CABINET OFFICE

IDENTITY FRAUD: A STUDY

Cabinet Office
July 2002

CONTENTS

Foreword	3
Executive Summary	4
PART ONE: THE PROBLEM	**7**
Chapter 1: Introduction	7
Chapter 2: The extent and nature of the problem	9
Chapter 3: How is it possible to establish a false identity?	17
CHapter 4: Counter-fraud activity	27
Chapter 5: Lessons from the private sector	31
Chapter 6: Lessons from overseas	36
PART TWO: APPROACHES TO SOLVING THE PROBLEM	**44**
Chapter 7: The need for a strategic approach	44
Chapter 8: Securing the issue of identity	46
Chapter 9: Countering offences	57
Chapter 10: Detection and prosecution of identity fraud	62
Chapter 11: The way forward	69
ANNEXES	**70**
Annex A: Meetings held by the project team	70
Annex B: Extent of the problem by organisation	73
Annex C: How secure is the government's issuing of documents used as evidence of identity?	79
Annex D: Major national databases in the public sector	85
Annex E: Glossary of terms	86

FOREWORD

Identity fraud is a serious and growing problem for the UK. Identity theft is a harrowing experience for the individuals whose identity is taken over or stolen. And identity fraud and theft have many and increasing links to organised crime. Illegal immigrants, trafficked into the UK by organised criminals, need false identities to access goods and services here. In running drugs and laundering money, concealment is of the essence – and false identity can help. False identity is also the key to much financial fraud, for both the public and the private sectors.

It is against this background that the Government launched a study to explore the extent and nature of identity fraud and theft in the UK, both in the government and in the private sector, and to come up with possible solutions to the problem drawing on best practice both in the UK and overseas. As identity fraud is a cross-departmental problem, the Cabinet Office drew together a team from a number of government departments to look at the issue. Interviews with a wide range of public and private sector organisations informed the team's thinking.

The study concludes that we will never completely eliminate identity fraud, but that there is much that we can do to make life very much more difficult for the organised criminal – and the opportunist. Tightening up the processes used for the issue of documents commonly used as evidence of identity – passport and photocard driving licence – can make identity fraud very much harder to perpetrate. Action here is already in hand and more is planned. More thorough checking of identity at point of use would be both possible and desirable. And better joining up of counter-fraud activity, both within government and between government and the private sector, can also make identity fraud easier to detect and to punish.

This study has been completed in conjunction with the work on entitlement cards, the subject of a parallel consultation exercise by the Home Secretary. The analysis and conclusions of this report clearly have a bearing on the consideration of entitlement cards, but are not dependent on their adoption. A number of consultation questions on identity fraud are set out in the Home Office consultation paper, drawing on the work of this study, and the Government would welcome views on these.

We are determined, as a government, to crack down on identity fraud. To do so effectively will require co-operation from both the private sector and from individual members of the public. I am grateful for the help extended to the study team in its work by many private sector organisations. I hope – and confidently expect – that we can widen those exchanges of information and ideas during the consultation period. These, above all, are problems to which we need to find the way forward in partnership.

The Rt Hon Andrew Smith MP

EXECUTIVE SUMMARY

The Extent of the Problem

1. ID fraud is an important and growing problem linked to organised crime in a number of forms: illegal immigration (including human trafficking); money-laundering and drug running; and financial fraud against government and the private sector.

2. It is not easy to gauge the amount of identity fraud. But the minimum cost to the economy is in excess of £1.3bn per annum. This compares with the estimated total economic cost of all fraud of at least £13.8bn per annum. Identity fraud is possible because of weaknesses in the processes used to issue documents used as evidence of identity, and the processes used to check identity at point of use.

3. Most current processes for issuing government documentation used for identity verification, and a range of unique identifying numbers, do not meet the highest private sector or overseas standards of security. Government databases are also considerably less than fully accurate, and checks on identity at point of use less than in the private sector.

4. Where financial fraud is concerned criminals target the public and the private sector indiscriminately, often looking for the weakest links. But counter-fraud efforts are not similarly joined up. “ID theft” is not in itself an offence, and penalties for those who make fraudulent applications (for example for passports) are very small. Prosecutions are comparatively rare.

5. The private sector does not, for the most part, entirely rely on government-issued documents to check identity where its commercial interests are at stake. Rather, it checks identity against databases held by credit reference agencies which show the “historical footprint” left by an individual in the community. The footprint is also what those legitimately developing an alias identity to work undercover find it hardest to invent, when an identity is fabricated. Many private sector bodies also check applications for goods and services against a central register of frauds and fraudsters.

6. Some overseas countries use identity cards as part of their counter-fraud strategy. An identity card is only as secure as the processes used to issue it and the safeguards employed against counterfeiting and theft. In the US, where the social security number and associated card have, through use and custom, become the de facto unique identifier and identity card, identity theft is rife.

The Way Forward

7. Countering identity theft and fraud requires an overarching strategy to make the issue of documents used as evidence of identity and the issue of unique identifying numbers more secure, to counter the use of counterfeit and stolen documents and to detect and prosecute identity fraudsters. Tackling just one of these areas will not yield significant dividends.

8. The creation of a single document (an entitlement card) could be beneficial in replacing the present “mosaic” of documents used to establish identity if accompanied by much more secure processes for the issue and use of the document.

9. Processes for issuing documents used as evidence of identity need to be made more secure. The source document on which passport and driving licence issue depends – the birth certificate – is not itself secure, nor is the system of countersigning by a professional. For most people, checks against databases run by credit reference agencies will give much more satisfactory validation and verification of identity. For others, face-to-face interviews represent a secure alternative.

10. Additional levels of security can be achieved through checking applications against a register of known frauds and fraudsters, such as is run in the private sector by CIFAS, and through the use of IT systems which can check applications for consistency against data already held by government.

11. For the longer term, it may be worth giving consideration to the creation of a register of citizens who have left the UK and are resident overseas.

12. A central register of stolen documents (passports, driving licences, National Insurance number cards etc) would reduce the value of such goods in the market. And wider exploitation of simple anti-counterfeiting measures can reduce the use of wholly fictitious identities. The concept of a biometric marker on key documents used as evidence of identity has attractions. But the technology has yet to be proven on any sizeable population; and introducing such a system would carry significant risks and costs.

13. Detection and prosecution of identity fraud falls to many government departments and private sector bodies. Stronger co-ordination of counter fraud activity is needed. The existing cross-departmental group – the Interdepartmental Identity Fraud Forum (IIFF) – responsible for joining up government activity to counter identity fraud should be reconstituted with stronger terms of reference and on the basis that private sector organisations should also be invited to join the group. It would be helpful to raise the profile of work to prosecute offenders.

14. Prosecution of offenders should be pursued more vigorously. One way to ensure this might be through the creation of a new offence of identity theft, which might make successful prosecution both more worthwhile and easier.

Consultation Questions from the Home Office Consultation Paper

The parallel Home Office consultation paper on Entitlement Cards invites views on a number of consultation questions on identity fraud and the strengthening of government checks on identity. These questions reflect the main findings of this report. They are:

P16 The Government invites views on the early steps it would like to take to tackle identity fraud and welcomes expressions of interest from the private sector to collaborate in this work.

P17 Views are invited on whether checks on applications for passports and driving licences should be strengthened to the degree outlined in Chapter 5 of the Home Office document (on how a scheme might work in practice) whether or not the Government decided to proceed with an entitlement card scheme based around these documents.

P18 If more secure passports and driving licences were issued based around a common identity database shared between the UK Passport Service and the DVLA, the Government invites views on:

- whether it should take the necessary legislative powers to allow other departments to access this identity database to allow them to make their own checks;
- whether it should allow the private sector to access the identity database provided this was done with the informed consent of subjects.

P19 Views are sought on whether the Government should procure a service from the private sector which checked applications for services against a number of databases used by the credit reference agencies or similar organisations and selected biographical data held by the Government.

P20 Views are invited on whether a summary-only offence of identity fraud should be created.

PART ONE: THE PROBLEM

CHAPTER 1: INTRODUCTION

Why this study?

1.1 The theft of an individual's identity is a harrowing experience for the victim and the theft and fabrication of identities is of increasing concern to the state.

1.2 For individuals, the experience of identity theft can touch centrally on the victim's relation to the world. Victims may need time to rebuild their reputations and their credit histories. Most distressing are "Day of the Jackal" frauds, where a criminal assumes the identity of a dead infant. Parents may be contacted by the police to answer for crimes allegedly committed by someone who in fact died in infancy.

1.3 For the state, theft and fabrication of identity is linked to organised crime in a variety of ways, for example:

- illegal immigrants require identity to access goods and services in this country;
- drug couriers and criminals engaged in money-laundering rarely operate under their own identity. Identity theft and fabrication constitute one of a number of ways of avoiding detection;
- organised criminals can and do perpetrate large-scale frauds against the state and against private sector bodies through the use of false identities.

1.4 Evidence from the private sector (see paragraph 5.12) shows that identity fraud has grown significantly in recent years. Trends in criminal activity suggest that it will continue to increase – one possibility is that this will be facilitated by the emergence of specialist identity brokers.

1.5 This study takes stock of the extent and nature of the problem and develops a range of solutions to counter identity fraud.

The method used in the study

1.6 The study was carried out by a team of civil servants drawn from the Department for Work and Pensions (DWP), Inland Revenue (IR), HM Customs and Excise and the General Register Office for England and Wales (GRO(E&W)) and led by the Cabinet Office.

1.7 The team visited a wide range of government departments, private sector organisations and bodies responsible for detection and prosecution of identity fraudsters.

Scope and relation to other work

1.8 A number of other studies bear on issues addressed in this report, notably:

- work on entitlement cards. This is the subject of a parallel consultation paper by the Home Office;
- the PIU report on privacy and data-sharing bringing forward proposals in this area, which was published in April 2002.

1.9 The action recommended in this report concerns primarily fraud against government. But that action should have knock-on consequences for action against identity fraud in the private sector. For example, if the issue of passports and photocard driving licences becomes more secure, their use as proof of identity when exchanging money at bureaux de change becomes more secure.

Structure of the Report

1.10 Part One of this report assesses the present position:

- Chapter Two discusses the extent and nature of the problem;
- Chapter Three discusses the issue of documents used as evidence of identity;
- Chapter Four discusses current counter-fraud activity;
- Chapters Five and Six discuss lessons learned from the private sector Ch-archangestr667gy 0 -tackleentity;

•Chapter Four discusses current couEight /1 -o7ronslDys•

CHAPTER 2: THE EXTENT AND NATURE OF THE PROBLEM

Summary

2.1 Identity fraud arises when someone takes over a totally fictitious name or adopts the name of another person with or without their consent.

2.2 It is not easy to gauge the extent and nature of identity fraud:

- proper measurement would need to take account both of obtaining genuine documentation under false pretences and of theft and counterfeiting;
- what is measured is only **detected** identity fraud.

2.3 But the team's work suggests that the minimum cost to the economy of identity fraud is at least £1.3bn pa. That is in addition to the identity fraud committed in order to access goods and services, for example by illegal immigrants.

What is identity and what is identity fraud?

2.4 There are three basic elements of identity:

- biometric identity: attributes that are unique to an individual, i.e. fingerprints, voice, retina, facial structure, DNA profile, hand geometry, heat radiation, etc;
- attributed identity: the components of a person's identity that are given at birth, including their full name, date and place of birth, parents' names and addresses;
- biographical identity, which builds up over time. This covers life events and how a person interacts with structured society, including:
  - registration of birth;
  - details of education/qualifications;
  - electoral register entries;
  - details of benefits claimed/taxes paid;
  - employment history;
  - registration of marriage;
  - mortgage account information/property ownership;
  - insurance policies;
  - history of interaction with organisations such as banks, creditors, utilities, public authorities.

2.5 Identity fraud arises when a person pretends to be someone else in order to obtain goods and services through:

- the use of a totally fictitious name (sometimes referred to as a false identity); or
- the adoption of a real person's name (alive or dead) with or without their permission (sometimes referred to as a hijacked identity).

2.6 Misrepresentation of circumstances, where a person gives incorrect details about one or more aspects of their identity (eg lying about their age to reduce their motor insurance premium or to avoid compulsory retirement) is not usually considered to constitute identity fraud. However, simple misrepresentation may stray into the invention or capture of a whole new identity. If a person is aware that an organisation's database identifies people solely by their date of birth, then by giving a false date (even if it is only wrong by a single day) they are knowingly and fraudulently allowing the organisation to attribute them with a separate identity.

2.7 Identity fraud is not an offence per se, but an enabler for other offences. It is very rarely committed for its own sake. There are three basic reasons for a person to develop a second (and possibly, subsequent) identity:

- **to avoid being identified in the original identity (concealment).** This includes illegal immigrants wishing to stay in the country, money-launderers, disqualified drivers who wish to continue driving, paedophiles wishing to continue working with children, people with poor credit histories wishing to obtain financial services, wanted criminals and bigamous marriages. False identity is also used by those working undercover – some terrorists etc working against the interests of the UK, but equally by undercover law enforcement officers, and the security services;
- **to make a financial profit from some form of fraud.** This includes credit frauds such as defaulting on loans/mortgages, multiple claims to welfare benefits, claiming educational qualifications to obtain a certain job;
- **to avoid financial liability.** This includes reneging on outstanding debts, tax/VAT avoidance and avoiding paying child maintenance.

2.8 Identity fraud is sometimes categorised as "organised" versus "individual". However, care must be taken to maintain a fairly loose interpretation of "organisation" in this context. Any individual seeking to commit identity fraud is likely to need outside help – whether to purchase genuine, forged or counterfeit documents or to help them make use of documents obtained by deceit. But such help can be fairly small scale and informal in nature.

Direct measurement of identity fraud is difficult

2.9 Accurate measurement of the extent and cost of any fraudulent activity, including identity fraud, is notoriously difficult. Although detected fraud can be measured, extrapolating that into a total figure requires a degree of guesswork.

2.10 Measuring identity fraud presents additional problems. There is often no clear distinction between identity fraud and fraud generally. The absence of an offence relating specifically to identity fraud does not help. Organisations, including government departments, which are not looking for identity fraud are unlikely to measure it.

2.11 Moreover, identity fraud can be perpetrated in a number of ways: through obtaining genuine documentation from government sources (but under false pretences), through theft or sale of genuine documentation (including unissued blanks), and through forgeries. All need to be estimated to give a true account of the picture.

2.12 What can easily be measured by government organisations which issue documents widely used as evidence of identity, is the extent of attempted fraud that is **detected** (though some organisations do not at present routinely collect information on detected identity frauds). Detected fraudulent applications for passports or driving licences form an unknown percentage of the totality of fraudulent applications.

2.13 Detection rates depend on the thoroughness of the processes used within an organisation to authenticate an identity. Authentication requires both validation and verification: validation being the process of establishing that a claimed identity exists (ie. relates to a "real" person) and verification being the process of establishing that the person using the identity rightfully "owns" it (often done by testing for detailed knowledge of the identity which typically only the rightful owner would have). Lax procedures (driven, for example, by customer service priorities) can lead to low detection rates.

Current figures suggest the problem is large

2.14 Even when the extent of fraud is known, it is not a simple process to translate this into a figure representing the financial cost. Research for this report suggests an annual figure of £1.3 billion pa is the minimum quantifiable cost to the economy arising from identity fraud. This figure is certainly an underestimate, as it only includes those figures that are available, and does not include areas such as Local Government, health services or education where it is known that identity fraud exists, but there is not sufficient data available to estimate the cost. Details are at Annex B. Box 2.1 summarises some key points. The figure of £1.3 billion compares with an estimated total economic cost of all fraud (not just identity fraud) of £13.8bn pa. That estimate, which was also considered to be an underestimate, was generated by National Economic Research Associates (NERA) in its report "The Economic Cost of Fraud", prepared for the Home Office and the Serious Fraud Office and published in late 2000.

2.15 In many cases the costs and benefits associated with tackling identity fraud, though large, are unquantifiable – for example, the cost of a passport in the hands of a terrorist, the cost of a paedophile continuing to work with children or the cost of an election result won on the basis of fraudulent ("personated") voters.

2.16 In attempting to assess the scale of the problem the project team has drawn upon information from agencies, departments and the private sector. Many of the figures given are estimates; for others local data has, where possible, been extrapolated to give a national figure. Box 2.1 sets out evidence both that relates directly to the scale of identity fraud and to indirect evidence, i.e. that which points to the use of fraudulent identities for other purposes, for example:

- trafficking of people into the UK and illegal immigration more widely: if illegal immigrants are to enjoy goods and services, from the public or the private sector – or, indeed to work – in the UK, they will usually require a (false) identity;
- drug running: drug couriers also often adopt a false identity rather than risk using their own;
- money-laundering: money-laundering depends on concealment of identity, not on identity fraud per se (concealment may be achieved through the creation of a fictitious company as much as through false individual identities). But money-laundering regulations require the providers of financial services to "know their customer", and the Joint Money Laundering Steering Group has produced (and updates) Guidance Notes on how to do this;
- organised fraud: developing multiple identities to make fraudulent claims to state benefits or, in the private sector, credit card applications etc. Organised fraud – rather than individual fraud – is increasingly likely to be the source of identity fraud in future, as new technology, such as "chip and PIN" procedures for the use of credit and debit cards, cut down on the scope for opportunistic identity fraud.

2.17 When seen in percentage terms, some of these figures suggest that the extent of the problem is not that widespread:

- the figure of 1,484 detected fraudulent passport applications represents 0.03% of total passport applications;
- the figure of 3,231 driving tests stopped represents approximately 0.23% of the total number of tests;
- the number of entry documents at UK ports of arrival in 2000 detected as being counterfeit were just 0.006% of the total.

Box. 2.1: The Extent of Identity Fraud

Coming up with a "headline" figure for the extent and cost of the problem is fraught with difficulty. Nevertheless, the following figures for the year 2000–2001 (except where otherwise indicated) show the scale of the problem:

- A total annual cost of at least £1.3 billion;
- 3,231 driving tests terminated prematurely because of doubts over the driver's identity;
- 1,484 fraudulent passport applications detected;
- approximately 50 cases of fraudulent documentation detected every month at Terminal 3, Heathrow;
- In the course of a two week exercise targeted at Portuguese documents in June 2001, 59 fraudulent documents detected at selected UK ports and the Benefits Agency National Identity Fraud Unit. The majority were counterfeit identity cards, detected at NIFU;
- Although there is little reliable information on the number of people trafficked into the UK, a recent Home Office study estimated that 1,500 women a year are trafficked for sexual exploitation;
- In 1999 over 21,000 illegal immigrants were detected; during the same period 5,230 were removed or left voluntarily;
- 18,500 referrals to the Financial Services Authority under the money laundering regulations;
- 564 cases involving identity fraud identified by the Benefits Agency's Security Investigation Service;
- In the private sector, one estimate is that around 1–2% of transaction value is lost through fraud and that about 3–5% of all fraud is identity fraud.

An account of the extent of the problem on a department by department basis is given at Annex B.

