

THE VALUE OF IDENTITY AND THE NEED FOR AUTHENTICITY¹

Gareth Jones and Michael Levi²

DTI Office of Science & Technology Crime Foresight Panel Essay, for *Turning the Corner*, December 2000,

Introduction

1. This is an essay on identity: how it is formed, how it is used, how it can be abused, and how we might reformulate it to fit in with the era of commercial relationships between strangers in the private and the public sectors. In the early decades of the 21st century, we need to show who we are to obtain a bank account (to make it harder to launder proceeds of crime as well as to reduce fraud); to get credit or even to pay money from our bank and other accounts; to gain access to private and, increasingly, public facilities; and sometimes to get into our own homes and those of our friends, as fear of crime – whether based on accurate or inaccurate risk data - drives some of those who can afford it increasingly towards life in gated communities. Identity is important because people can do harm by pretending to be someone they are not: this harms not only the businesses and the private individuals who lose money and the would-be secure establishments that are ‘invaded’ against their will, but also the people whose identities are ‘borrowed’, whose reputation and credit ratings are harmed and who can be, in a sense, victims of miscarriage of justice because the impostor is taken to be them. Opportunities for crime that make use of impersonation are widespread, but by no means all of them are taken advantage of by criminals, whether they be career criminals for profit, hackers for play, or those practising industrial and/or political espionage. Otherwise, such crimes would be far more common than they are. But as corporations, governments and individuals make greater efforts to protect their property and their personal security, the closing off of other opportunities may increase the temptations of impersonation. As in many other areas of contemporary life (such as travelling by train), the ratio between risk and its actualisation can vary over time, depending on (a) the skill set of current and potential offenders and (b) the measures taken by a range of potential victims to protect themselves.
2. The way that the economic losses arising from impersonation are distributed depends on the contractual arrangements (in for example, our credit card contracts between cardholder, retailer, and card issuer/acquirer), but the consequences of having a bad credit rating caused by others without one’s knowledge or even the feeling of having one’s identity ‘alienated’ can be a major source of fear of crime, which reduces the quality of life and inhibits e-commerce. Society and commerce depend on trust, and assurance of identity is one important facet of that trust, though it simultaneously indicates distrust that people might not be who they claim to be. So this is, we believe, an important topic that goes beyond the creation or inhibition of economic crime opportunities – significant though that is in itself – and touches issues such as the sense of integrity of self, which is disturbed profoundly by impersonation. As e-commerce develops and face-to-face commercial and even working relationships become progressively (or, according to some, regressively) rarer, the need to demonstrate our identity to strangers will become increasingly commonplace. In this essay, we have no space for comprehensive coverage of the issues, but we will pluck out and develop some of what we believe to be the key themes.

3. In order to understand how an individual's identity is initially formed, where it is referenced, and the methods by which it can be attacked, it is first necessary to record the principal events in life through which an identity is established. This goes to understanding 'who' we are, and is key to finding the starting point for retrospective scrutiny, should the validity of the identity be subsequently queried. Of course, 'who we are' is only one facet of the identity jigsaw, 'what we are' – our various biometric codes- are other reference points distinguishing ourselves as unique individuals, though they serve to confirm or refute an identity already established (otherwise there is nothing to check against).
4. The earliest point in an individual's life at which they are identified, is parental notification to the hospital / mid-wife of the newborn child's name. Subsequently the parents provide the Registry Office with information about themselves and their child, some of which is recorded on a letter from the hospital at which the child was born. The parents are provided with evidence of the child's birth in the form of an 'Extract of an entry in a Register of Births' (what is commonly called the birth certificate), together with an abbreviated certificate of birth. The latter details the child's name plus 'event' details, but no information about the parents. These certificates are uniquely numbered. Subsequently the parents are given a National Health Service Preliminary Medical Card detailing the child's forenames, date of birth and sex, plus their National Health Service Number, compiled from information upon the birth certificate. The child's identity is now formally established, and unless later in life the child as an adult elects to change their name, all subsequent references to that person are uniquely linked to their newly formed identity. As they progress through formative years, their education, qualifications, employment, interaction with Government and commercial bodies, retirement and ultimately their death, these life events are capable of being linked together.
5. The exceptions to the usual process of registering a birth include adoption and immigration. In the case of adoption, a similar but necessarily 'concealed' process occurs. Immigrants will generally possess a birth certificate / identity card / passport issued by the country of which they possess citizenship.
6. As the individual matures, provided that they are living in Great Britain and their parents are in receipt of child benefit, they will be issued with a National Insurance Number shortly before they reach the age of 16. Should automatic registration not occur, they can subsequently register as an adult. About a third of all new registrations are non-automatic adult registrations. Despite being an obvious method of referencing an identity, the National Insurance Number carries little commercial credibility because it cannot be easily checked for validity, and the National Insurance Number card carries none whatsoever as a 'proof' of identity.
7. Retrospective changes cannot be made to a registered birth. Individuals over the age of eighteen who want to change their name have three options – change of name by deed poll, statutory declaration, or advertisement. Deed poll changes under the age of 18 require the written consent of the parents. None of these methods permit the retrospective issue of a birth certificate in the changed name, nor gender (in cases of gender re-assignment), and new bearer documents such as driving licences and passports will not prima facie allude to this life event. Once the previous identity has been renounced, it can only be exposed at the discretion of the first party by production of the deed / statutory declaration, or occasionally by reference to the London, Edinburgh or Belfast Gazette, in which the change of name may be published. The publication of change of name either by deed poll or

