly, we would expect any other countries with which we exchanged information to have the same regard for human rights and data protection as we have in this country. There would be no question of exchanging information with countries that we thought might misuse information about UK citizens in any way.
- 3.27 Any understanding that we entered into with overseas social security administrations would restrict the additional information we exchanged, over and above that already permitted by European law or existing agreements, to the minimum level necessary to prevent fraud. We would ask for more details about a claim from an overseas administration if we had a strong suspicion that a fraud had occurred.
- 3.28 **We would welcome views on whether we should be able to exchange benefit information with other countries subject to the safeguards described above.**

Information gathering powers in other government departments

- 3.29 There are already precedents for what we are proposing. Within the UK, other government departments have a range of powers to obtain information from the private sector.
- 3.30 The Home Office took powers in the Immigration and Asylum Bill 1999 to require information on passenger manifests from travel companies on request. The Home Office has not begun to collect this information yet but intends to in the near future. Financial institutions are also required under the Criminal Justice Act 1988 to report suspicious transactions which could be related to the proceeds of serious crimes, such as money laundering or drug trafficking, to the National Criminal Intelligence Service.
- 3.31 To check tax returns, the Inland Revenue and Customs & Excise have powers to obtain information direct from businesses responsible for paying taxes or duties. Customs & Excise also have powers under the VAT Act 1994, the Finance Act 1994 and the Customs & Excise Management Act 1979 to require any person in possession of documents that belong to another business to provide them to Customs & Excise. Both departments also have powers, in cases of serious fraud, to get warrants to search premises and to seize information from innocent third parties such as banks, lawyers and accountants. The current Finance Bill contains provision to enable the Inland Revenue, where serious tax fraud is suspected, to seek an order from a circuit judge for the production of original documents from third parties needed as evidence.

- 3.32 The Inland Revenue also has powers, which do not need prior judicial approval to require some institutions to provide regular reports of certain financial transactions. It can require information on specific schemes that it polices, such as ISAs and information on interest paid on savings, and it can also obtain information from the private and public sector, under the Taxes Management Act 1970, to check compliance with the tax rules. Under these powers it can require reports:
- of money held on behalf of the owner, for example reports of information held by auctioneers or letting agents;
 - of commissions or payments for services, for example payments to actors or window cleaners;
 - of all property sales;
 - from tenants and managing agents about the letting of properties;
 - giving details of grants or subsidies paid out of public funds;
 - from stockbrokers on share issues and transactions; and
 - from auctioneers about transactions.
- 3.33 Auditing bodies, such as the Audit Commission and the Accounts Commission, also have powers to obtain information from third parties in the operation of their audit functions, including the audit of an organisation's ability to address fraud.

Safeguards

- 3.34 We are concerned to ensure that there are adequate safeguards in place to ensure that these powers are not misused:
- we will introduce a Code of Practice to guide staff in applying these powers;
 - staff will be subject to strict rules and penalties over whom they share information with;
 - information will be shared only by officers authorised to do so; and
 - senior managers will conduct regular checks to ensure that the Code of Practice is being followed.
- 3.35 Safeguards are considered in greater detail in the next chapter.



Human Rights

- 4.1 The Human Rights Act comes fully into force from October 2000. It incorporates rights and freedoms from the European Convention on Human Rights into UK law. The Human Rights Act makes it unlawful for a public authority to act incompatibly with the Convention rights, unless an Act of Parliament left no choice. A case can be brought in a UK court or tribunal against a public authority if it acts incompatibly. Under the Human Rights Act, all legislation must be interpreted and given effect as far as possible compatibly with Convention rights.
- 4.2 Article 8 of the European Convention on Human Rights is particularly relevant.

■ Article 8 of the European Convention on Human Rights

Everyone has the right to respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

- 4.3 This right can be limited when it is necessary to achieve an important objective such as the prevention of crime or is in the interests of the economic well being of the country. However, any interference with it must be in accordance with the law, and proportionate to the intended goal. We will ensure that our approach is consistent with these requirements.

Data protection

- 4.4 We also recognise that we have obligations under law about what information is obtained, how this is processed, how securely it is held, how long it is retained and the circumstances in which information might be disclosed to third parties. In all of these respects, the public has a right to expect that we provide the safeguards they are entitled to under human rights and data protection law.