2.18 But there is reason to believe that the quoted figures do not give an accurate estimate of the extent of identity fraud:

- processes used in the issue and checking of documents used as evidence of identity are not secure (see Chapter 3 below);
- the financial cost of identity fraud is almost certainly under-reported. In the private sector, in particular, it is suspected that much identity fraud is not fully investigated or categorised as such, being written off instead as "bad debt";

- to this data on financial costs we can add data from the DWP on National Insurance Numbers (NINOs), and in particular the Secure NINO Allocation Process ("SNAP"). Details of SNAP are in Box 2.2. In these cases, there are no direct cash benefits of identity fraud. Rather individuals seeking a NINO (who will in almost all cases have arrived from abroad) may, in particular, be trying to pass one of the hurdles on the road to employment.

Box 2.2: The Secure NINO Allocation Process ("SNAP")

SNAP was originally piloted in Balham and since April 2001 has been introduced across the country. Its effect is to tighten the gateway to NINOs by aligning processes for both employment- and benefit-inspired applications including:

- face to face interviews to corroborate documentary evidence with identity information supplied by the applicant and employer where appropriate;
- introduction of UV scanners to identify forged and tampered documents;
- standardised training to improve the standard of interviewing and 'back office' checking to identify duplicate numbers etc.

SNAP resulted in 579 arrests between January 1999 and March 2002. In the first ten months of the national roll out over 11,000 applications resulted in the non-issue of NINOs in cases where previous processes may well have allocated a number. This includes instances where documentary evidence was not corroborated by the interview, false documentation was identified, the application was withdrawn (e.g. where more evidence was requested and not supplied) or a NINO was not required. It does not include cases where the person failed to attend their interview.

The problem is growing

2.19 Strong evidence that identity fraud is a growing problem comes from *CIFAS, the UK's Fraud Prevention Service*, which was originally set up as a forum for lenders to share information about fraud and attempted fraud and now has members from across industry. CIFAS figures showed an increase in identity fraud of 462% in 2000 compared with the previous year, followed by a further increase of 122% in 2001, although some of the increase in 2000 is accounted for by changes in their systems/growth in membership. Fuller details on CIFAS are in Chapter 5.

2.20 The Association for Payment Clearing Services (APACS), the body that deals with fraud relating to bank and credit cards, estimates that all credit card crime has grown from £95 million in 1998 to £411 million in 2001 and will increase further to £650 million over the next four years. They attribute the vast majority of this growth to organised crime. The industry view is that as authentication procedures for credit cards are significantly strengthened over the next two years, fraudsters will shift their focus further upstream in the process, resulting in more "account takeover" (whereby genuine accounts are hijacked for fraudulent purposes) and other identity fraud.

Case studies further illustrate the extent and nature of the problem

2.21 We can also bring life to these dry numerical indications of the extent of the problem by considering some cases of successful counter-fraud activity. Case studies are in Boxes 2.3 to 2.6. These case-studies further illustrate the nature of the problem – and the difficulties in measurement.

Box 2.3: Case Study: A Success for CIFAS

The CIFAS system prevented one potential fraudster, who was eventually prosecuted and imprisoned, from succeeding with an intricately-planned £1m scam. Having sat 28 driving tests across the country, obtaining different identity documents from each, and registering on the electoral roll for a variety of rented properties, he was able to open multiple bank accounts. He cycled money between these accounts for several years, building up a healthy transaction history. This then enabled him to obtain multiple loans and credit. One CIFAS member became suspicious by the unusual nature of payments between bank accounts and the subsequent data search revealed the extent of the scam, which affected many more members.

Box 2.4 Case Study: An Identity Factory

A man and woman were charged with conspiracy to make false instruments of payment following a police operation that resulted in the couple's house being raided. Computer equipment worth around £100,000 was recovered. This included a plastic card printer, a plastic card embosser, a high quality colour laser printer and scanners. Rubber stamps were also found in the name of some high street banks, the UK Immigration Service and a foreign immigration service.

14,000 blank documents were recovered, including:

- blank driving licences;
- bank and utility company statements;
- birth and marriage certificates (both UK and foreign);
- educational certificates;
- UK Immigration Service headed paper;
- NHS Medical Cards;
- Nursing qualification certificates; and
- wage slips.

Thousands of NINO cards were also found in various stages of preparation.

"Shopping lists" were also recovered that indicate that the couple had been providing a supply of false documents to order.

Box 2.5: Case Study: Income Tax Fraud

Three individuals worked for various tour operators over a period of time. Their declared income to the Inland Revenue was minimal. They used their funds to buy various residential property around the Folkestone area and then later expanded into West London. The income from these properties – 72 in all – and gains from the sales were not declared to the Inland Revenue.

What appears to have been a very simple fraud was anything but, as some of the properties were bought in false or hijacked names or in names that had been varied slightly. Not only had the business enterprise and properties been hidden from the Inland Revenue but the defendants had also hidden the true ownership of the properties from the local authorities and their tenants: the owners used their aliases to open bank accounts into which rent was paid.

One particular alias used belonged to a US national currently living in New York. She had been a student in the UK and had lived at one of the properties owned by the defendants. When she had returned to the US the defendants hijacked her identity, including her National Insurance number.

In court, the judge found all three defendants guilty and awarded not only custodial sentences, but confiscation in the sum of £2.5 million.

Box 2.6 Case Study: An Opportunistic Tax Fraud

A man purchased shares in privatised utility companies using 25 false names, mostly a combination of his own name, his mother's and wife's maiden names. It is an offence to purchase shares in this way. Having acquired the shares he opened over 100 bank and building society accounts.

A tax fraud arose from the fact that the annual dividends payable on the shares gave rise to a repayment of tax deducted on dividends. The fraudster claimed in each of his false names for each set of dividends he received – stating that the identity belonged to someone in receipt of State Pension. This generated tax repayments that he was not entitled to, involving £7,000 to him plus £600 to his wife. He is reported to have savings of over £300,000.

The fraudster also used the false identities to purchase property and he did not disclose the rental income on these. Further, he used the false identities to gain employment as an examination marker.

CHAPTER 3: HOW IS IT POSSIBLE TO ESTABLISH A FALSE IDENTITY?

Summary

3.1 It is possible to assume a false identity or obtain false documentation used as evidence of identity whether the tests of identity applied are "attributed", "biographical" or "biometric". But "attributed" identity is by far the easiest to assume under false pretences.

3.2 Current processes for issuing documentation used as evidence of identity are not secure. Government is currently examining afresh the issues surrounding the validation and verification of identity (and checks on identity at point of use) in the context of e-government.

3.3 Documents used as evidence of identity (once issued) can be checked against government and private sector databases. But the databases are not all that clean. They suffer from "excess" records (mostly not fraudulent) and are not, for the most part, actively managed.

How is it possible to assume a false identity?

3.4 It is possible to assume a false identity – either a wholly fabricated identity or the identity of another person – in a number of ways:

- the elements of identity that constitute "attributed identity" can be assumed by securing the appropriate documentation. These can be genuine documents issued by government departments on the basis of false information supplied by applicants. Alternatively, genuine documents once issued can be stolen, or indeed sold on (there is believed to be some trade in NINOs, with people leaving the country and not planning to return who are prepared to sell on their numbers and NI records to others). A third option is forgery of documents either for "primary" use, or false or forged foreign documents can be exchanged for or used to acquire the genuine UK product;
- a "biographical identity" can be assumed only by living in a community and appearing on appropriate public and private databases, such as the electoral roll, on an ongoing basis. It is much harder for those working undercover to acquire the right biographical identity than to acquire suitable documentation. But this is of course possible with enough time and ingenuity (periods allegedly spent overseas in a history can cover absence from UK databases);
- "biometric identity" cannot be assumed by another human being. But to be used in practice, an individual's biometric marker must be matched either against an identity document containing a matching biometric (eg fingerprint) or against a database (as in iris recognition). Biometric identity – or at least documentation using biometric markers – can be falsely assumed if processes for its issue are insecure and/or if identity is not confirmed through biometric checks at point of use. The effect of this can be minimised if the central system can guarantee to only issue an identity document on the basis of a unique biometric.

3.5 False identity can be assumed either upstream of an offence (ie at the point of document issue or entry onto a database, eg when a credit card is issued) or at the point that an offence is committed (eg when a stolen credit card is used by someone other than the cardholder.)

A variety of documents are used as evidence of identity and can be seen as forming a mosaic of documentary evidence for identity

3.6 The UK does not have a national identity card or single identity database. So a number of documents issued by government, none of which were designed to be universal unique identifiers, are used for validating and verifying identity.

3.7 The two most widely used documents which are accepted as evidence of identity by public and private sector organisations are:

- passport – but this is a travel document rather than proof of identity (although it includes a photograph);
- photocard driving licence – but this is proof of ability/right to drive, (although it includes a photograph).

3.8 Other government-issued documents relevant to the establishing of identity include:

- the birth certificate – but this is a record of a historical event and does not have a necessary link to the individual bearer of the document;
- National Insurance number (NINO)/NINO Card – but this is only an identifier for the purpose of recording National Insurance contributions and income tax and for claiming benefits (the NINO card even states “This is not proof of identity”);
- NHS Number/NHS number card – but this is merely proof that a person is registered with a GP.

3.9 Similarly although the VAT registration certificate is not an identity document it is widely accepted that the registration of a trader for VAT and the issuing of a VAT number lends the trader legitimacy. An entry in the electoral register is also widely used as a reference to confirm someone’s identity.

3.10 Although the Home Office Immigration and Nationality Department (IND) do not issue any documents that they intend should be used as evidence of identity they do endorse passports with a person’s immigration status and issue forms which serve as passport replacements (eg the SAL1 form). They also correspond with immigrants and asylum seekers and this correspondence is sometimes used by other government departments as evidence of identity. For the future, the Home Office will increasingly issue asylum seekers with an Application Registration Card (ARC) containing a biometric (a fingerprint). This will prevent multiple applications and the sale of documents between asylum seekers.

3.11 Each of these government-issued identifiers can be used as a starting point or ‘breeder document’. One document can be used as evidence of identity to obtain another, more persuasive item of evidence of identity.

The issue of documents forming this mosaic is far from highly secure

3.12 It is clear, then, that many processes within government result in government issuing documentation that can then be used as evidence of identity elsewhere in both the public and private sectors to obtain other goods and services.

3.13 Few of these processes meet the highest standards of security. This is for a variety of reasons. All government bodies that issue documents used as evidence of identity take responsibility for trying to ensure, as far as is practicable, that documents are issued to the right person. But all departments are dealing with large volumes of throughput (for example 5.3 million passports per year) and they are all subject to conflicting business drivers and customer service requirements (for example issuing passports in time for people to go on holiday). There will always be a tension between security and control, customer service and process costs. The challenge is to devise systems for validating and verifying identity at acceptable cost in terms of impact on service delivery. Boxes 3.1 and 3.2 summarise the current issuing processes for passports and driving licences, two key documents used as evidence of identity.

Box 3.1 Passport Issue

Between April 2000 and March 2001 5.3 million passports were issued. In the same period 1,484 (0.03%) fraudulent applications were detected. Of these, 301 used deceased identities, 1,003 used another person’s identity or documents and 110 used a fictitious identity.

UKPS has recently set up a fraud and intelligence section which will provide an infrastructure and the skilled resource to provide a more systematic and consistent approach to fraud. They have also seconded a resource into NCIS to enhance links with the Police and to develop a protocol.

UKPS has recently amended the passport application form to encourage countersignatories to supply their own UK passport numbers. This will enable UKPS to check against their own database to verify the information they are being provided with and should reduce the time delays in writing to countersignatories selected for validation checks. UKPS may write to the countersignatory themselves or conduct checks with professional bodies such as the Law Society or General Medical Council.

On the basis that the vast majority of applications are genuine and so that resources can be better targeted on suspect applications, UKPS are considering how to use a credit reference agency as part of the validation process.

Box 3.2 Driving Licence Issue

There are currently 38 million driving licences in issue. Between April 2000 and March 2001 DVLA issued 5,400,040 licences which comprised 735,874 provisional licences; 1,152,237 renewals (licence expired); 831,584 exchanges of UK licences; 510,254 duplicates (licences lost or stolen); 2,128,895 replacement licences (change of name or address); and 41,196 exchanges for foreign licences. Around 17% of applications are rejected for a variety of reasons including incorrect fee and incomplete documentation. DVLA cannot be certain how many of these are processed on re-submission of the amended application.

In 60% of applications the supporting document is a UK passport. In these cases the passport is deemed to be proof of identity and only rudimentary checks are carried out. Where applicants do not provide a UK passport they provide a birth certificate (and marriage certificate where appropriate) plus a photograph which, together with the application form, must be endorsed by a countersignatory. DVLA do check a proportion of countersignatories. Any suspicious applications are referred to an enforcement section for further in-depth checks. Staff who work in this section are building up knowledge and expertise in identifying false documents.

As the driving licence system is required by law to be self financing DVLA is under pressure to keep cost increases to a minimum. The cost of resourcing any increase in the level of identity checks would need to be funded by an increase in the licence fee.

3.14 In the light of emerging conclusions from this study, DVLA and UKPS have begun to work together on proposals to improve the security of the issue of driving licences and passports. Details are given in Part Two of this report.

When identity is checked at point of use against other documentation or databases, processes are also far from fully secure

3.15 Every time an individual approaches government to obtain goods and services this inevitably results in the government department having a process to deal with the request. There is an inevitable tension between customer service and any enforcement effort which seeks to isolate suspicious applicants and prevent fraud occurring.

3.16 Most processes start from the need to provide a fast efficient service. But there are a number of ways in which government departments check identity. These include:

- ***checks against government databases –*** All departments check applications against their own databases to avoid duplicate applications. As part of the Modernising Government initiative departments have been encouraged to provide increased access to their databases to each other, where legal gateways permit. Thus Inland Revenue (IR) staff have access to DWP's Departmental Central Index (DCI) where the information

is relevant for their own function relating to National Insurance contributions and Working Families Tax Credit and are entitled to seek information from HM Customs and Excise in respect of their customers;

- ***checks against private sector databases –*** Most fraud sections in government departments have had for some years access to some private sector databases for electoral register information and companies such as Dun and Bradstreet for company data. Increasingly departments are turning to credit reference agencies such as Equifax and Experian to support their decision making and application processing service. The newly formed Criminal Records Bureau obtains applicants' consent to use Experian data as a means of corroborating the identity details they have provided;
- ***physical scrutiny of documents –*** Increased availability of IT equipment and software means that it is easier than ever for fraudsters to produce counterfeit documents at home. Utility bills in particular are considered to be easy to reproduce. The use of digital photographs and security features by DVLA and UKPS makes it harder to tamper with their documents and counterfeits are generally of poor quality. The serial numbers of stolen blank birth certificates are notified to departments. UKPS routinely check applications against these records particularly when they are presented with newly issued birth certificates;
- ***risk assessment/profiling –*** This is used to identify potentially fraudulent applications so that they can be subjected to greater scrutiny and more in-depth checks. For example, HM Customs and Excise has developed a risk assessment system to target potential missing traders who try to register for VAT. The Inland Revenue has been at the forefront of identifying potentially fraudulent applications through the application of risk assessment/profiling. For example all self assessment returns are subject to electronic risk assessment drawing on the information in the returns themselves and other information which has been provided to the Inland Revenue;
- ***use of biometrics and photographs –*** sophisticated use of biometric data, apart from law enforcement agencies who routinely use both fingerprints and forensic data as part of their investigations, is currently only in place in the case of the Home Office which records fingerprint details of all those who apply for asylum in the UK. But a number of departments use photographs to confirm identity. For example, candidates at both the theory and practice parts of the driving test must bring with them either a passport or another document bearing their photograph and their signature. Alternatively they may produce a photograph which has been endorsed with a certificate in the prescribed form by an appropriate person. Most bring a provisional photocard driving licence, issued by DVLA following their usual identity checks. At both stages the Driving Services Agency examiner must not conduct the test if the candidate fails to supply evidence of their identity.

3.17 The same tension between customer service and anti-fraud effort can occur in the private sector. But security there, in at least one important sector, is currently being stepped up. An initiative being taken forward internationally and in the UK to replace the current magnetic strip and signature panel on

credit and debit cards with “chip and PIN” technology. This will mean using a PIN whenever cards are used (ie not simply at cashpoints). This system is already in use in France – and has succeeded in exporting a lot of credit card fraud from France to other countries.

New issues for the validation and verification of identity arise with the government’s commitment to e-service delivery

3.18 The Prime Minister’s target that all government services should be capable of delivery electronically by 2005 raises new issues for the validation and verification of identity. The Office of the e-Envoy has been consulting on proposals about what authentication levels are appropriate to different sorts of e-transaction, on registration and enrolment for e-service delivery, and on how “digital certificates” of identity can be provided.

e-Transaction authentication levels

3.19 “Authentication” is the process of validating and verifying a claimed identity. This includes: establishing that a given identity exists; establishing that a person is the true holder of that identity; and enabling the genuine “owner” of the identity to identify themselves for the purpose of carrying out a transaction electronically.

3.20 The Office of the e-Envoy suggests that there should be four levels of authentication (0,1, 2 & 3) for e-transactions. Level 0 authentication is appropriate where the communications between the parties are of an informal nature. Level 1 authentication is appropriate where the relationships between the parties are of a personal nature but where mistaken identity would have a minor resource or nuisance impact on one or more of the parties involved (including the “real” person). Level 2 authentication is appropriate between parties which are of an official nature and failure to undertake the transaction may be interpreted as a statutory infringement that may incur a penalty, or may involve the communication of information of a commercially or personally sensitive nature. Level 3 authentication is appropriate between parties which are of an official nature and where mistaken identity may have significant financial impact or impact on the health or safety of installations or individuals.

3.21 The appropriate authentication level for each type of electronic transaction will be agreed jointly between the relevant government department and the Office of the e-Envoy. At present only a limited number of services are offered of which three (the filing of VAT (C&E) returns, PAYE returns and self assessment tax returns) are at Level 2. No government department currently offers electronic business transactions that require Level 3 authentication.

Registration and Enrolment

3.22 Before anyone is able to undertake a business transaction electronically they will need first to register with the Government Gateway and then enrol for one or more services provided by a government department.

3.23 At present there are two ways of registering with the Government Gateway – either by the individual choosing a password and being issued with a User ID, or with a digital certificate. No definitive guidance has so far been issued by the Office of the e-Envoy on the highest authentication level transaction that should be allowed via the use of a User ID and password but as described above IR services at Level 2 are based on User ID and password. It is also likely that before someone is able to make a transaction requiring a Level 3 authentication that a face-to-face interview between the parties involved would be required.

3.24 The private sector has not yet expanded to meet the anticipated demand for digital certificates by individuals. There is presently only one provider (Equifax). To validate and verify identity before issue of a digital certificate, Equifax run on-line checks to confirm that the applicant is aware of information that could only be known to the "genuine" individual.

3.25 The registration process itself will depend on the requirements of the particular service but will always involve giving a full name and choosing a password/obtaining a digital signature. A User ID is then sent in the post. This is an important safeguard built into the system. The address used is that held by the government department which runs the service the person is enrolling for. For example, to enrol with the Inland Revenue's internet service for self assessment, the citizen needs to provide their tax reference number and either their postcode or NINO. The details entered are then checked against the information held to verify identity (including address). Only where these checks are satisfied will the User ID be issued to the address already held by the Inland Revenue.

3.26 A person who is already registered and enrolled for one service may enrol for another using their existing User ID and password (or digital certificate). But they will not be able to use that service until they receive through the post to the address held by that second department the activation key for that service. So again there will be a cross match to known facts held by that department before that second service is accessible.