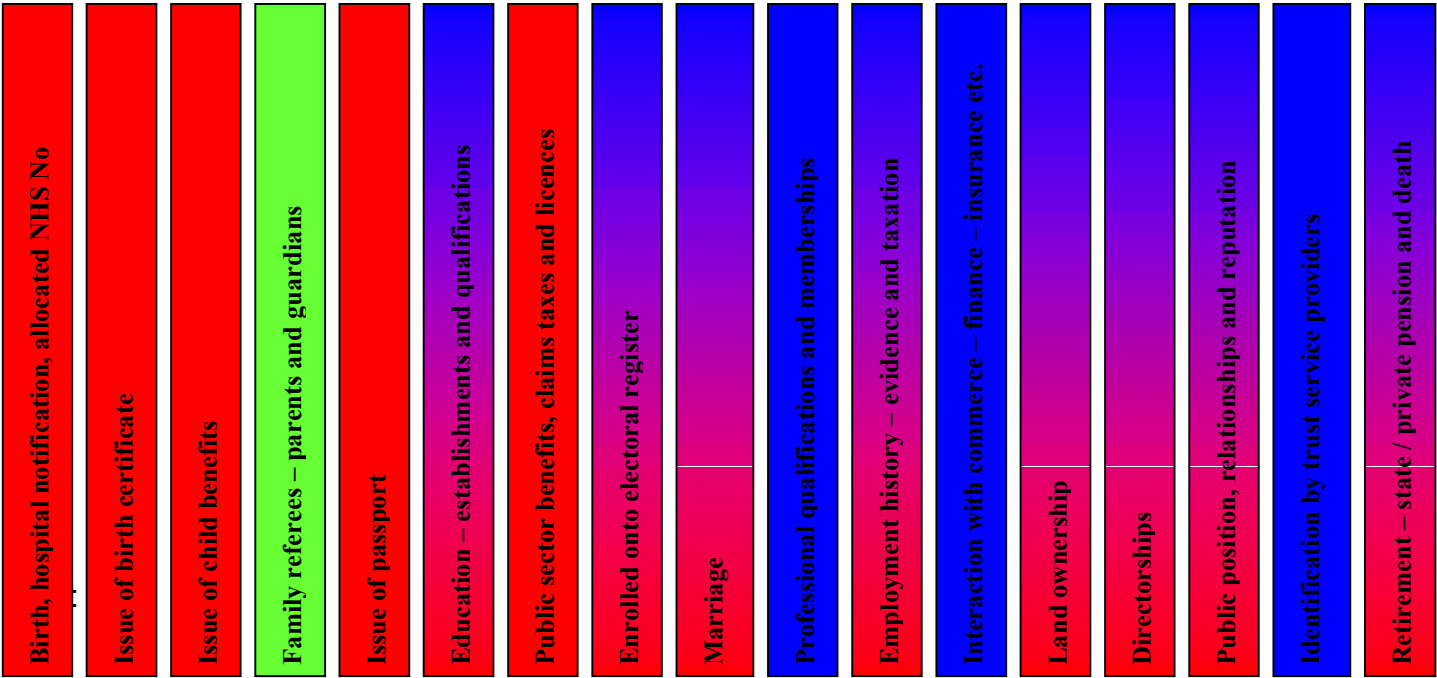
statutory declaration is *not* mandatory, a fact that is ideal for individuals who do not want to draw attention to matters affecting their credibility such as convictions, but is sympathetic to individuals that have changed their name for more personal reasons such as gender re-assignment, fear of violence etc. However, it draws a serious question mark over the reliance placed upon bearer documents when used in a cumulative fashion to evidence identity in the commercial sector.