Additional safeguards

- 4.5 We have published a Code of Practice which governs the DSS's data matching activities. This is available on our website at <http://www.dss.gov.uk>. This explains in detail the legal basis that we have for obtaining information and the safeguards that are provided by our procedures for handling this information:
- when asking an information owner for data, we will identify the items which we would like to match against our records, and provide the reasons for asking for that data. The DSS and the information provider will formally agree the data that we will take;
 - we would ask only for information that the law allows us to have. We will select only information that allows us to detect fraud or error;
 - we will agree with information providers in what form and how often the information is given to us, and how we dispose of data when it is no longer required for data matching purposes;
 - the data specification agreed by the DSS and the information provider ensures that we receive only the data which is required;
 - when we receive the data, we will check to ensure that it conforms to the specification and is of a sufficient quality to prevent unnecessary mismatches. If it does not conform to the specification, we will decide with the information provider how the relevant data can be supplied. As far as possible, we will take only data which is accurate and up to date; and
 - normally, we will keep the data for no more than nine months. In most cases, the data will be discarded before then, because it will be out of date.
- 4.6 We intend to publish a new Code of Practice to take account of the new powers proposed in this document. It will set out the circumstances in which information can be sought, who is authorised to use the new powers, and the penalties for breaching the Code. We will involve those from whom we will seek information in the details of the Code, but we would welcome views now as to its contents.
- 4.7 We take a variety of measures to protect customer information from unauthorised access and disclosure and to detect and deter our staff from doing this:
- we have produced detailed guidance to staff on when customer information may be disclosed to third parties, to ensure compliance with our policy and the law. The latest copy of this guidance, the *Protection of Customer Information Guide*, can also be viewed on our website;
 - where staff have access to DSS computer systems, it is only to those parts of systems and those customer records which are necessary to perform their duties. Random samples of accesses that have been made to computer systems are checked by managers to ensure that these are for legitimate business reasons and that there is evidence to support this. In addition to these random checks, we regularly examine computer data for evidence of more deliberate abuse, such as browsing of computer records for personal reasons;

- DSS computer systems have comprehensive audit trails (records of the activity on a particular record, or by a particular member of staff) which enable any suspicion of misuse to be investigated;
- the unauthorised disclosure of official information is considered to be serious misconduct by the DSS, which may result in dismissal. Similarly, misuse of DSS computer systems, which includes unauthorised access to computer records, is also considered to be serious misconduct, and may result in dismissal;
- in addition to any disciplinary action which may be taken, the DSS will initiate legal proceedings where they are considered appropriate, for unauthorised access to, or disclosure from, social security records; and
- we have included in social security legislation a specific offence of disclosing information to unauthorised persons. Section 123 of the Social Security Administration Act 1992 makes it an offence for anyone who is or has been employed in social security administration to disclose personal information acquired in the course of their employment without lawful authority. An offence under this section is punishable by a term of up to six months' imprisonment and/or a fine.

4.8 We would welcome views as to whether the safeguards described above, including the proposed new Code of Practice, are sufficient.



Reducing the burden on business

- 5.1 We believe that fraud within the tax and benefits system is a burden on the honest taxpayer, whether they are individuals or businesses. Unpaid tax and overpaid benefits represent a huge cost that must be made up by higher taxation and lower public spending to help the law abiding. What fraudsters steal through benefit fraud could be spent on hospitals, schools, and numerous other public services.
- 5.2 Whilst benefit fraud is largely seen as customer fraud, it also allows unscrupulous employers to gain an advantage over their competitors. Firms who knowingly employ people defrauding the social security system are able to undermine those who choose not to. They may undercut their prices and harm the prospects of those who act within the law.
- 5.3 However, we must avoid wasting resources – either our own or those of the businesses from whom we seek information – in pursuit of checks that seldom yield results. We will seek to obtain information only where there is a reasonable prospect of success. We want to work with businesses in order to achieve this. Consequently, over the consultation period, we will be seeking views from businesses and business representatives about what steps we can take to ensure that we do not place unreasonable demands on businesses. We will also work with them to develop a firm estimate of the volume of enquiries that could be made, the best way of making these enquiries, and the cost to business that would be involved.
- 5.4 To begin this debate, this chapter sets out a preliminary Regulatory Impact Assessment, including provisional estimates of the possible volume of enquiries and costs.

Preliminary Regulatory Impact Assessment – purpose of measures and intended effects

- 5.5 This document consults the public on whether or not the Department of Social Security (DSS) should be able to obtain information from the private sector in order to help crack the problem of fraud and error in social security benefits. It seeks to set out how such information could be used to check claims before we pay them, to check entitlement during claims, and to catch fraud where it slips through those checks.

Options

- 5.6 The DSS can obtain information from three points:
- the claimant;
 - other government departments; and
 - the private sector.
- 5.7 We already receive information from claimants and from other government departments. For example, we ask claimants to provide documents to prove who they are, and we obtain information from the Inland Revenue about when people start work. Therefore, the questions are:
- Do we continue with only the information we can already obtain?
 - Do we take powers to obtain new information from the private sector?
- 5.8 This document has explained that fraud occurs because claimants lie about their circumstances. It has also explained that claimants do not lie only to DSS, but that they also lie to other government departments. However, Chapter Three explains that the private sector often knows the truth about these people. This is why the DSS is consulting on obtaining information from the private sector.