3.27 Once someone has enrolled for a service, processes are in place to validate and verify the identity of the person seeking to make an electronic transaction each time they do so. Some processes are more secure than others: for example, the requirement simply to quote a User ID and password prior to each transaction does not guard against a third party fraudulently using stolen or borrowed information. A digital certificate would be more secure if it included a form of biometric or if a number of questions were asked that only the "real" person would be able to answer.

3.28 It would seem then that e-service delivery confirms the emerging conclusion: that the surest way to validate and verify identity is through face-to-face interview or through validating identity against databases and verifying identity by checking that the applicant knows information that others would not be aware of. Next most secure are password and PIN systems with safeguards being operated by government departments.

Databases are not immune from problems: data is not clean, there are excess entries and records are not actively managed

3.29 There is no single database that can be used to verify or validate a person's identity when they apply for public sector services. Instead, the public sector has a number of databases with varying degrees of national coverage, each with a different data set and different sources of updates.

3.30 These databases have been developed for administrative purposes within individual departments or, occasionally, for shared use by departments. None of them has the prime purpose of identifying individuals although all of them may, to a greater or lesser degree, be used to do so. Entry to the databases is controlled by the processes used for issuing documents used as evidence of identity such as those described in Boxes 3.1 and 3.2 for passports and driving licences.

3.31 Three of the main databases – the Electoral Register and those maintained by the UKPS and the DVLA – are essentially elective. Entries on the databases are dependent on people applying for a service or registering their details, and so do not cover the whole of the population.

3.32 By contrast, the NHS Central Register (NHSCR) and DWP Departmental Central Index (DCI) databases come closer to covering the entire resident population. In the case of NHSCR only people who move to England, Scotland or Wales after they are born and who never register with a NHS GP will be missing. The DCI, which includes all allocated NINOs, is missing those people for whom no Child Benefit was claimed when they were children and who subsequently have neither claimed benefit or worked, or have only worked in the "shadow" economy.

3.33 In the absence of a UK population register, increasing use is being made of private sector data sources, such as those provided by credit reference agencies. These are often based, in part at least, on publicly available data sources; the mode of operation with data from the various regional electoral register databases is for the agency to purchase the individual databases for a nominal fee, collate the data and sell it as a single database. This data is also supplemented by commercial data about individuals.

'Excess' records

3.34 All the databases researched suffer from a common perceived problem in that the number of records held show some excess over the expected population. There are several reasons for this.

3.35 Records are held for people who are deceased. This may be because a database has no automated link to GRO. Even where a link exists – or where, as with DCI, GRO(E&W) sends weekly death notifications to a database – it will not present a completely accurate picture because the GRO(E&W) database does not include details of all deaths that occur abroad, and because in some cases the informant notifying deaths to GRO(E&W) may not be able to accurately give the name or date of birth of

the deceased. And in some instances, such as National Insurance records, there is a valid business reason for holding records for deceased persons (to facilitate payment of benefits based on inherited entitlements).

3.36 Records are held for persons living abroad. These may be UK citizens who have left the country permanently or for lengthy periods or foreign nationals who have lived and worked in the UK long enough to have developed a presence on a number of government databases but have now returned to their country of origin. This is an issue for all databases as there are no official records covering emigration, but some are impacted more than others. For example, Electoral Registers are 'self policing' to a certain extent because they are compiled annually. Even without notifying anyone of movement abroad, the fact that someone is not present to register at a given address will usually result in removal from the register. On the other hand, a National Insurance record will remain permanently on DCI irrespective of residence in the UK.

3.37 Human and system error will cause all databases to hold duplicate records. Individuals may or may not notify changes of name, marriage, divorce etc. For example the DVLA database has problems with female drivers who obtain a provisional licence, do not pass their test, marry and then obtain another provisional licence without informing DVLA that one had already been obtained. In all databases, even where no change of name has happened, duplicates are created by misspellings, data input errors, etc. And where tracing routines fail to identify an existing account a duplicate will be raised.

3.38 Some 'duplicate' accounts will be raised as a result of deliberate fraud – where an individual invents a new identity in order to obtain benefits or services to which they are not entitled. For example, a disqualified driver may create a false identity and sit a further driving test in order to obtain a licence that they are not entitled to hold. But the problems naturally attendant on developing and maintaining databases mean that by far the largest proportion of duplicates will be caused by error not fraud.

3.39 Some of these problems may be alleviated when the GRO(E&W) establishes its centralised database of births, marriages and deaths in England & Wales – the subject of a recent consultation exercise – but it is unlikely that this will be a total panacea.

The extent to which records are 'actively' managed

3.40 Records and accounts can be actively managed by:

- investing resources in cleansing data. This can take the form of routine management to identify and delete obviously inaccurate records or by more sophisticated routines such as matching data across systems to correct errors and remove duplicates;
- use of risk management and data mining techniques to identify anomalies, correct errors and pursue fraud;
- encouraging individuals to "police" their own records.

3.41 Some active account management by government exists, but it would be possible to undertake more. For example, an entry on the DVLA database is automatically valid until an individual reaches the age of 70. This does not cause any problems from the perspective of the core business of validating an individual's right to drive, but it may increase problems and complexities on the system, creating potential difficulties from an identity perspective. Currently databases are managed to meet the specific business needs of each organisation within resource constraints.

3.42 On the whole, data protection requirements and IT architecture constraints prevent automatic cross-referencing between databases. So it is difficult to access government data to confirm identity by reference to other data sources. And it is easy for databases to become misaligned with each other when an individual tells one department about a change of circumstance but not another. Cross-referencing does happen in some tightly defined circumstances – for example DWP and Inland Revenue exchange some change of circumstance information and check NINOs between systems. But there is no general power to cross-reference in order to confirm an individual's history.

3.43 As to "policing" of records by individuals, data protection legislation gives people the right to access to government records and thus an opportunity to check their accuracy. But in practice this is difficult to achieve:

- individuals may not be aware of the existence of any given database;
- they may not understand their rights to access or know how to engage with the organisation which manages the database;
- even when provided with the information it may not be in a form that they can readily understand;
- there is often little incentive for them to ensure that the data is accurate.

3.44 Identity issues may create a need for more active management above and beyond the strict core business requirements of any one IT system.

So both databases and process could be made more secure – but at some cost

3.45 There are a number of ways in which processes for the issue of government documents that are used as evidence of identity could be tightened. These range from improving the security of existing processes – as has been done for the issue of NINOs with SNAP – through improved risk profiling, to more fundamental changes in processes. These could involve more checking of applications for documents against "biographical" databases and/or checking against central registers of reported frauds and fraudsters.

3.46 And databases, like processes, could be made more secure. Part Two of this study sets out the pros and cons of taking action to improve the processes for issuing documents used for identity and quality and accuracy of databases.

3.47 A further important aspect of the current position, however, is counter-fraud activity. This is surveyed in Chapter 4.

CHAPTER 4: COUNTER-FRAUD ACTIVITY

Summary

4.1 The present chapter looks at counter-fraud activity in government. It concludes that:

- a wide range of bodies is involved in the detection and prosecution of identity fraud and theft, normally as part of a wider counter-fraud strategy;
- there is already joint working between those involved in counter-fraud activity, though this is variable in its impact;
- areas worth considering for further work would include more effective joint working, more sharing of data and intelligence and more active and effective prosecution policies.

A wide range of government and private sector organisations is engaged in the fight against identity fraud

4.2 Identity fraud touches many organisations, including most central and local government organisations. These organisations range in size from single figures to thousands of staff nationally. The nature of counter-fraud efforts accordingly varies from large-scale professional investigative organisations to small groups meeting informally to exchange local information.

4.3 The level of resourcing and the profile of counter-fraud activity depends on the size of the affected organisation and on the nature of the service provided:

- within DWP the Benefit Fraud Investigation Service (BFIS) has around 5,000 staff dealing primarily with frauds surrounding false declarations to obtain benefits to which the individual has no entitlement, i.e. working whilst in receipt of benefit and failure to declare a “living together situation”. Identity fraud, however, is not generally a feature in BFIS investigations and is usually dealt with by the (much smaller) Benefit Agency Security Investigation Service (BASIS), whose staff of 280 concentrate on organised criminal attacks on the benefits system;
- HM Customs and Excise have a counter-fraud force of around 7,000 who deal with the illegal importation of drugs, alcohol and tobacco as well as policing the VAT system. Inland Revenue also employ significant numbers of counter-fraud staff.

A number of factors are reinforcing government’s action to counter fraud

4.4 Government action to counter fraud is currently being reinforced by a number of new initiatives, including:

- **a new emphasis on prevention as well as cure.** Counter-fraud activity for most organisations today forms only one part of a wider overarching strategy which seeks to improve the overall level of accuracy in service delivery. Counter-fraud measures are not seen as add-on security processes; rather security must form an integral part of processes at the design stage. So whilst many departments and organisations have

dedicated counter-fraud staff, the responsibility for countering fraud lies with every member of staff. Many departments are also seeking a total quality approach to their work, incorporating counter fraud strategies into the management of their processes;

- **the development of a more professional cadre of counter-fraud staff.** A more professional approach is now being encouraged and many counter-fraud staff and managers have already gained, or are gaining, Professionalism in Security (PinS) accreditation from an external body;
- **a greater focus on good quality analysis and intelligence.** A number of departments are developing their intelligence and analytical capability and increasing focus is being placed on the value of high quality intelligence and analysis. Increasingly this will be used to support the development of policy as well as to support investigative operations. There is also evidence of the recognition of the need for intelligence, analysis and data to be shared, although sharing both intelligence and data can be very difficult in some areas.

Co-operation between departments is effective but could be further improved

4.5 For many years government departments and local authorities have actively, if sometimes informally, co-operated to discuss intelligence and operational matters, to share best practice and at a higher level to determine policy. Groups may be local, regional or national and officials are increasingly meeting international colleagues too. Co-operation is based on the certain belief that fraud of any kind exhibits balloon-like properties, in that when one part of the problem is successfully squeezed by counter-fraud effort, it will expand into a new area.

4.6 This co-operation between government departments in some cases has been formalised into full joint-working with the establishment of cross-departmental teams.

4.7 But there are some current barriers to further increases in co-operation:

- the benefits of counter-fraud activity in one department often only accrue to another department. Conversely, a lack of rigorous procedures in one department may have an adverse effect on another;
- the structure of government and of individual departments, each being responsible for its own policy, structure and reporting mechanisms, also makes the setting of policy objectives, goals and targets for cross-boundary counter-fraud activity difficult. Each party must know what it hopes to achieve before agreeing with others what the common policy objectives should be;
- there is a lack of agreed mechanisms for measuring performance. This is often fraught with difficulty because the needs of individual organisations must be subordinate to the collective needs of all the partners. A balance has to be struck to enable each organisation to be satisfied that they are meeting their policy objectives and are gaining from the deployment of their resources.

Data sharing and data matching could be further exploited

4.8 Data sharing is widely used in the private sector in its efforts both to prevent and to detect fraud, including identity fraud. Details are in Chapter 5. In the public sector too, data sharing can be a useful tool in the detection and investigation of crime. Some departments such as DWP and IR have made specific legal provision for data sharing with other departments. In IR's case this is of long standing and covers many but by no means all government departments.

4.9 More data sharing within government could be a significant step to minimising fraud through the early prevention and detection of fraud. But many barriers to increased data-sharing exist, ranging from the reluctance of individuals or departments to share or exchange data, to legal prohibitions. The interpretation of the Data Protection Act is not always straightforward and some departments do not have sufficient clarity around their own data protection policies, so staff can be unsure of their position and consequently take the least risky option. These issues are further discussed in the PIU report on Privacy and Data Sharing.

A more robust prosecution policy could bring more of those responsible for identity frauds to justice

4.10 A further inhibitor on effective counter-fraud work is a lack of consistent prosecution policies and practices, and an apparent lack of enthusiasm for prosecuting identity fraudsters. Some departments, such as DWP, HMC&E and IR, have their own lawyers and take their own proceedings in Magistrates' Courts or institute proceedings using the Theft Act and other Acts in co-operation with the police. Others, including DVLA and UKPS, rely on the police and the Crown Prosecution Service to take proceedings on their behalf. Some of the difficulties in prosecuting passport fraud are set out in Box 4.1.

4.11 The penalties imposed for cases of attempted identity fraud vary greatly in their severity. In the case of a fraudulent passport application a charge is usually brought under the Theft Act, for a deception to the value of £28.50 (the cost of a passport). The Act carries a maximum penalty of up to 7 years imprisonment but, whilst some courts hand out custodial sentences of 2 to 5 years, many will merely issue suspended sentences or conditional discharges.

4.12 In cases of large scale passport fraud, UKPS will attempt to prosecute with the more serious charge of conspiracy, rather than deception, but such attempts are not always successful.

4.13 The case for making changes to the present law will be considered in Part Two. Chapters 5 and 6, meanwhile, discuss the lessons to be learned from the private sector and from overseas.

Box 4.1 Difficulties in Prosecuting Passport Fraud

The take up of prosecution cases for passport fraud is not uniform. This is particularly noticeable in some of the Regional Passport Offices which have large catchment areas covering a number of different police forces.

Where a fraudster is identified at a public counter, the police and the CPS will usually prosecute (or, with the agreement of UKPS, pass the individual to the Immigration Service for processing as an illegal immigrant). In such cases, UKPS staff will have done all the work necessary to establish that the applicant is attempting to obtain a passport in a false identity.

There is less success where the individual is not present. There can be some delay in the papers reaching the local police station and by the time they visit the address the fraudster may have moved on; or it is a ‘drop off’ address; or the occupants deny all knowledge of an individual in the fictitious identity.

Furthermore, anecdotal evidence suggests that some magistrates are not prepared to convict in a false identity. This is demoralising for enforcement staff who spend time gathering the necessary intelligence and evidence to send cases forward. It also means there is little deterrent effect to potential fraudsters who are unlikely to face prosecution.

CHAPTER 5: LESSONS FROM THE PRIVATE SECTOR

Summary

5.1 Within the private sector there are a number of processes in place to validate and verify the identity of an individual seeking financial services, including banking facilities. In some cases, this is to comply with government regulations to prevent money laundering. In others, it reflects the commercial interests of private sector bodies.

5.2 Private sector methods for establishing identity focus less on checking of documents (although a partial exception is the checks required to satisfy money laundering regulations, and some checks made for lower-risk financial products). Rather, the private sector checks identity against a range of databases. This is partly for reasons of cost and partly because the private sector does not feel able to rely on government-issued documents, but also because there is public demand for increasingly fast and trouble-free processes. The range of data sources includes the following:

- data held by credit reference agencies which can establish, with a fair degree of certainty (and on-line in real time if necessary), the credit-worthiness of individuals but also the extent to which they have a well-established "biographical" identity;
- a central register of identified frauds (CIFAS) which can help weed out further fraudulent applications for credit or other goods and services;
- IT systems which can cross-check details on an application for financial products for consistency against either the data held on a company's own systems or against a national database.

Money Laundering Regulations

5.3 The extent of identity fraud to facilitate money laundering is not known since the essence of money laundering is concealment (though statistics on referrals to the Financial Services Authority (FSA) are set out above in Box 2.1) Concealment is equally possible with a false business identity as with a false individual identity.

5.4 In addition to the natural wish of financial sector organisations to maintain integrity in processing transactions, they are also required to comply with the Money Laundering Regulations 1993.

5.5 The Joint Money Laundering Steering Group (JMLSG), an industry body, has issued guidance notes to help organisations across the financial services sector with the interpretation of the Money Laundering Regulations. The guidance includes procedures for obtaining sufficient evidence in respect of any person or company wishing to transact or form a business relationship with a financial services organisation. The requirement in all cases is to obtain satisfactory evidence that a person of that name lives at the address given and that the applicant is that person, or that the company has identifiable owners and that its representatives can be located at the address provided. The guidance notes are not legally binding, however.

The guidance advises that assessments should be risk-based rather than prescriptive, and can be satisfied by a check against a credit reference agency database and a CIFAS database check.

5.6 The FSA checks to ensure all financial organisations have adequate systems and processes in place. It offers guidance on systems and controls. The FSA has access to banks' records to check that they are complying with guidelines and legislation. It can require banks to put in a plan of remedial action if a fault is found, and under the Financial Services and Markets Act is able to take disciplinary action (including prosecution) against those who do not adhere to the legislative requirements.

5.7 With the growing use of electronic, postal and telephone banking, financial organisations have increasingly less face-to-face interaction with their customers and less opportunity to scrutinise their identity. Banks have in the past – to follow earlier versions of the JMLSG guidance – tended to use the '2+2 rule', whereby identity is proved by providing two documents providing evidence of a person's name, and two with their address. This system is easily overcome with false documentation, however, and the JMLSG guidance now advises against its use.

CIFAS – the UK's Fraud Prevention Service

5.8 CIFAS is a database of fraud and attempted fraud to which a number of private sector organisations contribute. It was established in 1988. Its founder members in the retail credit industry were joined firstly by finance and leasing organisations, then banks and credit cards, followed by building societies, insurance companies, telecommunications companies and mortgage lenders. Its membership totals around 240 organisations.

5.9 Members of CIFAS are required to operate effective in-house procedures to enable fraud or attempted fraud to be identified. Cases are classified into different categories, including "False Identity Fraud" and "Victim of Impersonation".

5.10 When a member receives a customer application it checks the address against the CIFAS database to see if it is flagged. If there is a flag, details of the relevant CIFAS category and details of the member who instigated the original entry will be given. It is then the responsibility of the second member to contact the first member and request details of the case. The second member must then assess the application in the light of the information received and either notify CIFAS of a further attempt to commit fraud, or if the application is not fraudulent to proceed with their normal account opening process.

5.11 CIFAS also offers a "Protective Registration" service to people who have had their identity documents stolen or are otherwise concerned that they may have been the victim of identity theft. This allows them, for a small fee, to flag their own address on the CIFAS database. There are processes in place to ensure the person reporting the theft is the true owner by crime reference numbers or sending a confirmation form to the address on file.

Consignia is currently co-operating with CIFAS to combat fraud and particularly identity theft by making mail redirection data available to CIFAS members, in a case by case basis, for use in fraud investigations.

5.12 CIFAS' figures measure incidents of fraud, rather than the number of people committing fraud. They recorded a 462% increase in the number of cases of false identity fraud between 1999 and 2000 (2,189 to 12,310) and a further 122% increase in 2001 (27,279 cases). In addition they recorded 26,000 cases of impersonation in 2001. Some of the increase in 2000 is due to the combined effects of a change of system of classifying reported frauds and an increase in the number of members, but it is clear that identity fraud is rising. CIFAS believes that about a third of its members' losses are written off as customers going missing (eg to avoid bad debts), but much of this could be down to identity fraud.

Credit Reference Agency Databases

5.13 Experian and Equifax are the two largest credit reference agencies in the UK, holding data on over 40 million people spanning several years. They act as trusted third parties for private sector organisations in their relations with their customers.

Box 5.1 Credit Reference Agency Information and Methods of Working

Credit reference agencies were created to enable lenders to make swift decisions about the risk of advancing credit to applicants. Lenders pooled their lending experiences so that people who had shown themselves to be good financial risks could benefit from obtaining further services without the delay imposed by further checks. Credit reference agencies provide information, decision making support and application processing services to many companies around the world, protecting not only against financial loss but also money laundering and impersonation. They provide a means of checking whether an individual exists, through the presence, or otherwise, of a consistent financial record. The absence of any records, or lack of consistency of such records, does not mean the identity is false; any negative matches are referred for future checks. In other words, they can say an identity is real, but they cannot say it is false.