8. Individuals are not the only legal identities in the UK. Identities can be corporate in nature - companies are separate legal entities to their officers. Whilst a national numbering system distinguishes one registered company from another, problems emerge when individuals adopt 'trading names', and these non - registered businesses appear to have a corporate identity, but for the purposes of identification should be considered to be individuals by name. Whilst larger companies can be easily identified by their public trading history, smaller ones have little if any identity credibility, and are properly identified through their officers' identities. (Fraudulent companies can of course seek to simulate the identity of large, famous ones to give themselves a spurious credibility.)
9. The features of an individual's identity can be classified into two groups. The first is 'attributed' identity, given at birth and includes full name, date of birth, time of birth, place of birth, parents' names and address. The second group is 'biographical identity'. This relates to interaction between the individual and third parties as they move through life. Such references are held in both the public and private sectors. The value and purpose of classifying the elements of an identity in this way is found later on, where the issue of identity fraud is considered in depth. All individuals have an attributed identity, but other than educational references, minors and students have thin biographical identities in the commercial sector, as do certain other minority groups such as vulnerable persons and immigrants. This data shortage often occurs also for people who have lived abroad and have no UK public data or credit history references.
10. So identity is not just illustrated by birth certificates and other 'attributed identity' characteristics. Whereas an original birth certificate is persuasive in showing where we have come from and who we are, the diagram overleaf shows that there are other 'biographical identity' life event references that record the existence of identity that are more accessible. The diagram demonstrates that third parties looking to prove identity do not need to look too far back in time towards the event of birth to find reliance. There is a wealth of life events that follow the registration of birth that are persuasive in the chosen process of identifying an individual. It can be seen that as the individual ages, there is a distinct shift in the currency of the identification evidence from the public sector to the commercial sector. Also, the volume of evidence within any of the life event blocks will vary from person to person.
11. At this stage what is shown in Table 1 is just the availability of life event evidence and in which sector it is referenced - public and / or commercial. This indicates that comprehensive evidence of identity is available within or from both sectors. In general, the evidence flowing from these life events is only accessible with the individual's consent. Non-consensual availability of cross sector life event evidence is only legitimate through legal exceptions and orders. This separation of life event evidence supports the individual's right to privacy, and leaves the choices surrounding disclosure entirely within their gift. The measurement of that life event evidence and the processes that go towards ensuring the individual has a right to use them are considered later.

Table 1.

‘Progressive Life Event Diagram’

Key - identity reference owned by or available through:
 Public sector: **red**
 Commercial sector: **blue**
 Both public and commercial: **red and blue**
 Family: **green**



Approximate time line of ‘life events’ – some are repetitive, some concurrent with existence of life. →

13. The basis upon which life event evidence is found includes a mix of media that has evolved from centrally and locally held registers to copies of the same on microfiche, paper documents, publications, individual’s memory and attestation, and finally – in great abundance- data. Traditionally, identities are compiled from the starting point – the birth certificate – but this is increasingly redundant. In a new age of greater interactions that are *not* face to face, with higher expectations of instantaneous responses for customer service, and new thinking on matters of establishing trust, the fact-on-computer usually characterised as ‘data’ is king and provides for significant personal and commercial advantages for those able to leverage them. The following is a list of persuasive data types that can be used in some way to establish identity, and for fraud prevention aims that are necessary in such a process. The data items or ‘characteristics’ within these are often very detailed, and sufficiently so to find consistency and reliance, or expose inconsistencies and the risk of fraud. Typically the data types include

- Electoral register entries
- Mortgage account information
- Property ownership and leasehold
- Credit account and other financial facilities information
- Insurance policies (motor from 2001) and claims (motor and home)
- Marriage and financial associations

- Previous addresses
- Telephone numbers – fixed and mobile
- Employment information from applications for financial services
- Directorships
- Satisfied court judgements
- E-mail address
- Higher educational qualifications
- Forwarding addresses – re-directions
- Previous address linking
- Previous authentication events
- Payment systems facilities – debit / credit / cheque / charge / virtual wallets etc.
- Prima facie fraud risks at individual and address levels – suspect and victim

14. Other non-personal data can also be accessed to visualise the individual from their name and address. It does not prove identity, but offence profiling by socio-economic and geo-demographic features suggest that it is persuasive in calculating an individual's data provided identity score (see later). For many years, commerce has appreciated the benefits of sharing data to prove / disprove identity, and some of these data types are now accessible together through a single database call. Thus if paper referenced identity is the champion of old, the new challenger is the data orientated alternative. The joust as to which carries greater probity is considered in a subsequent section of this paper, and is for the applicant to choose from, for the law provides that they can decide whether to consent to having their application dealt with on an electronic basis, or fall back on paper alternatives to prove who they are.