The proposals

- 5.9 The DSS is considering taking new legal powers to obtain information from the private sector about particular individuals who are suspected of fraud. They may be suspected for a variety of reasons. In some cases, DSS will have received information from the public which results in a fraud investigation. In other cases, details provided at the point of claim, or uncovered when the claim is being reviewed, might make a benefits officer suspicious enough to cross-check information with the private sector. Suspicion may also arise because a person is in a group which is known to have a high proportion of fraud and error based on reliable information from our research into the scale and nature of fraud.
- 5.10 This document also puts forward the idea of obtaining general information which is not sensitive where this would help fight fraud – for example, obtaining details of premises where no water or electricity is being consumed and checking to see if anyone claiming benefit says they live there. However, DSS respects people's right to privacy and their right to expect confidentiality from their bank, building society and so on. Consequently, we are not considering making general enquiries about sensitive information for no good reason – for example, obtaining information on bank accounts *en masse* is not envisaged.
- 5.11 This document also invites views on whether DSS should be able to exchange information with the insurance industry in order to combat benefit and insurance fraud. More on all these proposals can be found in Chapter Three.

Benefits

- 5.12 DSS cannot fight fraud without information. We estimate that between £2 billion and £4 billion of tax payers' money is lost because of fraud and error in social security each year. Consequently, the benefits of obtaining information from the private sector would be significant. For example, in Income Support (IS) and Jobseeker's Allowance (JSA), over £400 million is lost through people lying about their earnings, income and capital each year. If fraud through this means was reduced by 25 per cent as a result of these measures, we would save over £100 million every year.

Compliance costs for business

- 5.13 Last year, the DSS conducted:

- over 700,000 fraud investigations;
- 1.2 million checks at the point of claim on IS and JSA; and
- 1.3 million checks during IS and JSA claims.

In many instances, we will be able to check details with claimants to our satisfaction, or the claimant will confess that they had lied or omitted to tell us something that would change the amount of benefit they were entitled to. In other instances, the information we need could be obtained from another government department. We estimate that:

- up to 75 per cent of fraud investigations might require us to make a check with a private sector source, and that this check could take an average of 15 to 45 minutes (some will take much less time than this while others could take much longer); and
- up to 20 per cent of checks conducted by DSS at the point of claim and during the claim could require us to make an enquiry of the private sector, and that these enquiries could take an average of 5 to 15 minutes each.

Based on the earnings of clerks and cashiers, including employer's overheads, being £16 per hour (*New Earnings Survey*, 1999) we estimate that the total cost to business could be between £2.8 million and £8.3 million.

- 5.14 Should these measures be introduced, their impact would fall upon larger businesses such as the large financial institutions and utility companies. We do not expect any impact on smaller businesses.
- 5.15 Local authorities will need to make similar enquiries about Housing Benefit (HB) and Council Tax Benefit (CTB) claimants, although enquiries made by the DSS will not need to be duplicated by local authorities. We do not expect the cost to business resulting from these enquiries to be more than half that brought about by DSS enquiries, that is between £1.4 million and £4.1 million.

- 5.16 These costs do not take account of any savings to the private sector that might result from DSS uncovering, or helping them to uncover, frauds against businesses. For example, a person claiming from DSS and an insurance company on the basis of unemployment when they are actually in work.

Minimising the impact

- 5.17 Should these measures be introduced, DSS would work closely with businesses to minimise the impact upon them. Any legislation would make clear that DSS could not make unreasonable demands upon businesses – for example, ask for detailed information to be provided in an unreasonable time. The precise detail of how the powers would work in practice would be fully set out in a published Code of Practice as discussed in paragraph 4.6.



- 6.1 This consultation document has been prepared to provide an outline of the possibilities for obtaining information from the private sector. It results from the report by Lord Grabiner QC in which he said “I recommend that the Government should examine how it can make use of information from private sector sources, put in place a Code of Practice and, if necessary, legislation”.
- 6.2 This document is intended to provide you with an opportunity to express your views on these possibilities before we develop detailed proposals to bring before Parliament. We are particularly interested in your views on the issues raised in Chapter Three, the safeguards described in Chapter Four and the Regulatory Impact Assessment in Chapter Five.
- 6.3 The DSS will look at all of the responses. We will provide a summary of responses so that you can find out who responded and the consensus of what they said. If you would not like your identity to be published please indicate this clearly on your response.
- 6.4 The address for responses to the consultation process is:
- Data Sharing Team
Department of Social Security
6th floor
The Adelphi
1–11 John Adam Street
London WC2N 6HT
- Responses can also be emailed to: datasharingteam@ms41.dss.gsi.gov.uk
- 6.5 **The closing date for replies is 21 October 2000.**
- 6.6 This document is available from the DSS website at <http://www.dss.gov.uk>.

Further copies of this publication are available free of charge from:

Welfare Reform (Fraud)
Freepost (HA 4441)
Hayes UB3 1BR

Tel: 020 8867 3201

A service for textphone users is available on:
020 8867 3217

The lines are open Monday to Friday from 9am – 5pm.
Please quote code BFGIN.

Copies are also available in large print, Braille, audiocassette and in Welsh from the above address.

This document can also be accessed on the Internet at:
<http://www.dss.gov.uk>

© Crown copyright
Produced by the Department of Social Security
Printed in the UK
July 2000