Basic data from electoral registers and the Postal Address File is overlaid with information about bankruptcy cases and county court judgements and, crucially, existing credit agreements, so covering the vast majority of the population (as even socially disadvantaged communities tend to have mobile phones and hire purchase agreements). Data is constantly being recorded so the company is increasingly able to provide substantive past histories (e.g. jobs, mortgages, addresses).

Both Experian and Equifax are audited regularly and operate on high security, regularly liaising with the Office of the Information Commissioner on data protection issues.

5.14 Whilst the public sector holds ‘womb to tomb’ information, the majority of information held by credit reference agencies relates to transactions in mature life. People who for whatever reason do not have any credit or mortgages, and are not on the electoral register, are not well catered for (although information such as postal addresses and telephone numbers provide some detail).

5.15 The level of scrutiny applied by lenders is based on a sliding scale of risk assessment. Lenders will consider the “score” attributed by the credit reference agency, and interpret it in the light of their own risk policies in deciding whether or not to proceed with the transaction. A number of factors are considered, including the desirability of the product, for example an application for a credit card would attract less scrutiny than an application for a mortgage. One high street retailer assumes that 85% of applications for credit will not have a problem, so a threshold is set that will weed out and allow them to concentrate on the remaining 15%. Such a threshold might be that 4 consistent records going back 6 years would be sufficient not to attract further checks.

IT systems can be used to check data for consistency

5.16 IT systems, such as the widely used Hunter system, can be used to check data for consistency. Box 5.2 describes the Hunter system. But it is not unique; other systems, such as Experian’s “Detect” product, offer a similar data cross-checking service.

Box 5.2 “Hunter” IT Systems

Local Hunter is an IT system used within organisations to check applications for mortgages, current accounts, savings accounts, personal loans, motor finance, credit cards, insurance claims, insurance policies, student loans and places at universities. It is installed at over 70 sites in the UK, including UCAS and the Student Loans Company. The system looks for inconsistencies between applications and existing information already held by the organisation – applications are checked against themselves, any previous claims or applications, suspect information and other known fraudulent data. Where the organisation is a member of CIFAS, the CIFAS databases are also checked.

National Hunter, developed in 1993, is a broader system which enables members to cross-check application data between themselves. National Hunter was originally set up to cross-check mortgage applications between different mortgage lenders, but has since expanded to cover credit cards and accounts, motor finance and personal loans. Any inconsistencies or oddities between application data supplied are flagged for follow-up. As the system operates in batch mode, it is best suited to the processing of applications where speed is not of the essence. Similar Hunter systems are run for the creditor insurance industry (Register of Claims) and general insurance (Insurance Hunter).

5.17 Such systems differ from CIFAS in that they offer a cross-matching facility of information (eg multiple claims, same telephone number quoted but for different addresses, different salary level quoted) across different address on the system, whereas CIFAS is currently a list of names where fraud has been identified (although in July 2003 it will become a sophisticated cross-referenced database of frauds).

Conclusions

5.18 Even with the anti-fraud measures in place in the private sector, the project team's research indicated that over £680m of fraudulent transactions are committed each year. There are a number of reasons for this:

- the rewards of organised crime are significant and give strong incentives to commit identity fraud. The fight against identity fraud is an ongoing struggle. Even the most radical measures are unlikely to lead to the total defeat of the fraudster;
- although there is increasing agreement in many sectors that "fraud is not a competitive issue", there are others, notably where new products and markets are being rapidly developed, where commercial incentives lead businesses to accept high levels of fraud as they increase market share. For example, the development of internet banking may have led to higher levels of fraud;
- companies are conscious of the balance to be struck between inconveniencing or annoying good customers by seeking proof of identity and carrying out anti-fraud checks.

5.19 That said, there is little doubt that the counter-fraud measures in place in the private sector do significantly raise the hurdles over which the identity fraudster must jump – and that there is much the public sector can learn from best practice in the private sector.

CHAPTER 6: LESSONS FROM OVERSEAS

Summary

6.1 This chapter summarises the results of research on the extent and nature of identity fraud – and action to counter identity fraud – overseas.

6.2 The main conclusions are that:

- all countries experience the same difficulty in establishing the extent and nature of the problem;
- the USA is particularly worthy of note in that it has a de facto – but not an official – identity card in the Social Security/driving licence card, and is by far the most advanced country both in its experience of and its attempts to deal with identity fraud. Identity fraud in the USA is rife;
- some EU countries are introducing electronic networks to act as 'virtual' databases to control data protection rules for interchange of information between government bodies. This is to improve the quality of government data and combat fraud. Although their remit is wider than identity fraud specifically, such systems are considered to have the potential to improve identity fraud problems by improving data quality overall;
- there appears to be a problem common to many EU countries of identity fraud being used to assist in trafficking of people into the EU and illegal immigration more widely. The Netherlands and Republic of Ireland use similar tactics to the UK to detect identity fraud; setting up specialised units to check for counterfeits and false documentation and using a system of interviews to verify whether an individual's history and documentation match.

USA

6.3 The USA has a major problem with identity fraud and identity theft amongst its 285 million citizens. In a survey in June 2000, 44% of respondents had been victims of identity theft. In the fiscal year 2001, the Social Security Administration's Office of the Inspector General received over 115,000 allegations of which over 65,000 (57%) involved misuse of Social Security Numbers (SSNs) and/or identity fraud. A detailed report by the US General Accounting Office in 1998 could reach no comprehensive conclusions about either the prevalence or the cost of identity fraud, but it is generally recognised that the phenomenon has grown exponentially in recent years and will continue to grow with increased use of electronic commerce.

6.4 The USA recognises that the problem is largely due to function creep of the SSN, which is now used almost universally from mortgage application forms to military and student identification numbers. Its universality has become its own worst enemy, in that its power (to engage in financial transactions, to obtain personal information, to create or commandeer identities) makes it a valuable asset and one that is subject to limitless abuse. The Social Security card/driving licence often features as a de facto identity card, not least in frequent checks for under-age drinking.

6.5 Fraudulent SSNs are usually obtained by presenting fraudulent identity documents to the issuing offices. The processes for ensuring that SSNs are only issued to genuine claimants are relatively weak. There is no system of countersignatures. False SSNs are also fairly widely available for sale on the internet.

6.6 The US Identity Theft Act, passed in 1998, made identity theft a criminal offence, established a federal complaint and consumer education service for victims of theft (the Fraud Hotline) and gave more teeth to the Federal Trade Commission to fight identity theft. Forty-nine States also have their own laws on identity theft.

Canada

6.7 Canada shares some of the characteristics of the USA so far as identity fraud is concerned. Its 31 million citizens carry no identity cards as such, but the Social Insurance Number (SIN) card is ubiquitous and subject to function-creep. No data on identity fraud in the economy as a whole is available. Most identity fraud involves acquisition of a SIN to defraud benefits services or gain credit. In 1998 Human Resource Development Canada (the Canadian equivalent of DWP) carried out a review of identity fraud in its programmes. The review was unable to accurately assess losses to society resulting from identity fraud, but resulted in significant improvement of HRDC programmes and systems. The review was focused on ensuring that benefits staff are able to check identity documents of those claiming benefits (i.e. not on the wider economy). Following the review, the Auditor General and the Canadian Parliament sanctioned a publicity campaign to raise awareness amongst the public, employers, HRDC employees, victims of identity theft and the police of the problem of SIN theft and ways to minimise it. The main message was that the SIN card should not be used as an identity document. Other results from the review included:

- increased sharing of information about identity fraud with other administrators in Canada and overseas;
- large-scale training programme for HRDC staff and introduction of new fraud detection tools eg UV scanners;
- creation of an Identification/Fraudulent Document Guide for staff;
- consideration of development of a case management process to link possible repeated fraud activities.

6.8 The legal framework makes it illegal to apply for a second SIN, or to use a SIN to defraud or deceive. There are 18 legislated uses of the SIN, and people are encouraged to avoid using it for any other purpose.

6.9 The Proof-of-Identity programme requires people wanting a SIN to provide a primary document and a supporting document. If either of these is not in English or French, it must be accompanied by an official sworn translation. As in the USA, there are many different types of a single document, eg birth certificate, as they are issued by State/territory and not federally. Recent training for HRDC staff has improved the processes for checking these.

The Netherlands

6.10 The Netherlands has no unique identifier for its 16 million citizens, probably because of a widespread antipathy towards identity cards resulting from historical resonance from World War II occupation. But it does have well-developed systems for keeping track of stolen and lost documents: the Verification of Identity System (VIS).

6.11 The VIS system is operated by the Dutch Police. Details of around six million documents are held on the central database. Details are recorded for identity documents (mostly driving licences and passports) which have been reported lost or stolen. Whilst the majority of documents recorded are Dutch, details of documents issued in other countries are also held. Details of deaths are also held in case someone tries to assume the identity of a deceased person. The database can also be used to validate some of the data recorded on a document. This includes validating the “country code” and the number of digits used on a passport.

6.12 Public and private sector organisations can use the database: there are around 2,500 terminals used to access the database nation-wide. Around three million checks to validate documents are made annually. During 2000 there were 16,115 matches against the database i.e. details of a document presented to prove identity was held on the central database indicating that it had been reported lost or stolen or the person was deceased.

6.13 The Netherlands have specific offences in the area of identity. Forging any identity documents (wherever issued) including, for example, a driving licence could attract a 5-year sentence. There is a separate offence of using someone else’s identity.

6.14 The Netherlands authorities take social security fraud very seriously and in the last five years or so have increased their counter-fraud activities markedly. One anti-fraud unit has recently undertaken a project investigating identity fraud. The project concentrated on improving the ability of staff to recognise forged and tampered documentation. (An example of how simple information can combat fraud is that they regularly come across forged UK Identity Cards supplied by persons purporting to be UK citizens, who have bought them not realising that the UK does not issue identity cards.) Officials now use UV scanners to check documents, the VIS system to check for stolen document use and a system of interviews to check a given story against the documentary evidence.

6.15 Foreign nationals have to register and provide documentary evidence of identity to gain permission to remain in the Netherlands, work or claim benefits.

6.16 There are also strictly controlled circumstances under which a person can change his or her name. Anyone can change his or her forename(s) by deposition in front of judge (a charge is levied per letter of name changed). Family names can only be changed if there is a ‘reason’ for doing so such as psychological damage or a desire to take a name that is about to die off.

6.17 The Netherlands have also introduced an electronic exchange of information routing system to combat fraud and inefficiency. At present it only covers electronic data traffic within the Netherlands, but in the future links are planned with other countries. It holds information that allows it to identify whether data protection considerations permit transmission of requested information between given databases. It does not hold any data itself, but merely acts as a virtual link between the party requesting data and the party supplying the data, looking after proper routing, comprehensible software, standardisation, data integrity/security, data protection and privacy considerations. The system allows convenient transmission of information between organisations covering employment, Social Insurance (pensions, child benefits) Tax, Home Office and the Ministry of Justice, so that changes of circumstance reported to one government body are passed to all appropriate interested bodies. This is perceived as a significant advantage for citizens as it reduces the burden of red tape. The system is not specifically aimed at countering identity fraud, but as it will improve the quality of government data overall should increase data security.

6.18 The Dutch also use risk management techniques, data mining, risk rules etc to check for benefit fraud – which frequently has an identity component. For example they identified the fact that specific nationalities claiming child benefits for twins represented a risk factor and found that running risk rules against their databases produced a fruitful source of referrals.

Belgium

6.19 In addition to carrying compulsory identity cards, all 10 million Belgian citizens must notify their address to the police, who then visit the house to check actual residence. An individual without a registered address is not able to access government services. Belgians also have a ‘SIS’ card for social security purposes which has a small data storage capacity but no cryptographic functions, and is used for identification at hospitals, pharmacies etc.

6.20 Over the next 18 months new identity cards will be issued in Belgium. These, like the older cards, will include a photograph but will also have a chip and digital signature to facilitate e-business with government. These cards will include social security and driver’s licence information. There is no perception that the new card will be particularly costly as the ‘secure’ identity cards that will be replaced are expensive to produce and the administrative infrastructure to support them is already in place.

6.21 Belgium is developing a ‘Crossroads Bank’, which performs broadly the same functions as the Dutch data routing system. This acts as a central clearing house between secure email addresses, and holds information that allows it to identify whether data protection considerations permit transmission of requested information between given databases. The intention is to develop this system to allow convenient transmission of information across government.

Finland

6.22 Although identity cards ("FINEID" cards) are voluntary, they are widely used amongst the Finnish population of 5 million. Newer versions can (at the holder's request) have electronic chips and can be used for public key cryptography. Take-up of the smart card option has, however, been low.

6.23 A unique identity number is used as a key for all government information about individuals (including social security, health services and even banks). The entire population and all buildings are registered with the Population Register Centre, whose database is used by government departments to avoid repeated requests for information and for verification of information. The register is also used by private sector companies, eg to ensure the accuracy of their mailing lists (individuals can opt out of this use).

6.24 There is a much greater acceptance of the use by government of personal data, especially where the citizen benefits by not having to reproduce information. For example, the 1990 census was conducted simply by collating information from various databases using the unique identity number, without any involvement by individual citizens at all. Banks and employers also provide taxation authorities with electronic information about individuals, which allows the authorities to compile tax returns automatically as "proposals". Taxpayers can either accept or amend the proposal (around two thirds accept the proposals unchanged).

Denmark

6.25 All 5 million Danish citizens have a unique personal identity number linked to a centralised civil registration system which holds data about name, address, marital status (including spouse), place of birth, citizenship, kinship (parents/children), declaration of incapacity, profession, membership of the Lutheran Church of Denmark, voting rights, municipal circumstances, registration notes and death. This system was introduced in 1968. The personal identity number is used by almost the entire public administration system including tax authorities, as well as banks and insurers (who have restricted access).

6.26 Citizens are legally obliged to inform the government eg when they move house. A single change is then made to the database and this data is then made available to all relevant public authorities. Between 1968 and 1995 individuals were also issued with a card bearing their name, identity number, date of birth, address and date of birth (but no photo). This was stopped as it was thought to be ineffective and expensive.

Republic of Ireland

6.27 Increasing levels of immigration to Ireland over the last 10 years has led to an increase in identity fraud, illegal employment and fraudulent benefit claims.

6.28 The Irish Department of Social, Community and Family Affairs have introduced changes to combat these problems (following assistance from the UK) including:

- increasing training and awareness of the problems with front line staff;
- staff interviewing claimants to try to verify their stories. Even simple things like asking claimants to complete application forms in the language claimed as their native tongue, or asking them about the geography of where they came from, have had results in identifying false applications;
- setting up a small document verification unit to check for forged documents, record information and check national and international trends.

6.29 Ireland has also signed a Memorandum of Understanding with the UK, aimed at improving exchange of data, as permitted under the respective national law of the participants, co-operation and assistance in administering national legislation and the provision of assistance with specific investigations and enquiries.

France

6.30 No national figures are available for identity fraud in France. It operates a system of identity cards for its 60 million citizens. Although these are not compulsory, formal proof of identity (such as a passport) must be presented to a senior law enforcement officer on request as part of an identity check. Identity cards are issued for 10 year periods, but even after expiry can be used as proof of identity providing the photograph is recognisable. A new identity card system was introduced in 1987, and at the same time it was decided to tighten card issuing processes. Requests for replacement of old style cards were subject to the same controls as new applications, with particular attention given to scrutinising the validity of documentary evidence provided to verify identity.

6.31 There is no unique lifetime numbering system used for identity cards as replacement cards will bear a new number not associated with the previous one – although internal computer checks are used to seek to guard against the issue of fraudulent duplicates.

6.32 Legal constraints forbid the exchange of personal information between government departments and between public and private sector organisations – unless a judicial investigation is underway, in which case disclosure of information is mandatory.

Australia

6.33 Recognising in the late 1980s that identity fraud was on the increase, Australia planned to introduce a national identity card for its 19 million citizens. However, in the light of privacy concerns (that there were insufficient safeguards in place) and the realisation that most ordinary people were involved in minor tax evasion (e.g. by paying cleaners/car mechanics in cash), the Government decided against implementing the proposed scheme.

6.34 Australia still has a perceived problem with identity fraud, although in common with many other countries has not been able to quantify its extent financially – except to the extent that it is growing. For example, the New South Wales Registry of Births, Deaths and Marriages has concerns with increasing numbers of counterfeit birth certificates being used for fraudulent purposes and has sought to counter this by developing a Certificate Validation Service to allow a user organisation to check birth certificate details against the Registry's database via a secure Internet connection.

6.35 In the early 1990s, the federal government created the Parallel Data Matching programme in an attempt to prevent taxation and social security fraud. This system sought to identify individuals claiming benefits to which they were not entitled and also individuals who had not made claims to which they were entitled. In 1996–7 this was said to have resulted in savings of $AU 157 million against a cost of $AU 157 million.

6.36 Australia also has a perceived problem with Tax File Numbers (TFNs) issued by the Australian Tax Office. The ATO database is used by a wide range of other government departments. The ATO is investigating methods of improving the integrity of the TFN system by data matching to identify and remove duplicates and progressing strategies for archival of inactive records – although concerns have been expressed at the potential cost of this method as opposed to flagging records as inactive.

6.37 The use of the TFN in general and the data matching programme has attracted criticism from both the academic community and special interest groups concerned with personal liberty issues. Specific criticisms include:

- ***'function creep' of TFN –*** Critics argued that this ended up being de facto a general identification scheme – even after the abandonment of the Australia Card in the face of widespread public disapproval – and that this represents an attack on civil liberties and an invasion of privacy because the circumstances in which an individual must seek a number (gaining social benefits, obtaining various forms of tax relief) are such as to make possession of a TFN compulsory in practice;
- ***data matching –*** Concerns around the widening uses of the TFN have been exacerbated by worries about the parallel data matching programme. Here, criticism centred on perceived problems caused by poor quality of government data leading to high levels of mismatches and intrusive investigation of suspected fraud where data across government did not match accurately; and inaccurate cost benefit analysis, which failed to include all costs and benefits in particular the costs associated with handling referrals, those costs incurred by agencies supplying the data and costs of investigating/prosecuting criminal offences.

Other Countries

6.38 *New Zealand:* There is no unique identifier for New Zealand's 4 million citizens. Identity is proved by a two-step system of primary identification (including birth certificate/passport etc) and validating information. There is an awareness that identity fraud is a growing problem, but no work has

been done to quantify it. There is no relevant legislation. There are some data matching activities between departments but these are not aimed at the detection of identity fraudsters.

6.39 *Spain:* A compulsory identity card is issued by the local police to all Spanish nationals at the age of 14 (the overall population is 46 million). Cards, which are valid for 10 years, must be carried at all times and produced to the police on request. The card includes the holder's name, address, photograph, nationality, signature, place and date of birth, parent's names and a machine readable zone with optical character recognition text. The card is used as a travel document within Europe and is needed in dealings with the government and commerce.

6.40 *Germany:* All 82 million citizens are obliged to carry photo identity with them at all times, in addition to presenting a passport eg when claiming benefits or a driving licence when vehicle checks are made. Home addresses are also registered with local civic authorities.