15. But politics and the control of the information society are subject to mood swings and media-fuelled panics, as the reactions to the BSE crisis and the hacking into Microsoft's own source codes illustrate: we are not good at coping with risk rather than certainty in public settings, even though business, police and the intelligence community have to do precisely this every day. Reactions to identity cards – commonplace in many other European countries – illustrate this. The outcome is that UK citizens have necessarily to be identified from a range of evidence of life events, rather than a single compelling (relatively) secure identity reference.

16. The systems and processes used to establish identity are common in as much as they can be passed or failed depending on how much evidence can be accumulated by the individual to support their identity. Both the issue of a passport and the issue of a driving licence require a certain number of 'proofs' of life events to corroborate the information given in the application form. In the commercial sector, two proofs of identity and address from separate sources are required before most financial facilities can be opened and activated. This is a 'cumulative' concept, and one that is lacking in refined qualitative assessment. Individuals accumulate evidence of identity – proof documents, and if the number and type of these proofs meets the required threshold, the individual is deemed identified. This of course is complete tosh, not just because of blatant 'function creep', but also because it fails to deal with the fundamental problem of how to properly demonstrate identity in the UK – namely the unabated fraudulent attacks upon public sector systems, and the entire lack of feedback of fraud risks to parties that blindly rely on pseudo identity documents issued by them. In recent years inroads have been made to counter fraud and abuse, but the problem has existed for decades, and is unlikely to be tackled effectively. In short there is no public

sector silver bullet. This subject is considered in more depth under the heading 'Evidencing Identity'.

Identity Fraud Explained

17. Identity fraud can arise from the loss or theft of physical identity documents, from their improper taking from existing official and commercial files, and from mere simulation of being the person. There are five basic styles of personal identity fraud, though there are many variations within these forms. There are in addition four types of commercial identity fraud. The following list is compiled from public sector and commercial sector experience, interviews, and case analysis.

18. *Current Address Impersonation*. This is committed where the victim is:

- still resident at their current address, or
- still the owner / lessee but absent on extended holiday / working abroad, or
- the immediate previous resident of an address, or
- in the same family as the suspect or collusive with the fraudster, or
- has lost or suffered theft of evidence of identity documents

19. The fraudster will operate in one of a number of ways. In each case they will use the exact name of the resident occupier, and usually they know the correct postcode for the address. They will not usually be aware of all of the occupier's attributed identity characteristics - date of birth, and other low level detail such as place of birth, mother's maiden name, and even less of the biographical identity features - time at address, previous address, correct employment details. More practised fraudsters may obtain the victim's date of birth through research, typically where determined and organised fraudsters infiltrate positions of trust in the public sector. They may have access to detailed information about individuals' biographical identities, and this information may extend to their National Insurance number. Here the primary aim is to commit benefit frauds, but though studies of multiple criminality are only in their infancy, there is evidence to suggest that many criminals commit a variety of offences that relate to their skill and contact set, so the public/private sector divide is artificial.

20. Where the victim is still resident, they often use the Post Office re-direction service to collect identity evidence and details – such as bills, and have contracts into which they have fraudulently entered re-directed to their 'safe' address. This 'safe' address is often low quality residential premises or a commercial accommodation address.

21. Where the owner / lessee is absent but still connected to the property, typically where they have moved out for the medium term, the fraudster will be in a better position to copy their identity. They will have a greater understanding of both the low level attributed identity characteristics, and often the current biographical identity characteristics such as employment details etc. Because they are actually resident, they will be able to beat certain off line fraud prevention measures – such as home telephone checks and be able to support their new identity with genuine documents.

22. The third sub type of current address impersonation is where the victim was the immediate previous resident. This 'move in' type of fraud is very similar in style to the 'absent but still

connected' type – above. Typically the fraudster moves into an address – usually rented accommodation, establishes the identity of the previous occupant, and copies it. Post that has not been re-directed is used to gather information about the identity, and to provide documentary evidence – typically utility bills.

23. The fourth sub type is 'in family' and 'collusive' impersonations. The first is where the fraudster copies the identity of another family member – very often one of the parent's identities, and appropriates documentary proof – typically driving licence, bills, statements, birth certificate, to corroborate their identity. 'Collusive' is the term used where the accomplice allows their identity to be used by a third party. In both cases, the fraudster will possess knowledge of the attributed and biographical identity characteristics, and be able to support these with documentary evidence.
24. The final sub type is where the identity is copied from lost or stolen documents. The fraudster uses these in conjunction with a re-direction as the victim is still resident at the address shown on the documents, or, uses the documents in conjunction with a previous address impersonation (below), or takes a chance by not installing a re-direction on the home address. Invariably the employment details will be false, and the services of accommodation addresses are utilised to mask the fictitious nature of the employment.