PART TWO: APPROACHES TO SOLVING THE PROBLEM

CHAPTER 7: THE NEED FOR A STRATEGIC APPROACH

There are no simple answers to identity theft and fraud

7.1 There are no simple answers to countering identity theft and fraud, as Part One of this report has made clear. This is partly because there is a "mosaic" of documents currently used to validate identity and partly because fraudsters will always tend to attack the weakest links in the system – identity fraud is like a balloon that when squeezed at one point, expands in another.

7.2 Tightening up on the issue of passports, for example, is likely to lead to fraudsters paying more attention to photocard driving licences (or vice versa). And efforts such as the joint UKPS/DVLA project to tighten up on the issue of passports and driving licences, making it harder to procure genuine documents under false pretences, will lead fraudsters to concentrate more on theft of genuine documentation, counterfeiting, or identity takeover, where for example mail is redirected, details of an individual and their financial records are recorded, and theft is then committed through impersonation.

An overarching strategy to counter identity theft and fraud is required

7.3 So this report proposes an overarching strategy to counter identity theft and fraud:

- Chapter 8 sets out a range of options for securing the issue of documents used as evidence of identity, from tightening up existing procedures to adopting private sector methods of checking identity;
- Chapter 9 explores a range of options for countering the theft and counterfeiting of documents used as evidence of identity, and the use of genuine identity documents obtained under false pretences. These range from better checks against counterfeit documents to the introduction of biometrics on government documents;
- Chapter 10 looks at targetting offenders, through more joined-up action to detect identity fraudsters and more active prosecution of offenders. Options range from better use of existing liaison groups to the setting up of a Fraud Agency in government or a National Fraud Squad;
- Chapter 11 sets out the way forward.

7.4 The key elements of an overarching strategy to counter identity fraud are that:

- identity should be validated and verified on the basis of biographical checks for most applicants and checked against a register of known and suspected frauds – with those not passing such checks invited in for face-to-face interview;

- there should be a register of stolen identity documents available to both public and private sectors; simple anti-counterfeiting measures should be more widely adopted;
- there should be stronger and more joined-up action to counter identity fraud involving both public and private sectors, building on present liaison mechanisms.

7.4 Not all of the suggested ways forward will be equally applicable in all areas of the UK, particularly some of the options outlined in Chapter 10 around prosecution policy. Further consideration will be needed in implementing this report to ensure that the position in Scotland, Wales and Northern Ireland is properly covered.

CHAPTER 8: SECURING THE ISSUE OF IDENTITY

Summary

8.1 Many government agencies (including UKPS, DVLA, DWP and IR) issue documents which are later used as evidence of identity or numbers that serve as unique identifiers. This chapter sets out options for making the issue of such documents and identifiers more secure.

8.2 Some improvements could be made by simply tightening existing systems for issuing documents and unique identifiers. This could be done through increasing fraud awareness of issuing staff and making minor changes to procedures.

8.3 But given the nature of the basic processes, the gains from simply tightening those systems are limited. To increase security significantly would involve some or all of the following:

- supplementing existing systems with private sector-style checks against "biographical" evidence of identity from government or private sector databases (or both), making changes to the legal gateways for data-sharing where required. This would enable more identity fraudsters to be detected and would effectively offer a sophisticated way of risk profiling;
- greater use of face-to-face interviews for those not passing such "biographical" tests of identity, modelled on the DWP SNAP process;
- checking applications against a central register of known frauds and fraudsters – either a new government database or the existing private sector database (or both);
- more use of dedicated IT systems to check applications for internal consistency and consistency against other information held by government.

As described in Chapter 3 above, UKPS and DVLA are in the early stages of a joint programme aimed at tightening the issue of passports and driving licences.

8.4 Longer term options worth examining include:

- a register of people entering and leaving the UK against which applications can be checked;
- reducing the "mosaic" of identifiers by establishing a single entitlement card, subject to very secure issuing processes, that would combine the functions of the driving licence, the passport and the NINO.

It would be possible to tighten existing systems by improving staff training and increasing the rigorous scrutiny of applications

8.5 Existing processes for checking identity by those individual government agencies which issue documents used as evidence of identity or unique identifying numbers could be made more secure. This could be done by tightening up on staff training and increasing the number of applications subjected to rigorous scrutiny.

8.6 In Canada, following the realisation that identity fraud posed a significant problem, the Auditor General recently recommended that there needed to be a culture change amongst staff and the general population. Training courses including basic interviewing skills and false identity recognition are being developed for all staff involved in the Proof of Identity programme (i.e. all benefits staff) and UV lamps, magnifying glasses and microscopes are being provided to local offices. Box 8.1 sets out recent initiatives in DWP and UKPS.

Box 8.1 Initiatives to Increase Staff Awareness of Fraud

A number of initiatives to increase staff awareness of fraud were implemented in the last Parliament by the then Department for Social Security. In respect of Housing Benefit, which is administered by local authorities, a Verification Framework (VF) document was issued. The VF outlines the need to authenticate the identity of any person making or included in a claim, and how this should be done. DWP has also issued guidance to staff on the verification of identity and a public leaflet is also available “How to prove your identity for social security”. SNAP guidance has also been developed and issued to all staff involved in the NINO allocation process. Fraud awareness training is part of an ongoing process of initial and remedial training across the department.

In UKPS, all staff who examine passport applications receive basic training focused on identifying the extent of fraud, the problems and what to look out for. This is on the basis that potentially fraudulent applications will be referred to specialist fraud staff.

8.7 In the case of UKPA and DVLA, a further way to improve the security of document issue would be to check a greater percentage of countersignatories on passport and driving licence applications (as these are currently the basis of the link between checking that an individual exists and that the application is from the individual in question).

8.8 But the nature of current processes themselves precludes great security:

- the source documents required to apply for a passport or driving licence and to validate identity are not themselves highly secure – the birth certificate is simply a copy of a public record of a historic event and has no necessary link to the individual holder of the document. And there are particular problems with establishing the bona fides of overseas documentation;

- the reliance on a countersignatory to verify identity smacks of a bygone age in which local professionals who had lived in a neighbourhood for all their working lives could vouch for the bona fides of people with whom they had a long-term professional relationship. Furthermore, the countersignatory process has an exclusionary effect on people who do not come into contact with local professionals: in some areas people have no choice but to pay their GP £20 or so to countersign their application.

8.9 To make a step change in current security would involve a change of one or both of two kinds: greater use of face to face interviews for validation and verification, and/or greater use of checking against databases (government or private sector).

Face-to-face interviews offer greater security, but are time-consuming and expensive

8.10 Most processing systems are paper-based and applicants are rarely present. But face-to-face interviews allow officials to ask applicants probing questions about the information they have produced in support of their application, to scrutinise irregularities, and to check original documents and photographic evidence. The most secure process used for verifying identity is the DWP Secure NINO Allocation Process (SNAP), which works on this basis. But this comes at a cost, both in terms of resourcing the process and customer service levels (see Box 8.2).

Box 8.2 SNAP

The SNAP process shows the potential impact on customer service of introducing tighter processes. Although this is a national service the burden is not felt evenly across the country. Over 70% of all applications (300,000 p.a. as anticipated) fall to inner and outer London to handle, with concomitant pressures on staffing and accommodation. The main reason for this is that those coming from abroad to take up employment generally do so in the London area. Whilst in most parts of the country the new process has been introduced fairly easily, in some areas of London the waiting time for an appointment is some months.

There is also a significant financial cost: the cost of the new SNAP process is around twice that of the less secure processes previously used to check identity prior to issuing NINOs.

8.11 UKPS staff already operate a programme of interviewing customers if the application raises concerns about the applicant's identity. For people who apply in person at a Passport Office, concern is normally investigated in interviews by specialist fraud staff. In some cases applicants might be interviewed when they come to collect their passports. With postal applications (which comprise 90% of passport applications) where there

is concern, the applicant is invited to come into their local Passport Office, bringing with them further supporting documentary evidence. Fraudsters rarely turn up.

8.12 It would be possible to extend the use of face-to-face interviews. UKPS is considering a proposal that they interview all first time applicants, possibly using local agents. This is already done in the USA and to a more limited extent in Canada.

8.13 The cost of tightening up processes would potentially be significant but would obviously depend on the additional level of checking required. If costs or customer service considerations preclude face-to-face interviews for all those requiring passports or driving licences, it would be possible to extend the use of face-to-face interviews for groups with a high risk profile. That would, of course, depend on having suitable risk profiling arrangements in place.

Risk profiling could be extended through the wider use of "biographical" identity data to validate and verify identity

8.14 Risk profiling is already carried out in government. For example, UKPS have a programme of security audits and conduct a "lessons learned" exercise following any serious fraud cases. Both of these recommend improvements to their processes.

8.15 But more effective way of risk profiling applications for passports, driving licences, and numbers that serve as unique identifiers would be based on "biographical" rather than "attributed" aspects of identity. At its simplest, this means checking someone's identity against historical information held on databases (whether government or private sector) rather than asking to see their birth certificate/seeking a countersignatory to establish who they are. This essentially checks a person's "historical footprint" on the world.

8.16 Some such checking against databases is already undertaken in government, as reported in Chapter 3. But a significant increase in biographical checking would give potentially the biggest overall increase in security.

8.17 This methodology is tried and tested by the private sector, where any organisation wishing to give credit relies on the ability of credit reference agencies to draw together information from different sources to authenticate a customer's identity and develop a measure of their credit-worthiness (see Chapter 5 above).

8.18 It is presence on historical databases that is the hardest test to pass for those wanting legitimately to develop false identities i.e. officials working undercover. By the same token, biographical checking is potentially the surest way to find those seeking to defraud the state or the private sector under false identities, or to establish a false identity for other purposes (such as illegal working, money-laundering or drug trafficking).

8.19 “Traditional” straightforward credit scoring processes have become ever swifter and more user-friendly in recent years, and both the main credit reference agencies offer products which allow on-line identity authentication in real time. These systems are particularly suited to the electronic delivery of government services, where neither face-to-face interaction, nor the scrutiny of documentation submitted by post, is possible. In addition, historical information can be used for technologically advanced and novel authentication procedures. For example, Equifax has developed an “e-ID verifier” authentication system, which uses information held on databases to generate a series of questions to which only the applicant should know the answers. It is already in use as the validation mechanism for people using UK Online Digital Certificates.

8.20 The Criminal Records Bureau (CRB) takes a largely biographical approach to identity authentication. The CRB uses a large range of data sources, including GRO(E&W), GRO(S), DWP, DVLA, the Electoral Roll and Experian, and also hope to establish data-sharing links with GRO Northern Ireland and the BBC TV Licensing Unit. The Bureau compares the data that applicants provide in their CRB application with data held by these sources. This is done electronically, and some of the checks are performed on-line, whilst the customer is making their application (the majority of applications are made via the telephone).

8.21 But increased biographical checking would come at a cost and would raise significant data-sharing issues. There would be a need for legislation to open new data-sharing gateways. There would also be a need to confirm that new proposals were compatible with the Human Rights Act and the Data Protection Act. Separate procedures would have to be available for checking the identity of people who had legitimately failed to develop a footprint, for example young people or those who had been living abroad. It would be important to rotate the type of information that was checked, as otherwise it may be possible for fraudsters to anticipate questions and authentication methods. And measures would have to be put in place to ensure that any biographical checking, especially if it involved responding to questions, was not easily beaten by those close to the genuine applicant, such as family members, who could find out the answers to questions.

8.22 To be successful, cross-checking between databases relies on the data being reasonably clean. Data held by credit reference agencies is subject to many complaints to the Information Commissioner (not all, of course, are upheld). Their basic identification checks are heavily reliant on Electoral Register information, which is itself insecure (though less so for historical records over many years). There are also perceived problems with a number of government databases, as recorded in Chapter 3 above. Data quickly gets out of date and departments generally need to routinely maintain and cleanse their databases to ensure the highest possible level of accuracy (the major credit reference agency databases are refreshed monthly and so are more accurate than most government databases). But the e-ID verifier tool – and other identity checks – do not work on the basis that databases are completely clean: the system operator can define the level of accuracy required (for example 3 out of 5 questions answered correctly).

Government could create its own database – or build on private sector databases

8.23 Government could create its own database for checking identity. This could be based on either existing public databases (for example the new Civil Registration system in England and Wales, or Electoral Roll plus phone book) or a full range of key government databases (including DWP DCI, UKPS and DVLA databases).

8.24 But it is likely to be expensive (and risky) for the government to develop a single database of its own, or a full range of databases, against which to validate and verify identity. Options are set out in Box 8.3.

Box 8.3 Assessment of a More General Government Database

Government currently holds an array of data about individuals, in a myriad of separate databases. Making this data available to all departments would allow a person's "historical footprint" to be easily checked.

There are two separate options worth considering. One involves creating a new, single "super database", the second involves using existing data in a "virtual database" revolving around a central "hub".

Either a super database or a hub would be more secure than a system based on documents. The fact that only government data was used would mean that it would be more relevant to government business than the sort of financial information that forms the basis of the private sector databases. With robust security protection the system would be suitable for on-line access, and possibly also telephone access.

For either option, legal changes would be required; there would be concerns over privacy which would need to be addressed; there would be technical and data-quality issues; and a very large investment would be required. As with any system, it would not be entirely foolproof: determined organised fraudsters could still, over time, build up identities with a history on the database.

A hub option would be more technically straightforward but nevertheless would be neither cheap nor simple. A range of personal identifying information from a range of government databases could be accessed through the hub, so there would be costs associated with setting up the hub itself as well as making changes to the source databases to allow automatic updating of the hub.

A variation of the database concept might be a rather more simple central Government database of names and addresses, which would provide a single locus for citizens' contact with government.

The options would not necessarily carry the same pros and cons as buying in data from the private sector. Equifax and Experian receive up to 250,000 updates to information held on their records daily (every time an application for credit is processed or a credit card bill paid); many government databases would be updated far less frequently (tax returns, for example, are filed annually). The Government would also be carrying the risk and the cost if it were to develop its own database rather than rely on, or latch onto, an existing product and facility.

8.25 A more practical option would be to exploit existing commercial databases – for government departments to pay to use the services of one or more credit reference agencies. This already happens in certain cases, for example Inland Revenue, Jobcentre Plus and the Department of Environment, Food and Rural Affairs all use either Experian or Equifax or both. UKPS has just awarded Equifax with the contract that will allow UKPS to check passport applications using Equifax systems and data.

8.26 This option would enable government agencies to improve risk profiling – essentially to "tick through" perhaps 95% of applications for passports, driving licences or unique identifiers and concentrate on validating the identity of other applicants through more thorough methods such as face-to-face interviews.

8.27 The new UKPS contract with Equifax follows a pilot whereby passport applicants gave "informed consent" for UKPS to compare their information with that held by other organisations. One of the issues explored during the pilot was the number of customers who gave consent (which turned out to be almost everyone). Another issue is cost: use of credit reference agencies carries a cost which has to be covered by the passport fee.

8.28 A system of biographical checking would build on the tried-and-tested databases already in use, and would be able to make the best use of government data. In addition to any reduction in identity fraud, it would reduce costs spent on carrying out identity checks by allowing better targetting of resources.

Government could also check applications against a central register of known frauds and fraudsters

8.29 A further method of preventing and detecting fraud is to check applications for benefits or services against a database of addresses that are flagged as linked to an attempted or actual fraud. Such a database already exists in the private sector: CIFAS (see Chapter 5 above).

8.30 Government departments could pay to gain access to CIFAS information. But there would be difficulties with government membership of CIFAS. For example, full membership requires the member organisation to share information they hold about fraud or possible frauds, and it is not clear that this would be possible under current legislation. These issues would have to be examined further if this option were to be pursued.

8.31 Alternatively or additionally, the CIFAS model could be replicated, using government information. All relevant government bodies would become members of an organisation that would perform the same function for the public sector as CIFAS does for the private sector. Members would provide information about fraudulent names and addresses, which would then be stored in a database. Applications for benefits/services would then be checked against the database. Any suspect applications would then be subject to further checks before award/issue as appropriate.

8.32 Some government departments already share information. UKPS already passes information on fraud to the Immigration Service, Immigration and Nationality Directorate and the Foreign and Commonwealth Office including High Commissions, Consular Offices and other overseas issuing posts although this tends to be information on passports they subsequently discover were fraudulently obtained. They do not routinely pass information on fraudsters to other government departments.

8.33 There would, however, still be potential difficulties in wider sharing of information about fraudsters between government departments. One issue is whether current legal gateways enable the necessary information to be shared. Another is that the option would involve a significant administrative effort by departments. The practicality of the IT required and the costs of the option would also need exploration. And this option would deny the private sector access to government information – and vice versa.

8.34 It would seem, then, that membership of CIFAS by government bodies and building a government analogue are both options worthy of serious consideration. But further work would be required on:

- the option of accessing CIFAS data without reciprocal passing of information about government frauds (there is a precedent: the London Team Against Fraud and the National Anti Fraud Network receive CIFAS security alerts and information requests (mainly issued by the police via CIFAS) but do not contribute);
- implications of government joining CIFAS – in particular, the impact of the Human Rights Act and Freedom of Information Act on the existing private sector members of CIFAS and the funding implications of the substantial additional burden of complying with this legislation which they would have to bear if data was shared with the public sector. CIFAS might also need to impose controls over the way government handled information supplied from private sector sources via CIFAS;
- the costs of setting up a government analogue.

Other IT tools can help detect and prevent identity theft and fraud

8.35 Systems such as the Hunter fraud prevention system described in Chapter 5 above are widely used in the private sector to detect fraud by checking new applications and claims against themselves, previous applications and known fraudulent data.

8.36 CIFAS also has a Prevention and Investigation of Crime Tool (PICT), which uses data matching software to search the CIFAS database for links across applications and accounts. Any links which indicate multiple or organised fraud are fed back to CIFAS members to enable proactive fraud prevention. If affected members agree, a consolidated crime report is reported to the police.

8.37 There are already analogues within government. See Box 8.4 for details.

Box 8.4 Government Data Matching Exercises

The National Fraud Initiative

District Audit, which is an executive agency of the Audit Commission, originally began piloting the National Fraud Initiative in 1993 to help Local Authorities to improve the detection of Housing Benefit and student award fraud. NFI 1998, the last completed exercise, detected fraud and overpayments to the value of £42 million. 470 organisations were involved in that exercise, including Local Authorities, Police and Fire authorities, pensions agencies and central government bodies such as the Contributions Agency, Benefits Agency and IND. A total of over 5 million records on pension funds, payrolls, tenancy records, asylum seekers, renovation grants, market traders, taxi drivers and student awards were compared with 3.9 million Housing Benefit records. NFI uses long-established auditing powers to achieve this level of data-sharing.

DWP's MIDAS – Matching Intelligence and Data Analysis Service

MIDAS' core functions relate to the identification of discrepancies arising out of a data matching processes. Data matching overcomes inherent weaknesses in DWP's computer systems whereby data held on one individual, but on separate computer systems, is not automatically shared across DWP systems nor with data held by other government departments. As such it provides a successful tool in the detection of fraud, inaccuracy and overpayment. The Generalised Matching Service (GMS) uncovered £59.5m in overpayments during 2000–2001. The related Housing Benefit Matching Service (HBMS), currently involving 403 of 409 Local Authorities, uncovered Housing and Council Tax Benefit Overpayments of £37.2m over the same period. MIDAS also applies the various data sources held to meet requests generated from local DWP units. Many of these are fraud related. But identity fraud, as opposed to other types of fraud, is particularly difficult to detect through data matching.

Inland Revenue Data Mining and Data Matching

The Inland Revenue also has a number of data mining and matching facilities: a data warehouse contains data from a number of sources, both public and private sector. By using this to cluster together details of all income reported in respect of a given post code, the warehouse can identify potential fraud and evasion by use of false names, etc.

The Closer Working Intelligence Project is a new joint Revenue/Customs project. Two joint data analysis teams are carrying out analysis on joint Customs and Revenue data using a variety of tools to identify mismatches which point to areas of risk as well as facilitating processing for those who present little or no risk.

8.38 The systems described above are general counter-fraud measures that guard against misrepresentation of circumstances first and foremost. But their use to combat identity theft and fraud should not be overlooked. Costs for the data matching itself would not necessarily be high: the fee to join NFI

1998, for example, was less than £2000 for a large Local Authority. The MIDAS General Matching Service costs £4.5 million pa. However there would also be on-costs associated with investigating the frauds identified by the data matching. Departments would need to be incentivised to take action on referrals, especially as this work, while in the overall interests of protecting the public purse, may run counter to achievement of specific departmental targets.

8.39 But the success of the NFI over several years shows that significant savings can be made, and it should be possible to extend the range of government bodies which contribute information.

For the longer term, it might be worth developing a register of people entering and leaving the UK

8.40 It would useful to public service providers to know who was registered as being in the UK at a given time. In respect of identity fraud it is arguably more important to have a record of who has left the UK rather than who has arrived, to prevent hijacking of the identities of people who have emigrated. But it would also be important to know when a person has returned (as information about one-way traffic would be of limited use). Routine embarkation controls used to operate for non-UK passengers (EU citizens were also exempted in 1994) but this was stopped in 1998 and replaced by an intelligence-led approach. Some countries, such as New Zealand, do maintain thorough registers of those who have left their jurisdictions.

8.41 Such a system would make it much easier to trace people. It would assist fraud investigations across the board, particularly from the benefits and revenue departments. It should lead to increased co-operation with EC Member States and increased effort against pan European fraud. And it should make data on population migration flows much more accurate.

8.42 With the current form of passport, the difficulties in introducing such a system (and the costs) would be very significant. There are over 80 million entrances to the UK each year, and a corresponding number of exits, so there would be a huge cost of maintaining the record plus practical (and perhaps legal) difficulties with disseminating this information. A large IT system would need to be developed, which might be very expensive. It would not be easy to manage: controls would place a significant new burden on the travelling public which would not be popular.

8.43 But these problems might be reduced if a smartcard passport were ever to be introduced. There may, therefore, be a case for studying the viability of developing a register of emigrants and immigrants in the UK. But there are clearly many difficulties which would have to be investigated.

A further long-term option might involve the introduction of an "entitlement card"

8.44 Another option for the longer term worth exploration would be the introduction of a single card which would cut down the "mosaic" of documents and numbers used as evidence of identity. This is the subject of a current Home Office consultation exercise.

8.45 Such a card would carry a huge premium around its secure issue and reissue, and would reinforce the case for the issue of documents used as evidence of identity to be based on checking of "historical footprint" (ie checks of biographical identity) and face to face interviews in hard cases. Processes for issuing cards would have to be made more secure than current processes, as it would otherwise be the single ticket for a fraudster, giving access to a whole range of services.

Conclusions

8.46 There are many ways of enhancing the security of the processes that lead to the issue of documentation used as evidence of identity and the issue of unique identifying numbers. Some of those options would be at some cost in terms of service delivery; others would carry financial costs and IT risks.

8.47 If security is to be significantly improved, the keys are:

- greater use of checking against databases to verify and validate identity before issue of documents or unique identifiers;
- more use of face to face interviews to supplement these checks on "biographical" identity;
- government joining or developing a register of known frauds and fraudsters against which applications can be checked.

8.48 Even if the issue of documents used as evidence of identity is tightened, however, that is not the only action the Government will need to take in this area. If it is harder to get hold of genuine documentation/numbers under false pretences, that will increase incentives to counterfeiting and theft of identity – the subjects of Chapter 9 and 10 of this report.

CHAPTER 9: COUNTERING OFFENCES

Summary

9.1 There is a need to counter the fraudulent use of false identity documents as well as their issue. Even if the processes for issuing documents used as evidence of identity and unique identifiers are more secure, identity documents can be stolen or counterfeited and genuine identities can be "taken over".

9.2 Simple measures can help with particular problems:

- establishing registers of stolen identity or stolen identity documentation against which checking is possible;
- improved testing for counterfeit documentation and bogus identity numbers.

9.3 Technological solutions can also offer greater security against all three problems:

- the "chip and PIN" system being introduced for payment cards will make counterfeiting more difficult, make card theft less likely to be rewarding and should also guard against identity takeover;
- a biometric marker on documents used as evidence of identity would carry even greater security.

A central register of lost and stolen documents could reduce the value of stolen identity

9.4 There are two systems in use overseas, either or both which could be replicated in the UK to good effect:

- the VIS model in Holland (see Chapter 6 above) reduces the value of stolen identity documents to zero in that country;
- in the US, a Fraud Hotline has been established as part of the effort to counter identity fraud. The Hotline exists for people to report instances of fraud, waste, abuse and mismanagement in all of the Social Security Administration's programmes and operations. The remit is broader than the DWP's existing hotline for reporting benefit fraud, largely because identity fraud in the US centres around Social Security card misuse.

9.5 There is clearly potential for significant gains in this area. Around half a million UK driving licences are reported lost or stolen each year and the number of deaths reported is low. So there could be a significant number of driving licences in circulation that have been reported lost or stolen or relate to someone who has died. The same will apply to UK passports.

9.6 In the UK, the Protective Registration system run by CIFAS (see Chapter 5 above) already offers some of the benefits of the VIS/Fraud Hotline registers. The system enables people to register their own addresses as "suspect" for those applying to alter credit details or for new credit at those addresses, and this information is updated for Experian and Equifax twice daily.

Testing for counterfeit and forged documentation could be improved

9.7 It is not just the theft of genuine identities that needs to be guarded against, but also the use of totally fictitious identities by fraudsters and counterfeit or forged documentation. Fraudsters intending to create an entirely fictitious identity will usually have to produce supporting documentation from scratch (i.e. counterfeits), but they may be able to manipulate (forge) the details of existing documents. Staff testing documents need to be alert to both possibilities. Totally fictitious identities are, of course, easily exposed if there is any form of checking against databases. But there are counterfeiting factories in existence – see box 2.4 above – and measures need to be taken to prevent the use of counterfeit identity documents.

9.8 One aspect of preventing the use of counterfeit identity documents is about ensuring that security features on identity documents are frequently reviewed, to keep one step ahead of counterfeiters. This would be particularly important if entitlement cards were introduced, as they would have such high currency and would therefore be very attractive to counterfeiters.

9.9 But it is also worth looking at ways of improving the inspection of documents used as evidence of identity. Advanced forensic techniques are available for use with highly suspect documents. But it would be neither desirable nor possible to subject the vast majority of documents to this level of scrutiny. For mass use, close visual examination, including looking for watermarks and other security features can reveal alterations or the absence of features which would give grounds for suspicion and further in-depth scrutiny. Examination by UV light helps this process and also shows if a document is printed on the correct paper. The success of these basic checks in detecting counterfeits depends on the skill and knowledge of the operator, what the genuine document should look like, and the quality of the counterfeit. Detecting counterfeit overseas documentation presents a particular challenge.

It is possible to introduce safeguards either to link unique identifying numbers in some way to the individual or to make it more difficult to invent a valid number

9.10 The main identifiers issued by government are:

- the NINO/NINO number card;
- NHS number/NHS number card;
- passport; and
- driving licence.

Box 9.1 Testing for Counterfeits and Forgeries in DWP, UKPS, DVLA and IR

DWP's National Identity Fraud Unit is a central source of expertise and advice, which is also looking into developing remedial training on document examination. Although each DWP Local Office dealing with NINO applications has been issued with UV scanners there are sometimes difficulties in getting all staff trained in their effective use, particularly where volumes are low.

UKPS: Staff will UV scan documents if they are not satisfied about the bona fides of a document. Supporting documentary evidence is inspected by UKPS staff at the same time as the application form is checked. All UKPS staff who examine passport applications are trained in what to look for and instructed to refer suspicious documents to supervisors and/or 'specialist' fraud staff.

DVLA inspects all documents submitted in support of an application for a driving licence at the initial application stage. If there are any suspicions over the authenticity of a document presented in support for a driving licence, the documents are passed to a specialist enforcement section for further examination including the use of UV scanners. Every member of staff who is required to process driving licence applications receives appropriate training.

IR Tax Credits Office staff based in their National Identity Investigation Section routinely need to decide on the integrity of documents. They use UV scanning equipment and they too have received specialist training.

9.11 Each of these identifiers is registered on an appropriate government database. All of these identifiers issue supporting documentation (number card, passport, and driving licence) that can be forged or counterfeited. To do this effectively the forger must either 'invent' a plausible unique identifying number that appears in a valid format or hijack an already existing number belonging to another person – with or without their collusion.

9.12 In order to make forgery more difficult numbers can have special formats – sometimes containing algorithms – to either link the number in some way to the individual or make it more difficult to invent a valid number and easier to spot a forgery. Such checks exist for some but not all numbers that are used as unique identifiers.

9.13 Significant change to existing numbers and databases would be very expensive and would be prone to human error if it required a large scale re-issue of numbers to individuals. If changes were introduced from now onwards there would be a significant time lag before changes radically improved identity validation and reduced the error rate. Moreover, if too many staff were to know about the security device it could be prone to abuse; on the other hand if too few were to do so its utility would be reduced.

9.14 The options therefore seem to be more suited to being adopted for the issue of new numbering systems than to existing systems. Any new system of identity numbers should include an algorithm.

Technological solutions can help prevent "point of use" identity theft and fraud – but at a cost

9.15 As set out in Part One of this report, payment card issuers are moving to a "chip and PIN" system to improve security at the point of use, a technological fix that can prevent "point of use" misuse of payment cards. And in government, the Office of the e-Envoy is looking to develop smart card technology in support of the government's pledge on e-service delivery. But such systems come at a cost. The new "chip and PIN" system will cost upwards of £1bn in infrastructure costs to increase payment card security – on the basis of supporting 750,000 terminals and 120 million cards.

The use of biometrics

9.16 Biometric markers are one of a number of devices that can be used to protect against the use of stolen identity. As such, biometrics are not a solution in their own right, but a component of other counter-measures. A biometric marker can ensure that the bearer of the card at point of use is the individual to whom the card has been issued. Alternatively biometrics could be used as part of "closed" systems to ensure someone applying for the service has not already done so under another identity – though this is technically more difficult.

9.17 Biometric systems are in use in some parts of the world. There are trials of fingerprinting and iris recognition in Illinois, California and New York, and a trial of an iris recognition system for frequent flyers about to start at Heathrow. Similarly, hand geometry is being trialled to provide fast immigration services for frequent flyers entering the US and Canada. Argentina (population 34 million) is in the process of issuing identity cards with fingerprints. South Africa has already done so – but checking is manual (there are no biometric readers of the fingerprint on the card). A biometric – a fingerprint – is also in use in Spain on identity cards, again on a small scale. But insecure processes involved in its issue have apparently lessened the value of the card in the fight against crime. Details on biometric systems are set out in Box 9.2.

9.18 The Home Office consultation paper on entitlement cards suggests, however, that because of concerns about the cost and reliability of biometric systems catering for very large numbers of transactions, there should not be biometric "readers" to verify and validate the biometric on entitlement cards (if they are introduced) at point of use. Rather, at point of use, checks could be made against a database; and entry to that database should be governed by the production of a biometric (ensuring that there are no duplicate entries).

Box 9.2 Biometrics

Biometric systems come in a number of forms, including fingerprint verification, hand-based verification, retinal and iris scanning, DNA verification, facial recognition, voice recognition and signature recognition.

Biometrics offer a number of benefits. There is a far lower risk of counterfeiting than exists with documents. Biometrics cannot be lost or forgotten and checking processes are less susceptible to human error than, for example, checking photographs. All things considered, biometrics offer the highest level of security verification available.

But there are drawbacks. First, they are expensive: in addition to the cost of issuing the biometric, "reading" equipment is required. There are issues around public acceptability. Biometric systems are by no means foolproof: all types of biometric systems currently available run the risk of reporting "false positives" or "false negatives"; around 10–15% of "genuine" people will fail the test if it is set to minimise the numbers of fraudulent people let through. This is very much a developing area. Biometrics offer undoubted potential, but it is a potential which has yet to be realised in any large scale applications.

Further work on biometrics is being carried out by UKPS and DVLA on establishing a common database, supported by a biometric, for those who have driving licences or passports (or the proposed new entitlement card).

Conclusions

9.19 It is tempting to think that a simple solution can be found to prevent all misuse of identity documents after issue. That is not the case: despite the introduction of "chip and PIN", payment card fraud may continue to rise, with more use of identity takeover in particular by organised criminals. And biometrics, as a point-of-use identity check, are not yet sufficiently advanced to offer the additional security they promise to provide in the longer term.

9.20 In this area, then, the best way forward lies in simple measures: continued vigilance, training and use of UV scanners to detect counterfeits and forgeries, and a central register to reduce the value of stolen documents.

9.21 Despite the best efforts of government and the private sector, however, identity theft and fraud will sometimes be committed. So Chapter 10 looks at ways of improving detection and prosecution of identity fraudsters.

CHAPTER 10: DETECTION AND PROSECUTION OF IDENTITY FRAUD

Summary

10.1 There are three ways in which the detection and prosecution of identity fraud could be improved:

- better joining up of counter fraud action. Those committing identity frauds rarely stop at departmental boundaries. Once a false identity has been built, it becomes useful in committing offences against a range of organisations. This will include the private sector too and frauds will not necessarily stop at national borders. The response to the problem should reflect this;
- increasing the priority currently given to work to counter identity fraud in the criminal justice system;
- examining the case for a new offence of identity fraud.

10.2 The legal position in Scotland is, of course, different to that in England and Wales: it is the Crown Office, rather than the CPS, which prosecutes, and the common law is different. The recommendations that relate to the CPS and to the consideration of a new offence of identity fraud would need further thought in the Scottish context, when it comes to implementation of this report.

More active detection and prosecution policies are required to supplement more secure processes for issuing identity documents and action on theft and counterfeiting

10.3 However secure the arrangements for the issue of documents used as evidence of identity and the issue of unique identifiers, and however strong the arrangements to counter theft and counterfeiting, there will still be those who attempt identity theft and fraud and those who succeed in the attempt. Organised criminals will still want to run drugs (often under alias identities), traffic in people (who will want to work illegally), launder money (often under alias identities) and defraud the state and the private sector for financial gain (often through the creation of multiple identities and identity theft).

10.4 This chapter explores how the government can raise its game in the detection and prosecution of identity fraudsters and looks at the case more generally for collecting better management information on identity theft and fraud.

10.5 Counter-fraud action needs to be considered in the round and recommendations to improve detection and prosecution of identity fraud considered in the context of wider counter-fraud action – fraud and identity fraud are not always two separate crimes and certainly they are not always tackled by separate counter-fraud units in either government or the private sector. The proposals in this chapter on identity fraud are therefore advanced against this background.

The principles that should govern joined-up counter fraud activity are not hard to formulate

10.6 There are a number of general principles which should guide interdepartmental co-operation:

- strategic sharing of information: organisations should co-operate and share information at the strategic level, including the sharing of strategic threat assessments, for example about which trade sectors or geographical areas are being targeted, which groups of the community are involved, which methods are being used, etc;
- case-specific sharing of intelligence and information: a department or organisation which discovers an identity fraud should notify all other nominated organisations, where this is legally permitted;
- shared expertise: organisations should share their expertise and techniques in preventing, detecting and investigating identity frauds;
- joint action on prosecution: where offenders are found to have committed offences against more than one organisation, a joint prosecution should be pursued if at all possible.

10.7 Such joined-up activity should include a role for enforcement agencies, such as the National Criminal Intelligence Service, and should operate across the private/public sector boundary.

And there is a range of options for translating the principles into action

10.8 A range of options is worth considering:

- better joining up between existing liaison groups;
- a range of wider structural changes, such as the creation of government institutions/organisations similar to APACS and CIFAS; or a fraud hotline, which would allow more coherent collection of information about fraud; or the extension of the roles of existing bodies such as the National Crime Squad.

Existing liaison mechanisms, notably the IIFF, should be strengthened and expanded to cover the private sector

10.9 The cross-Whitehall Interdepartmental Identity Fraud Forum (IIFF), exists to help departments prevent and detect identity fraud. It is the only inter-departmental group on identity issues, thereby placing it in a key position to advise Ministers and others.

Box 10.1 The IIFF

The terms of reference of the IIFF are:

To develop a common multi-departmental approach to identity issues by:

- improving and formalising liaison between participating organisations;
- promoting the development and maintenance of common procedures for the verification of identity and promoting good practice; and
- seeking ways of changing procedures that hinder the prevention and detection of identity fraud and abuse.

IIFF is an expert group, with a depth of knowledge and experience, consisting of not only government departments that use and produce documents used as evidence of identity but also those making policy on evidence of identity procedures.

As well as advising on existing identity issues, the group's members are also responsible for taking forward major work programmes to improve inter departmental initiatives on evidence of identity. It looks at developing new methods and pushing back the boundaries in this field.

The group helps departments prevent and detect identity fraud by strengthening evidence of identity procedures and by facilitating co-operation across Government. It:

- endorses best practice;
- provides a consultation service to give advice from across Government perspective;
- provides a process overview showing the interdependencies and relationships between government departments; and
- compiles and distributes position papers highlighting initiatives and identifying problems and gives advice on how to address them.

This list is not meant to be exclusive as the IIFF not only seeks to provide leadership on evidence of identity but will also respond to changes of Ministers' objectives on the subject and related issues when required. It therefore deals with a range of issues and reports to different Ministers, depending on the subject area.

10.10 The terms of reference for the IIFF could be strengthened to reflect the principles set out in paragraph 10.6 above. And its membership could be expanded to include private sector representation. Under strong chairmanship, it could fulfill the need – drawn to the attention of the project team by private sector organisations – for better joining up of counter fraud activity across the public/private boundary.

10.11 Elements of its forward work programme could include:

- **the creation of a "register" of groups engaged in work to counter identity fraud:** there are a number of bodies with a co-ordinating role in the fight against fraud more generally, which would have an interest in identity fraud. The IIFF could build on this to ensure that the full picture of counter-fraud activity is always borne in mind by all players;
- **setting standards and targets:** each organisation needs to describe and to set their policy objectives and then to agree with others what constitutes a success. There is also be a case for cross-departmental targets in this area. This could help tackle the major problem in this area, which is the lack of incentives for departments to co-operate against fraud. From the standpoint of government, it is not important which department gets the result as long as government gains, the abuse is stopped, the offenders are brought to account and the public purse is protected. Departments need to be incentivised to act in accordance with this principle. The IIFF could be charged with coming forward with detailed proposals;
- **further developing and implementing an overarching identity fraud strategy:** in order to achieve true joint working there is a need to take forward the work of this report in developing an overarching fraud strategy. Each department must contribute to this strategy, understand their role in it and recognise that their policy may need to be modified to enable a broader success across government;
- **defining outputs on identity fraud:** as well as defining standards there is a need to define and to measure success or failure. A robust method of measurement would have to be instituted to enable each of the partners to measure the effectiveness of their actions and of the use of their resources;
- **developing better liaison on identity fraud with prosecuting authorities:** a more joined up approach to prosecution is required. There is much fragmentation with some departments conducting their own legal business with their own lawyers and some relying on the police and Crown Prosecution Service to prosecute on their behalf.