Previous Address Impersonation.

25. There are essentially two methods. The first is where the fraudster tells the truth about their attributed identity details – they are physically who they purport to be, but lie about their address history. They utilise available public data to establish the address of an unwitting third party of the same name, they then use the third parties current address as their previous address on the application form.
26. The second method is where they establish the identity of an unwitting third party and use their name, usually the third party is resident in reasonable accommodation, and use the third parties identity as if they have recently moved from their current address, to a (typically) low quality new address. They will use stolen documents to support their identity, as these will tie in with their false circumstances – the illusion that they have recently moved house, or if stolen genuine documents are unavailable, forge replacements.

Deceased Impersonation.

27. This has two styles – 'elderly' and 'child'.

- With 'elderly' deceased impersonation, the fraudster establishes that a death has occurred – usually from local obituary columns, probates disclosed by estate agents to fraudsters acting as prospective house buyers, and fresh graves in cemeteries. It is simple to find out the exact attributed identity details of the deceased. They then use these in conjunction with a current or previous address impersonation and invent a biography. It is rare for the fraudster to obtain official documents, such as passports, to support their identity, as the age discrepancy is usually enormous. Where the elderly deceased victim's property is in the hands of executors, the victim's residence can be used as if they are still living there.

- ‘Child’ deceased victims of impersonation are found by the fraudster searching for suitable identities in graveyards. The identity of a child is more prized because there will be little chance of conflict with established data. For example, there is unlikely to have been a passport, and certainly not a driving licence issued to them. Thus a fresh application will not seem unusual. The next step is to apply for a copy of that deceased child’s birth certificate, and use this in a subsequent application for a passport or driving licence. This is the source of the term ‘breeder document’. The birth certificate is the turnkey or precursor to obtaining a passport, the passport can be used to support an application for a driving licence, and so on. The fraudster will invariably establish the identity in the commercial sector by opening up utility accounts, opening accounts for certain types of financial service and even take a driving test to obtain a ‘full’ licence in a false name.
28. The evidence supporting the fraudulent use of a deceased child’s identity will therefore be genuine paper proofs, and potentially some recent commercial data. Given the newness of the identity, the fraudster will often use a ‘previous address impersonation’ method to establish an address history. In the alternative, they will ‘sleep’ the identity for up to a year, enrol on the electoral register and create the illusion that they were resident at the address for longer than is in fact the case.
29. *Developed identities.* As an alternative to copying, or partially copying a genuine identity, the fraudster can develop a credible fictitious identity. Historically this has been done by:
- abuse of public sector services – such as the Driver Vehicle Licensing Agency
 - change of name by deed poll
 - establishing a financial background based on untested lies and paper proofs that carry no real credibility as identity documents – such as utility bills.
30. By changing an address and then in a separate episode changing the name on a driving licence, a genuine public sector bearer document can relatively easily bear the details of a false identity. The introduction of photo card driving licences and the new fraud prevention measures to check the identity of the applicant, suggest that this sort of fraud will be reduced. However, these measures are not infallible, and for collusive impersonations, it is easy to get photo card replacements for non-photo card paper licences, with the fraudster’s photo on the new document. In time, this type of fraud risk will reduce further.
31. It is acknowledged that the fraudster will have to take the risk of exposing their facial features to subsequent investigation, but identification from photographs has not historically been a reliable method of establishing the true identity of the offender.
32. Transactional impersonation. This involves fraudsters presenting themselves as the bearer of (usually) a stolen or mislaid payment device such as a debit card, credit card, or cheque. They may alter the signature of the real operator of the account, but this is not as prevalent as leaving the signature intact, and practising the signature to pass off the forgery as being genuine. Over recent years the explosive growth in the use of counterfeit cards has magnified this type of impersonation, and is highly common for a variety of reasons such as the ease of counterfeiting the plastic, the availability of such counterfeits to criminal gangs, the availability of magnetic card readers to clone the details of the victim’s card to the counterfeit, and the inability of systems to adequately guard against this type of behaviour.

33. Transactional impersonation is analogous to other 'presentation' types of identification fraud seen in areas beyond financial services. This includes the presenting of stolen or counterfeit cards and passes which create the illusion of trust or permit access to premises. The impersonations of Police through fake warrant cards, utility officials and such like professions through work identity cards feature regularly in offences of artifice burglary. Thus the issue of identity fraud is not limited to impacting upon commerce alone.
34. *Commercial identity fraud.* There are several ways in which companies can be attacked, such as by surreptitiously registering new bogus Directors and by transferring the company's registered address, or copying its identity by loading fake web sites to the Internet that look very similar to the genuine company's site, with the aim of collecting information about an individual and their payment card, with which to subsequently commit card not present fraud. The victim is both the individual that has unwittingly given their identity away to the fraudsters, and the genuine company who have lost a genuine customer, and through press exposure may lose many more potential customers through a lack of trust and loss of reputation.
35. Finally in the real world, some companies are purchased by fraudsters who give false names, dates of birth and addresses, thus committing identity fraud at two levels. The company is genuine in its registration, but not in its trading intent. Its Directors have used false identities to avoid subsequent tracing activity from officials and creditors.
36. The impact of identity fraud upon business is substantial. The following tables of information have been provided by those organisations that collect reliable statistics on the extent of identity fraud. Together they represent the lions share of commercial victims, though there will always be companies that do not contribute data, so should be viewed as the lowest reliable figure, rather than a true full blown picture on the extent of criminality in this area. These organisations are CIFAS – 'The Fraud Avoidance System' and APACS – the Association for Payment Clearing Services.

37. CIFAS Filing		
Year	Cat 1	Cat 2
1988/90	2,745	6,831
1991	849	4,481
1992	474	3,895
1993	365	4,107
1994	1,483	8,715
1995	521	7,140
1996	1,132	13,250
1997	2,231	17,847
1998	1,902	16,810
1999	2,172	17,676
2000 (to Aug)	5,867	14,410
Total	19,741	115,162

Category 1 - False identity at real address

Category 2 - Victim of impersonation

Table 2 – provided courtesy of CIFAS

Application identity fraud in the commercial sector

These figures are drawn from the CIFAS system's database.

They show the number of addresses where their members have filed CIFAS loadings – which command a high probability of proof of fraud.

CIFAS state that false identity fraud is increasing dramatically, and project that with the future growth of remote account opening, fraudsters will use the new channels of introduction to their advantage.

The value of all CIFAS loadings has grown to a 1999 figure of £165.38m and year 2000 Jan to Aug of £120.03m

	Other	Card not Present	Application fraud	Counterfeit	Mail non-receipt	Lost and stolen	Total
1991	1.6	0.4	2.0	4.6	32.9	124.1	165.6
1992	1.0	1.3	1.4	8.4	29.6	123.2	165.0
1993	0.8	1.6	0.9	9.9	18.2	98.5	129.9
1994	0.5	2.5	0.7	9.6	12.6	71.1	96.9
1995	0.3	4.6	1.5	7.7	9.1	60.1	83.3
1996	0.5	6.5	6.7	13.3	10.0	60.0	97.1
1997	1.2	12.5	11.9	20.3	12.5	66.2	122.0
1998	2.3	13.6	14.5	26.8	12.0	65.8	135.0
1999	3.0	29.5	11.4	50.6	14.7	80.1	189.4

Table 3
**APACS
Fraud Losses
in £m**

Note recent exponential growth in card not present and counterfeit fraud

38. The impact upon business of these offences is felt in the form of cost. Cost in terms of loss of funds, cost in the deployment of resources to administer the problem, and in the case of transactional impersonations, cost through the loss of confidence that the real account opener has in the facility, which they may then treat with caution or abandon all together.

39. The impact of the fraud does not rest solely with the commercial victim. The true owner of the identity – who is invariably unaware of the iniquitous activity being committed in their name - has an administrative mess ahead of them to resolve. They have to disassociate themselves from the offences, clean their data records to reflect their non-involvement in the frauds and potentially erroneous default notices, and organise for the re-issue of documents and cards. They may have to provide witness statements to Police, attend court proceedings, and this can go on for many months and even years. Thus such persons that have the misfortune of initially suffering the theft of their wallet or handbag, or compromise of its contents, or just bad luck in being picked by a fraudster as a well-heeled victim, then suffer the secondary impact of crime in the form of fraud.

40. Where the identity copied is that of a deceased child, typically to obtain passports, the consequences include not just illegal immigration but also possible distress to the family if the authorities call on them.

41. So what are the motives for changing identity for both criminal and genuine purposes? Broadly speaking the motives include:

- theft and deception in acquisitive crimes
- hiding of unattractive antecedents – crimes and civil embarrassments – bankruptcy. The future availability to employers of information about criminal convictions of new and existing employees, could well encourage convicted persons to change their identities more often
- obtaining information about another for use in blackmail, court proceedings, or press revelations – the case in which the tax details of Lord Levy were deceitfully obtained from the Revenue in 2000 is an example of this
- citizenship and ability to unlawfully remain in the country
- legitimate victim and witness protection from violent and determined offenders
- legitimate changes of forename following gender re-assignment or change of surname that through the development of slang terms that are unattractive and embarrassing.