There may also be a need for new organisations within government

10.12 In the private sector, the combination of market forces and joint planning between private sector organisations has led to the creation and growth of organisations such as APACS, CIFAS, Experian and Equifax. In government, there is a need to mirror some of these structures and to ensure that the right incentives are in place for departments to co-operate in action against identity fraud.

10.13 New institutional arrangements in government could take a number of forms. For example, there may a case for developing a government analogue of CIFAS as an institution/organisation as well as of the services it provides. (Chapters 8 and 9 set out the case for the service provision.) This would allow information about identity fraud to be collected in a single place, which would help support the counter-fraud effort. A fraud hotline, based on the US version, is another possible option.

10.14 There is also a case for establishing a Fraud Agency within government. This would bring together expertise across government, with potential economies of scale and would reduce 'silo' boundaries that militate against tracking and investigating fraud as it travels across departmental boundaries.

10.15 But a Fraud Agency would bring serious resource/training implications. There would be major issues to resolve in relation to boundaries between the new Agency and government departments on policy and operations. And it is debatable that all investigators in the fraud agency would work using common methods of investigations and to common policies. There are huge differences of approach even within departments: for example Customs officers investigating a bootlegging gang will adopt a different approach to an international VAT fraud scam.

10.16 From the perspective of identity fraud – and with a view to maximising the gains that can be made quickly and efficiently – the best way forward would be for the IIFF to resume its current role, but on the basis of revised terms of reference and to reinforce its membership with private sector representatives.

Prosecution policy and practice for identity fraud could be rationalised

10.17 When identity fraud is detected, perpetrators need to be brought to justice. Part One of this report showed that this does not always happen and set out some of the reasons for this state of affairs, notably:

- the lack of a prosecution arm to some government departments;
- low priority given to these offences; and
- the lack of a specific offence of identity theft or fraud.

There is a case for DVLA and UKPS to develop a prosecution arm to investigate and prosecute identity frauds in England and Wales

10.18 Prosecution works well at the moment in those departments, DWP and IR, which run their own prosecution arms, because they are able to investigate and prosecute fraud themselves.

10.19 This system could be introduced into DVLA and UKPA in England and Wales (in Scotland only the Crown Office can prosecute). This would potentially bring greater motivation for staff, would permit greater specialisation possible in an Agency's own regime and individual agencies would be better placed to decide on which are the best cases to proceed.

10.20 But the right expertise would need to be developed. Resource and additional infrastructure would be needed. UKPS and DVLA are unlikely to be able to import staff with the necessary experience unless additional remuneration was offered. Heavy recruitment and training costs would be incurred, and there would be on-costs associated with the increased capacity. It is not clear that the UKPS or DVLA would have a sufficient body of work to warrant separate arms.

10.21 This option would seem worth further exploration. But this would have significant implications for both agencies and much further work on the option would be required.

There is a case for reviewing the priority currently given to work on identity fraud in the criminal justice system

10.22 Chapter 4 set out the difficulties that those responsible in government for detecting identity fraud can experience in getting investigations and prosecutions taken forward by the police and by the CPS in England and Wales. There is a case for according this work a higher priority.

10.23 For the Home Office, departmental priorities are set out in the department's Public Service Agreement. While there is a PSA target on organised crime, identity fraud does not figure in this as such. Moreover:

- current prosecutions have a generally low rate of success and it may appear fruitless to target limited police resources on a less productive area, rather than on crimes against the person;
- as it is expensive to pursue cases through the courts it could be argued that it would not be worthwhile in terms of penalties imposed. Currently an attempt to obtain a passport fraudulently is prosecuted as an attempt to fraudulently obtain an item worth £28 i.e. the value of the application fee.

10.24 For CPS, work is effectively demand led. Policy is to take forward any prosecutions, including prosecutions for identity fraud, which pass two tests:

- the evidential test – whether there is enough evidence to provide a realistic prospect of conviction against each defendant on each charge;
- the public interest test – a prosecution will usually take place unless there are public interest factors tending against prosecution, which clearly outweigh those tending in favour.

10.25 Notwithstanding these difficulties, it would seem worthwhile for the IIFF to explore these issues further. In particular there is a need for further, more detailed discussions with ACPO and CPS about what problems would arise if such cases were to be given a higher priority; and how the problems of working across police authority boundaries (identified as a problem in Chapter 4 above) can be tackled.

10.26 It would also be worth considering further the role of prosecution policy for local authorities. The questions here are whether there is any central body that would control/guide/influence such a role – or collect information about prosecutions.

10.27 For all players, however, the creation of a new offence of identity fraud might, however, of itself, lead to more prosecutions – if prosecution was easier and penalties greater.

There is a case for creating a new offence of identity theft or identity creation with the intent of fraudulent use, which would carry new higher penalties

10.28 There is a case for the creation of a new offence in England and Wales of identity theft or identity creation with the intent of fraudulent use (in Scotland it may not be necessary to create a specific offence because of the scope of common law). This is covered in some depth in the Home Office consultation paper on entitlement cards.

10.29 Identity fraud is normally part of a much more serious set of offences committed by organised criminals. Charges brought against those responsible for identity fraud are therefore normally for more serious offences. However, sometimes it may be right for police to disrupt criminal activity before more serious crimes are committed. And in those circumstances it might be helpful for there to be a specific offence of identity fraud. This would also serve to make easier the prosecution of offenders.

10.30 Moreover, the offences commonly used to prosecute identity fraud-related crimes do not sufficiently take into account the serious damage and harrowing experience of individual victims of identity theft. Such offences are often prosecuted as conspiracy under the Theft Act. This takes account only of the financial loss, not the personal injury involved. So another possibility would be for the Home Secretary to ask the Sentencing Advisory Panel to look at the levels of sentencing for these categories of offences, and to propose to the Court of Appeal that guidelines be reframed or revised. The Court could then decide to issue guidelines increasing sentences for these categories of offence.

10.31 These proposals also warrant further study by IIFF. In particular there should be further investigation of the deterrence effect of contrasting policies, drawing on the views of stakeholders: courts, academics and other analysts, accountants, lawyers, and best practice in other countries.

There is a case for collecting better management information on identity theft and fraud

10.32 Finally, as this study has made clear, statistics collected for identity fraud are neither comprehensive nor robust. Therefore it is impossible for government to calculate how much fraud exists, what the real risks to individuals, the state and the private sector really are and what costs are incurred. Lack of any kind of reliable baseline also means that is will be difficult to calculate the impact of any strategies to combat fraud.

10.33 The IIFF should consider this as an early and urgent part of its work programme, working with departments to agree reporting requirements.

CHAPTER 11: THE WAY FORWARD

11.1 This report represents the most comprehensive study of the specific problem of identity fraud ever carried out in government. Fieldwork for the study found a strong consensus across government and the private sector both that this was an important and growing problem and about the nature of the action required to tackle it.

11.2 On some issues identified in this report, the Government is already taking action. On others, the Government is today launching a consultation exercise. The Home Office consultation paper on entitlement cards, which draws on this report, seeks views of consultees on a number of questions to do with identity fraud. They are as follows:

P16 The Government invites views on the early steps it would like to take to tackle identity fraud and welcomes expressions of interest from the private sector to collaborate in this work.

P17 Views are invited on whether checks on applications for passports and driving licences should be strengthened to the degree outlined in Chapter 5 of the Home Office document (on how a scheme might work in practice) whether or not the Government decided to proceed with an entitlement card scheme based around these documents.

P18 If more secure passports and driving licences were issued based around a common identity database shared between the UK Passport Service and the DVLA, the Government invites views on:

- whether it should take the necessary legislative powers to allow other departments to access this identity database to allow them to make their own checks;
- whether it should allow the private sector to access the identity database provided this was done with the informed consent of subjects.

P19 Views are sought on whether the Government should procure a service from the private sector which checked applications for services against a number of databases used by the credit reference agencies or similar organisations and selected biographical data held by the Government.

P20 Views are invited on whether a summary-only offence of identity fraud should be created.

11.3 Future policy in this area will be influenced by the responses to the consultation exercise. Responses should be sent to The Entitlement Cards Unit, Home Office, Queen Anne's Gate, London SW1H 9AT or entitlementcardsunit@homeoffice.gsi.gov.uk.

ANNEXES

ANNEX A: MEETINGS HELD BY THE PROJECT TEAM

The Project Team held meetings with the following organisations:

APACS
Association of British Insurers
Association of British Insurers – Insurance Fraud Group
British Banking Association
Child Support Agency
CIFAS
Consignia
Criminal Records Bureau
Crown Prosecution Service
Department of Health – Directorate of Counter Fraud Services
Department of National Savings
Driving Standards Agency
DTLR (Electoral Register)
DVLA, Swansea
DWP – Fraud Strategy Unit (Leeds)
DWP – Child Benefit Centre
DWP – Internal Workshop on identity profiling
DWP – Matching, Intelligence, Data Analysis Service
DWP – AD9 Control Centre for the enhanced NINO Process
DWP – Analytical Services Division
DWP BA National Identity Fraud Unit (Newcastle)
DWP BASIS (Canons Park)
DWP Child Benefit Centre
DWP Departmental Central Index
DWP Glasgow CCU Enhanced NINO Process
DWP London Board Secretariat Enhanced NINO Process
DWP National Intelligence Unit
DWP Pensions and Overseas Directorate
DWP Personal Account Security Project
East London & City Health Authority
Employment Service Fraud Unit
Equifax

Excel Biometrics Exhibition 2001

Experian

Financial Services Authority

Financial Fraud Information Network

General Register Office (Scotland)

Haringey local authority

HMCE Business Services & Taxes Policy Group

HMCE Central Co-ordination Team, Central Intelligence

HMCE Financial Intelligence

HMCE Law Enforcement Policy

HMCE National Intelligence Class A drugs

HMCE Regional Business Service

HMCE Registration Modernisation Project

HMCE VAT Registration Group

HO – NASS Fraud Investigations

HO Biometric co-ordination group

HO Electoral Registration Policy

HO Immigration – Enforcement/arrest terms

HO Immigration – National Forgery Section

HO In-country applications for asylum and changes to immigration status

HO IND – Work permits

HO International & Organised Crime (Assets Recovery Agency)

HO National Asylum Seekers Support, Croydon

HO Property Crime Team

HO Immigration Service, Heathrow

IDEA

Inland Revenue Insurance Contributions Office – NI Integrity

Irish ID Fraud, Department of Social, Community and Family Affairs (telephone interview)

IR Business Services

IR Construction Industry Scheme

IR Personal Tax Division

IR Cross Cutting Policy (Prosecutions)

IR Cross Cutting Policy (Data Protection)

IR Internal Audit

IR NICO NI Integrity

IR NICO Technical Services Group
IR Tax Credit Office (Norcross)
IR WFTC National Intelligence & Identity Section (NIIS)
IR WFTC Operations
IR WFTC Persons from Abroad/DCI
IR/C&E Joint Shadow Economy team Newcastle
Lancashire & South Cumbria Health Authority
Lewisham local authority
Local Government Association
London Team Against Fraud
Lord Chancellor's Department
Metropolitan Police
National Audit Office (telephone interview)
National Audit Office
National Criminal Intelligence Service
No.10
Northern Ireland Office (Electoral Registration)
North Tyneside Council Electoral Registration
ONS General Register Office- Local Services Section
ONS Civil Registration Review
ONS General Register Office – Certificate Applications
ONS General Register Office – Fraud Section
ONS NHS Central Register
ONS General Register Office – General Section
Prof Michael Levi, Prof of Criminology Cardiff University
Reading Local Authority
Security Service
Serious Fraud Office
UKPS Fraud & Security Section
UKPS Liverpool issuing office
UKPS/CRB
UKPS/ELVIS
Westminster Council Electoral Registration
Wycombe Local Authority

ANNEX B: EXTENT OF THE PROBLEM BY ORGANISATION

Public Sector

HM Customs & Excise

1. The major concern is Missing Trader Intra Community Fraud (MTIC). This exploits the fact that between registered traders within Member States exported goods attract a zero rating for VAT.

2. The fraud generally operates between a number of traders in the EC usually supplying high value goods such as mobile phones or computer parts. The fraud involves a chain of traders in different EC countries exporting goods to each other. In all transactions the goods will be zero rated for tax purposes. But at some point one of the traders will charge the VAT and then fail to pay the output tax to the relevant tax authority and that trader will then disappear.

3. MTIC fraudsters often operate using false identities or by using front people. It is often difficult to establish the identities of the true directors and identify those committing the fraud. HMCE estimate total losses due to this at between £1.7bn and £2.6bn pa. It is impossible to say how much is directly attributable to identity fraud, but even allowing for just 10% would give a figure of between £170m and £260m pa.

4. HMCE also believe that around £390m is laundered a year: this is consistent with the estimate of £200m a year laundered through bureaux de change in Central London alone, and £490m in the UK as a whole in 18 months. Under the money laundering regulations all banks and financial institutions are required to know their customer. To exchange money at bureaux de change therefore requires proof of identity.

Department for Education and Skills

5. The DfES is aware of people who are not adequately qualified trying to gain employment as teachers, either through falsifying qualification documents or hijacking the identity of someone who is qualified. This also includes people obtaining false documents with the intent to commit child crime such as paedophiles or violent persons who have been banned from working with children.

6. No figures are available to indicate the scale of the problem.

Department of Health

7. One type of identity-related fraud that occurs within the NHS is evasion of payment of NHS charges or accessing of NHS services by non-entitled people using the identities of entitled people. There are no reliable figures for the cost of this type of fraud.

8. The Directorate of Counter-fraud Services recently carried out risk management exercises which indicated evidence of patient identity fraud:

   - 13 false identities from a sample of 4,921 optical cases (0.26%);
   - 14 false identities from a sample of 6,400 prescription cases (0.22%).

9. A major problem area of fraud within the NHS is where contractors (e.g GPs, opticians, dentists) claim costs for treating patients who do not exist or who are no longer registered at that practice. No estimate is available of the level of this type of fraud.

10. The NHS Central Register contains details of 2816 patients who are known to have attempted to register with more than one GP, for the purpose of obtaining multiple prescriptions.

Inland Revenue

11. Inland Revenue can suffer identity fraud in a number of areas. Specifically Working Family Tax Credits (WFTC) and Disabled Persons Tax Credit (DPTC) can be subject to identity fraud in much the same way as is the case with DWP benefits. Where identity fraud is an issue it may often represent an organised fraud against the system and therefore the financial impact per case can be high.

12. False identities can also pay a part in repayment tax frauds, where false identities can give rise to incorrect tax and repayment frauds. No figures are available to judge the extent of this, however the case study in Box 2.6 gives an indication of the type of fraud that can be perpetrated.

Driving Standards Agency

13. DSA conducts 1.2 million driving tests each year. Candidates are required to provide proof of identity at both the theory and practical tests. Candidates are known to try to use friends who are experienced drivers to take their tests for them, backed up by false identity documentation. In 2000/2001 there were 3231 cases where candidates for the practical driving test were prevented from taking their test because they were unable to satisfy the examiner of their identity, and 1200 cases where theory driving tests were not conducted for the same reason.

Department for Work & Pensions

14. In the period April 2000 – March 2001, 564 cases involving identity fraud were established by the Benefit Agency's Security Investigation Service. No information is available on the total number of identities involved nor on the total value of the loss to public funds.

15. A measurement exercise to measure the level and types of fraud in Income Support and Jobseeker's Allowance cases over the period April 1999 to March 2000 produced an estimate that the amount overpaid due to identity fraud was £3 million out of a total expenditure of £15,831 million, which is a very small percentage of expenditure (0.02%). A further £80 million

overpaid, attributable to persons not being found at a given address, will have included some cases of false identity. Given that the measurement exercise was not specifically designed to measure identity fraud, it is impossible to be precise, but it is reasonable to suppose that the loss to identity fraud might be £20–50m pa.

16. In addition Instrument of Payment (IoP) fraud which involves the presentation of lost, stolen or counterfeit girocheques or order books sometimes involves misrepresentation, but DWP does not count this as identity fraud.

Electoral Registers

17. Being able to vote is not the only incentive for people to get their names on to the electoral register. The major credit reference agencies require evidence that a person is on the register in order to validate and verify identity.

18. One local authority estimates that there are 15–20 cases per year where identities are being manipulated or created in order to get onto the electoral register. Nationally there are no figures to indicate how many people are registering in more than one constituency.

Local Authorities

19. Multiple identities are used to facilitate multiple housing benefit claims, while landlord identity fraud usually involves a fictitious identity for a landlord where the claimant is actually the owner-occupier.

20. One local authority visited by the team reported 4 cases of identity fraud, involving 60 multiple identities, while another reported 20 cases of landlord identity fraud.

Immigration and Nationality Department – Home Office

21. In Terminal 3 of Heathrow alone, around fifty fraudulent documents are found each month, and the detection rate is estimated to be at most 10%.

22. Home Office estimate potential savings of £6 million per 1000 reduction in clandestine entrants, i.e. an average of £6000 each. Given a 10% detection rate, this would equate to costs of £36m per annum resulting from this one entry point.

Lord Chancellor's Department

23. The Legal Services Commission (LSC) has some evidence that a very small minority of providers of publicly funded legal services may sometimes create bogus clients for the purpose of extracting payment from the LSC. Wherever such fraud is detected, the LSC requres the amount of money overpaid to be refunded. No statistics are available on the extent of this type of fraud. The total cost of legal services funded by the LSC is in the region of £1.6bn annually.

UK Passport Service

24. UKPS issues approximately 5.5 million passports each year. Around 1,400 fraudulent applications are detected annually, which is about 0.003% of the total number of applications. The actual number of fraudulent applications is thought to be higher and an ongoing exercise within UKPS is designed to provide a more accurate figure.

Driver and Vehicle Licensing Agency

25. DVLA's specialist enforcement team routinely refers cases to the Police for further investigation where fraud is suspected but no statistics are available on outcomes. It is known that the number of counterfeit photocard licences is on the increase (although to date those detected have generally been of poor quality).

General Register Office

26. In 2000/2001 GRO(E&W) recorded 247 suspicious applications for, theft of and fraudulent uses of birth and death certificates in England and Wales. GRO(S) estimate that in Scotland, the problem is about 10% of that level, i.e. 25 suspicious applications per year.

Police Forces

27. Anecdotal evidence indicates that a large proportion of unpaid speeding a parking tickets, where the Police are unable to track down the offender, are due to identity fraud. No figures are available.

Private Sector

Credit Card Fraud

28. The Association of Payment Clearing Services (APACS) estimate that in 2001 losses due to counterfeit cards, lost and stolen cards, and card not present fraud cost the card issuers around £370m.