42. It is now clear that our identities are under threat. Our life events are linked to them, and so are our rights, privileges and rewards. Our status in society is found from our identity, as is

our credibility and professional repute. Attacks upon our identities are invariably damaging, difficult or protracted to resolve, and lack transparency – the fraudster’s use of the identity may be short lived or protracted. Against this the legitimate changing of identity is subjectively justifiable, but a reasonably rare event. Here the first party drives the process, and the impact upon them of the name change is not felt or negligible.

Evidencing identity

43. There is no standard way of identifying individuals in the UK. However, newer ways of identifying individuals have recently emerged, and the validity of these in terms of probity and commercial functionality are contrasted against traditional methods.
44. The modern thinking on identity is that two separate equations should be satisfied. The first is to show that the individual actually exists. The second is to show that the applicant is or is not the individual they say they are.
45. Do the traditional methods of identification do this? The starting point for this exercise is to examine the current life event occasions that require identification, and the evidence of identity that has to be produced for that life event be recorded.

Life Event	Evidential Proof of Identity
Issue of original birth certificate	Letter from hospital Marriage certificate (optional)
Issue of certified copy of birth certificate	None
Issue of original NHS medical card	Automatic following birth registration
Knowledge of NHS number	None – derived from original birth certificate detail
Issue of National Insurance number Similar processes exist for proving identity for other forms of social security	Automatic following birth registration and provision of child benefit Adult registration: Face to face interview to provide historical information from age of 16 onwards for verification, plus proofs of identity: Either a passport, foreign identity card or original birth certificate, if birth certificate is a copy additional proof such as marriage. In absence of preferred proofs, at least two of the following: Travel pass with photo, SAL for asylum seekers, Form GV3, certificate of identity issued by H.O., Police registration document, full driving licence, local council rent card or tenancy agreement, life assurance policy, recent wage slips, Trade Union membership, cheque book, cheque guarantee card, bank statement, building society pass book, recent household bills, H.M. forces papers, store and credit cards, IS KOS EX.

Marriage	Passport or birth certificate for both parties, if previously married divorce certificate or evidence of previous partner's death
Issue of Driving Licence	Current and original passport, or Birth / adoption certificate with referee signature, plus photograph If name different, marriage certificate, divorce certificate or deed poll / statutory declaration
Issue of Passport	Renewals where applicant is over age of 16 at issue of original passport, submission of original passport only plus photo Renewals where applicant was under 16 when the original passport was issued require the original passport and countersignature from referee plus photo. New applications require a Birth certificate – original or certified copy. If the name has changed, original marriage certificate, divorce certificate or documentary evidence of change of name by deed poll / statutory declaration. More detailed procedures and options for proving identity exist for persons born before 1.1.83 outside of the UK, and for persons born abroad after 31.12.82. UKPA form IL/03/01 provides details.
Enrolment upon electoral register	None
Claim to enrol upon electoral register	Any proof of residence for relevant period (pre 10 th October) such as a tenancy agreement
Notification of Appointment of Directorship to Company House	None
Opening new utility account	None
Request for re-direction of mail	Two proofs in the name of the person submitting the request and addressed at their old address, same criteria for different surnames. One proof from each list. If a cheque is used to make payment, only one form of identity from List B. Separate arrangements for children under the age of 16.

List A	List B
Pension / Benefit book	Driving Licence, if photocard type, counterpart has to be produced
Cheque guarantee, debit or credit card	Council Tax payment book
Bank / Building Society Book	Two recent utility bills
Passport	Recent Bank / Building Society statement
National Savings Book	Council rent book
Store Account card	TV licence
Cheque book	

Opening financial services accounts

Deposit accounts - deposit cheque in same name as new applicant, or
Face to face: One proof of identity and one proof of address, or
Non face to face: two proofs of identity and two proofs of address
These procedures are very detailed, often vary between product types, and are documented within the Joint Money Laundering Steering Groups Guidance Notes, and the Finance and Leasing Associations Guidance Notes.