Insurance Fraud

29. Measuring fraud is as much of a problem for the insurance companies as it is for the public sector. Nevertheless, total annual losses due to personal insurance fraud are estimated at over £1bn (commercial insurance fraud is likely to be at least £2bn, but rather less of this is thought to be due to identity fraud).

30. While much of the fraud committed by individuals is opportunistic, with people inflating the value of claims, as much as 50% of all fraud losses in this area are thought to be pre-meditated in some way, with up to 50% of these being a direct result of identity fraud. This gives a figure of losses due to identity fraud in the range of £250m.

31. The motives for taking out insurance cover under a false identity vary. A person may manipulate part of their identity, such as their age, in order to receive otherwise difficult to obtain or prohibitively expensive cover, to hide a poor claims record or to obtain legally required insurance certificates. They may plan to make multiple (false) claims on a single event, or the insurance policy may be a means of laundering money illegally obtained;

CIFAS

32. CIFAS report that £62.5m of all fraud reported to them (by number of frauds reported) during 2000/01 fell into their categories of false identity or victim of impersonation fraud.

Total cost of identity fraud

	TOTAL	**£1364m**	
Organisation		**Costs (£m)**	**Notes**
Customs	VAT	215	Total MTIC fraud £1.7 – £2.6bn (midpoint £2.15bn). Assumes ID fraud is 10% of this
	Money laundering	395	Based on £490m over 18 months; consistent with £200m in c. London
DFES			No figures
DH	Health Authorities	0.75	Study done in 2 HAs only – no broader extrapolation permitted 2816 multiple registrations
IR	WFTC/DPTC		No figures
	Tax repayment		No figures
DSA	Driving tests		1200 not allowed to take theory test; 3231 not allowed to take practical. Costs are non-financial (unqualified drivers).
DWP	Instrument of Payment		No figures
	CSA		No figures
	Child Benefit		No figures
	Pensions & overseas		No figures
	Welfare fraud	35	C 1% of all welfare fraud (£2–5bn)
Electoral register			No financial costs
Local authorities	Housing Benefit		No figures
	Haringey		4 cases of ID fraud; 60 IDs
	Lewisham		65 IDs; 20 cases of landlord ID fraud
HO	Immigration	36	@ 50 pcm (Heathrow) x 10; £6000 per clandestine entrant

Total cost of identity fraud *continued*

	TOTAL	**£1364m**	
Organisation		**Costs (£m)**	**Notes**
LCD	Legal aid		No figures
UKPS	Passports		1484 Fraudulent applications
DVLA	Driving licences		No figures
GRO			247 suspicious applications for, theft of and fraudulent uses of birth and death certificates
GRO(S)			About 25 suspicious applications for, theft of and fraudulent uses of birth and death certificates.
Police forces	Unpaid speeding/ parking tickets		No figures
APACS	Credit cards	370	Includes use of counterfeit, lost/stolen cards and card not present fraud – 2001 estimate
Insurance companies		250	Based on £1 bn total; 50% pre-meditated; 50% of this being direct ID fraud
CIFAS		62.5	Value of false ID/victim of impersonation fraud (by number of frauds reported)

ANNEX C: HOW SECURE IS THE GOVERNMENT'S ISSUING OF DOCUMENTS USED AS EVIDENCE OF IDENTITY?

Passport

1. Between April 2000 and March 2001 5.3 million passports were issued. In the same period 1484 (0.03%) fraudulent applications were detected. Of these 301 used deceased identities, 1003 used another person's identity or documents and 110 used a fictitious identity. To counter the use of birth certificates of dead infants, UKPS staff now have on-line access to Events Linkage Verification Information System (ELVIS) data. Any suspicious applications are forwarded onto a Special Files Team for further in depth checks against external databases and enquiries with other agencies.

2. UKPS has recently set up a fraud and intelligence section which will provide an infrastructure and the skilled resource to provide a more systematic and consistent approach to fraud. They have also seconded a resource into NCIS to enhance links with the Police and to develop a protocol.

3. They have recently amended the passport application form and countersignatories are now encouraged to supply their own UK passport numbers. This will enable UKPS to check against their own database to verify the information provided and should reduce the time delays in writing to countersignatories.

Driving Licence

4. There are currently 38 million driving licences in issue. Between April 2000 and March 2001 DVLA issued 5,400,040 licences which comprised 735,874 provisional licences; 1,152,237 renewals (licence expired); 831,584 exchanges of UK licences; 510,254 duplicates (licences lost or stolen); 2,128,895 replacement licences (change of name or address) and 41,196 exchanges for foreign licences. Around 17% of applications are rejected for a variety of reasons including incorrect fee and incomplete documentation. DVLA cannot be certain how many of these are processed on re-submission of the completed application.

5. In 60% of applications the supporting document is a UK passport. In these cases the passport is deemed to be proof of identity and only rudimentary checks are carried out. Where applicants do not provide a UK passport they provide a birth certificate (and marriage certificate where appropriate) plus a photograph which together with the application form must be endorsed by a countersignatory. DVLA do check a proportion of countersignatories. Any suspicious applications are referred to an enforcement section for more in-depth checks.

6. As the driving licence system is required by law to be self financing DVLA is under pressure to keep cost increases to a minimum. The cost of resourcing any increase in the level of identity checks would need to be funded by an increase in the licence fee.

Birth certificates

7. Birth, death and marriage certificates are records of historical fact, not evidence of identity. The law allows any person to apply for a certified copy of any record held by the Registrar General. There were 1.8 million such applications in 2000 in England and Wales. Certificates in Scotland can be obtained from GRO(S) or from any of the 340 registration offices. A 10% estimate of those issued in England & Wales would be reasonable, i.e. 180,000.

8. Although an application cannot be fraudulent, those made to GRO(E&W) for birth or death certificates in England & Wales relating to persons under 50 years of age are subject to closer scrutiny. Applicants who are unable to supply full information about the birth or death are questioned as to their reasons and personal applicants are asked to provide evidence of their name and address. Suspicious applicants will be asked to supply the missing information before a certificate is issued. In Scotland, GRO(S) has linked all births and deaths between 1940 and 2000 on its database of vital events and has a system in place to check potentially fraudulent use of certificates.

9. The process for dealing with applicants wanting a certificate of their "own" birth, when a check for an infant death is positive and registrars are concerned there may be fraudulent intent, has recently changed. Rather than simply refuse the application and return the fee, the certificate may now be issued but endorsed with details of the child's death, thus rendering it useless for fraudulent purposes. This also has the bonus that the fee is retained while sending a clear message that checks are being made. GRO(S) employs a similar system of endorsing certificates.

10. GRO(E&W)'s Events Linkage Verification Information System is designed specifically to eliminate "Day of the Jackal" fraud by initially linking records of deaths of under 18 year olds with the relevant birth records. When complete, 485,000 deaths will be linked. UKPA, DVLA, DWP (Child Benefit, NIFU and the National Intelligence Unit), the Home Office Immigration and Nationality Department, the Criminal Records Bureau and the National Crime Squad have ELVIS data. GRO(S) has a similar system.

NINO cards

11. All children in respect of whom child benefit is paid are allocated a child reference number and this automatically becomes their NINO when they reach 15 years and 9 months. A NINO card is then issued to the recorded address. Therefore the vast majority of people in the UK are notified of their NINO through an automated process and have no need to apply for one. Around 700,000 NINOs are allocated automatically each year through this process.

12. DWP and Inland Revenue have established a NINO Board to oversee the management and control of NINOs. A secure NINO allocation process (SNAP) was introduced nationally in April 2001, following a successful pilot. All those who do not have a NINO must go through this process before one

is allocated. All applicants must attend for interview and provide sufficient background information to establish whether a NINO record should already exist and if so for it to be traced, or where one does not exist, for one to be allocated. This is backed up by staff in 13 Central Control Units who conduct checks against other public databases, trace existing NINOs and ensure that as much relevant information as possible has been collected at the interview stage.

13. This rigorous process has led to delays in new NINOs being allocated. DWP are currently refining the process to ensure the balance is right between customer service and the integrity of the process to ensure security standards can be maintained whilst making the allocation process less burdensome for less risky cases. SNAP could be seen as a model for other departments to verify the identity of their customers but such a rigorous process has significant administration cost implications and would inevitably have an adverse impact on customer service levels.

NHS Numbers

14. NHS numbers are allocated when a child's birth is registered at a Register Office or when someone, usually from abroad, registers for the first time with a GP. However, from November 2002, NHS numbers for babies will be issued by Maternity Units within NHS hospitals.

15. No action is taken to verify identity prior to allocation of new NHS numbers or when accessing NHS services. Consequently there may be opportunities for a person (eg a drug abuser who is seeking repeat prescriptions to register with a GP) using a false name or to register with more than one GP. However NHSCR is designed to pick up such duplications. There are also opportunities for health professionals to create bogus identities to increase their level of remuneration which is based on the number of registered patients on their books. Health Authorities are required to visit GPs every 3 years to carry out a 10% check on patients' records to ensure that it is still appropriate for them to be on the patients' list.

Construction Industry Scheme (CIS) cards

16. Self-employed subcontractors working within the construction industry must register with the Inland Revenue to be part of the Construction Industry Scheme. They are issued with either a card or a certificate which they need to show to their contractor before they are paid for the work they do. The contractor must not pay the subcontractor without sight of the card or certificate since this will determine whether the contractor can pay him before or after deduction of tax. The purpose of the scheme is to ensure that all those working in the construction industry are registered with the Inland Revenue and are paying the right amount of tax and NICs.

17. There are three types of card and certificate – a CIS(4) which entitles the subcontractor to be paid after a deduction of tax and CIS5 and CIS6 that entitles the subcontractor to be paid before deduction of tax. To obtain a CIS6 the subcontractor must pass three tests: business (whether they have stock, plant etc.), turnover (whether they make in excess of £30K over 3

years) and compliance (whether they pay their tax in full and on time). There are two types of CIS4 cards: a temporary card (CIS4(T)) which is valid for three months and does not carry a NINO; and a permanent card (CIS4(P)) which should carry a NINO. Any NINOs supplied are validated by production of a NINO numbercard or by faxing IR NICO for a trace on DCI.

VAT registration

18. Traders register for VAT by completing a VAT1 form. This form has recently been revised and now requires applicants to provide more information such as their NINO and personal details of directors. HMCE has devised a risk assessment sheet specifically designed to target traders suspected of Missing Trader Intra Community fraud, which is the department's highest VAT fraud priority. All applicants for registration whose score exceeds a certain level are not registered immediately but their application is referred to a Central Co-ordination Team (CCT) who carry out a number of further checks against a variety of internal and external databases to establish the bona fides of the application. About half are cleared by the CCT for registration at this stage and the majority of the remainder are referred for a visit.

19. HMCE receive 200,000 applications for VAT registration a year. After 12 months of operating risk assessment, over 1000 applications have not been pursued to full registration.

20. HMCE is currently developing an electronic trader register which will provide a single data repository containing all information about a trader. To assist the registration process and improve the verification and authentication of traders a data matching tool is being developed as part of the new system. This will match data provided by traders seeking to register for VAT against both internal and external databases. It is hoped to replicate the department's' current manual systems, including risk assessment, as a minimum.

21. A new VAT registration form was introduced for all applications from April 2002. The additional information contained in this form enables a greater variety of corroborative checks to be carried out to verify and authenticate traders.

Electoral register

22. Inclusion on an electoral register is based on information provided by the head of each household annually about people living at that address who are eligible to vote from October that year. From February 2001 the provision of rolling registration came into effect. This enables people who move during the year to register in their new area. They are asked to provide details of their previous address to enable their details to be removed from the register covering their previous address. However details of anyone already recorded at the new address are not necessarily deleted. Credit reference agencies place great reliance on the electoral register to verify identity. A person's credit rating is greatly influenced by the length of time they have appeared on the electoral register at one address. Yet Local Authorities do not take any action to verify the information they are supplied with from each household apart from occasionally when a Registration

Officer's suspicions are aroused by a rolling registration entry. It is therefore easy to create false or multiple identities or for the same person to be on more than one register.

23. The position in Northern Ireland differs somewhat from the mainland. There is a strong perception in Northern Ireland across both communities that there is a problem with electoral fraud, in particular personation, where individuals use multiple identities to vote more that once. There is no robust evidence for this, (there have been one or two arrests and very few prosecutions) but the perception of a problem has driven rather different legislation and policy from the rest of the UK. Since 1989 voters have had to produce proof of identity when voting by providing documentation from a list. Legislation designed to tighten security of identity recently gained Royal Assent. Measures to be introduced include:

- when registering on the electoral roll, the Electoral Officer will collect full name, date of birth, signature and NINO (if they have one). This information will be available to check validity of voting, and the Presiding Officer at the Polling Station will be able to ask a person's date of birth before issuing a ballot paper;
- an electoral identity card to be issued free of charge to those people entitled to vote but who might not otherwise have satisfactory proof of identity. In due course, all non photocard documents will be removed from the list of acceptable proofs of identity.

Immigration

24. EC nationals (almost 77 million a year) enter the UK with only minimal examination of their documentation at the points of entry. The documents of nationals from outside the EEA are subject to greater scrutiny but provided there is no breach of immigration rules their passports are stamped specifying the terms of their entry into UK. The majority are given leave to remain as a visitor for up to 6 months but the volume of traffic (12 million people in 1999) makes it impractical to keep records and consequently IND cannot check if people overstay or not.

25. Applications for extensions to the period of leave to remain can be made either by post or in person. Personal applications allow IND staff to check the identity of the applicant against their passport whereas this is not the case with postal applications. In 2000 around 11,000 applications for an extension or settlement were refused, while more than 230,000 were granted.

26. In 2000 IND received over 80,000 applications for asylum. Most asylum seekers produce no documentation to confirm their identity and it is often impossible to establish from which country they originated. Details of all applications for asylum and case progress and outcomes are recorded on a database, Asylum Casework Information Database (ACID). To prevent duplicate applications for asylum all applicants must provide fingerprints. IND staff are now able to cross match against a database containing 400,000 fingerprints, including all those who have applied for asylum and been refused. Fingerprints are removed from the system once asylum is granted.

Company Registration

27. Companies House is a registering body: it is not required, nor has it the power, to make in-depth checks on applicants wishing to set up companies. Applicants have to provide details of their current address (although for “corporate directors” (i.e. directors of several related companies) this does not have to be a residential address, and under new regulations it will soon be possible for directors of single companies to apply not to give their residential addresses, if they could prove they were under threat).

28. Companies House believes that the UK is the easiest place to become incorporated. Some countries require directors to present identity cards to register. Companies House is looking at possibilities for giving directors unique identifiers.

ANNEX D: MAJOR NATIONAL DATABASES IN THE PUBLIC SECTOR

Database	"Parent" organisation	Coverage	Number of records
DCI	DWP	UK; all people allocated a NINO since 1948, when the scheme was set up.	82 million (including 13.5 million records for people who are dead)
NHSCR	GRO(E&W)	England, Wales & Isle of Man; all people registered with an NHS GP when the system was created in 1991 plus people born since, or registered with a GP for the first time after 1991.	66.8 million (including 6 million records for people who are dead)
NHSCR Scotland	GRO(S)	Scotland	6 million (includes deaths since 1992)
Vital Events	GRO(S)	Scotland (Computerised searchable index, with digital images of all records capable of viewing by Government Depts via GSI to be available by mid 2003).	All births, deaths and marriages recorded in Scotland since 1855.
UKPS	UKPS	UK; people who currently hold a UK passport, or have held or applied for one.	55 million (includes 12 million with digitised photograph and signature)
Driver Licensing Database	DVLA	Great Britain; all people who have gained a driving licence since 1970 and most who have ever held one	44 million records (includes unknown number for people who are dead but DVLA not notified)
Electoral register databases	Local authorities	UK; People who will be 18+ in the coming year, who are eligible to vote and who register. The register is actually an amalgam of 480 local databases, rather than a single entity.	44 million records (includes small number – c.11,000 – of UK residents living overseas)

ANNEX E: GLOSSARY OF TERMS

ACID	Asylum Casework Information Database – IND database recording details of all asylum applications
ACPO	Association of Chief Police Officers
APACS	Association of Payment Clearing Services
Attributed identity	The components of identity that are given at birth i.e. full name, date and place of birth etc.
BASIS	Benefits Agency Security Investigation Service
BFIS	Benefit Fraud Investigation Service
Biographical identity	Life events and how a person interacts with society
Biometric identity	attributes that are unique to an individual i.e fingerprints etc.
CIFAS	UK's Fraud Prevention Service
CIS	Construction Industry Scheme
CPS	Crown Prosecution service
CRB	Criminal Records Bureau
DCI	Departmental Central Index – DWP's database
DfES	Department for Education and Skills
DPA	Data Protection Act
DPTC	Disabled Persons Tax Credit
DSA	Driving Standards Agency
DVLA	Drivers and Vehicle Licensing Agency
DWP	Department for Work and Pensions
ECHR	European Convention on Human Rights
EEA	European Economic Area
e-ID verifier	Automated authentication system run by Equifax, which uses data as the basis for a series of questions to which only the applicant should know the answer
ELVIS	Events Linkage Verification Information System, GRO(E&W) database

Equifax	credit reference agency
EU	European Union
Experian	credit reference agency
FFIN	Financial Fraud Information Network
FSA	Financial Services Authority
GRO(E&W)	General Register Office for England and Wales
GRO(S)	General Register Office for Scotland
HMCE	HM Customs and Excise
HMT	HM Treasury
HRA	Human Rights Act
HRDC	Human Resource Development Canada – Canadian version of DWP
Hunter	Software developed by MCL Ltd. to cross-check applications for consistency against themselves, against other applications on the same database, or against a national database
ID	Identity
IIFF	Interdepartmental Identity Fraud Forum
IND	Immigration and Nationality Directorate
IoP	Instrument Of Payment
IR	Inland Revenue
JMLSG	Joint Money Laundering Steering Group
JoFITs	Joint Fashion Industry Teams
JoSETs	Joint Shadow Economy Teams
LCD	Lord Chancellor’s Department
LSLO	Legal Secretary to the Law Officers
LTAF	London Team Against Fraud
MTIC	Missing Trader Intra Community Fraud
NASS	National Asylum Seekers Support

NCIS	National Criminal Intelligence Service
NERA	National Economic Research Associates
NHS	National Health Service
NHSCR	National Health Service Central Register
NICs	National Insurance Contributions
NIFU	National Identity Fraud Unit
NINO	National Insurance Number
PICT	Prevention and Investigation of Crime Tool
PIN	Personal Identification Number
PinS	Professionalism in Security
PIU	Performance and Innovation Unit
PSA	Public Service Agreement
SFO	Serious Fraud Office
SIN	Social Insurance Number (Canada)
SNAP	Secure NINO Allocation Process
SSN	Social Security Number (USA)
UKPS	United Kingdom Passport Service
UV	ultra violet
VAT	Value Added Tax
VF	Verification Framework
VIS	Verification of Identity System – Dutch database of lost and stolen identity documents
WFTC	Working Families Tax Credit

253317/0702/D4

Economic and Domestic Secretariat
Cabinet Office
70 Whitehall
London
SW1A 2AS
Telephone:020 7276 6097
E-mail: lsydney@cabinet-office.x.gsi.gov.uk
Web address: cabinet-office.gov.uk/cabsec/2002/idfraud.htm

Publication date July 2002