Opening an insurance policy – endowment, life, holiday, creditor, etc. None

Becoming employed P60 and NI number, plus optional references, educational certificates and CV checks

Issue of TV Licence None

46. Many of these processes have wrapped around them subtle crime opportunity reduction measures such as the need to receive the application form and product of it through the post, or the presence of data matching processes to identify anomalies and fraud risks which have been particularly successful: but these are not a mandatory part of the process. Ultimately, the probity of any of these processes needs to be tested for two things – validity and verification. The first is to ensure that the individual exists; the second to link the applicant to the identity. In reaching a conclusion it is necessary to reflect upon:

- The quality of the underpinning enrolment methods to establish initial identification upon which the proof is issued
- Whether the evidential proof contains any form of hard security and anti-forgery features
- Whether the evidential proof contains some form of unique data security – such as an encrypted reference number that can be checked
- Whether the evidential proof provides for some form of positive linkage to the individual presenting it
- Whether there is a method of identifying forged, lost and stolen documents, and instances of fraud at an individual / address level

47. None of these identification measures is fraud-proof. The identification and fraud prevention models in the commercial sector have developed at a significant pace, but less sophisticated enrolment models without data matching processes remain reasonably easy for a determined fraudster to surpass. Why is this the case? Essentially, it is because speed has primacy over checks, and the more important speed is in processing applications – whether these be for social security relief or for financial services– the easier it is for fraudsters to ‘pass’. Automated fraud prevention systems have become essential to supplement and improve upon manual diligence. Identification through bearer documents is regarded as adequate for the vast majority of applications – though they are laborious, expensive and stifle commerce - but this is so only because most people are honest and/or fear sanctions should they make misrepresentations.
48. The factors that appear to be constricting the veracity of these processes are threefold. Firstly, the simple truth is that the corroborative evidence used is not really self supporting – in the sense that there is no proof of identity required to obtain a birth certificate, nor an accessible audit trail to see who has done so. A birth certificate can be used to obtain a passport and a driving licence; a birth certificate, passport and driving licence can be used with utility bills and other such documents to obtain financial service accounts. Secondly, the way in which the processes calculate threshold carries little if any quality. These methods suggest that the sum of the process is equal to its contributing parts. In reality, accumulating a volume of paper proofs – all of which could be obtained by fraud, forgery or theft - does not provide for ‘verification’, and the low integrity of many of the documents suggests that the ‘validity’ of the proofs is questionable. Thirdly, in the UK, there is no regularised form of cross sector notification of fraud at an individual level and risk at a document level – such as the VIS system used in the Netherlands to notify third parties of fraud or risk within documents. Any commercial organisation, and for that matter other public sector organisations other than the issuing department, could be induced to accept lost or stolen evidence of identity as if it were genuine. This draws a serious question over the use of Government proofs for commercial identification purposes: even the impact of the CIFAS protective registration system (which records identities of potential and actual victims of fraud) is slight against the number of lost, stolen or compromised public sector proofs. Thus the control mechanism that would improve upon proof ‘validity’ and the measure of reliance that could be awarded to them is absent.
49. The identification and authentication processes that are presently being ratified by tScheme Limited are significantly stronger than any of the public sector and enforced through regulation commercial models, and carry substantial credibility, especially for higher level certificates. The profiles that have been developed are not just applicable to the issue of digital certificates, and subject to comments made later on in this paper, there would be real value in these being adopted into the real as well as the virtual world.
50. If the existing processes could be termed ‘champion’, are there credible ‘challenger’ models for identifying individuals that work any better? The latest commercial models to be introduced to the market rely heavily on data as opposed to paper, and proof or verification through automated and manual processes.
51. One such model from information solutions company Experian measures identity in a new way that harnesses credit scoring expertise to measure data evidence of life events, scores these for provenance and reliability - validity, and then tests all the data for consistency and fraud risks to provide for verification to reach a final identity score. Policy rules have been

coded into the system to detect automatically cases of identity fraud by impersonation and invention. This allows businesses to fast track credible customers with consistent identities, and follow alternative enrolment strategies where there is doubt. This method of measuring customer data and dealing with fraud risks has been tried and tested in an application-processing environment and found to be extremely successful.

The Experian Alternative

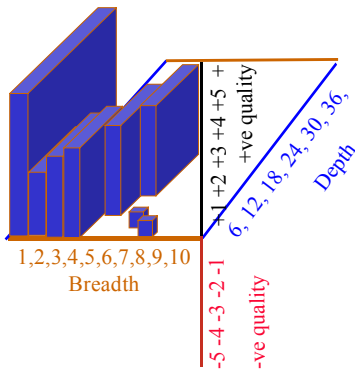


Table 4

A personal data landscape

This shows how the ‘validity’ of all available data proofs (represented by the blocks) can be objectively measured in three dimensions including volume, provenance and quality. The automated fraud detection system is used to establish ‘verification’ against the control data through the use of coded policy rules, which if triggered would reduce the score or cause referrals – depending on the measure of risk exposed.

52. Another way of using data and process effectively is ‘challenge and response questioning’. Here the applicant provides sufficient information about themselves for an initial data collection exercise to take place, then is asked more detailed questions about that data which in theory only they should know. Answering the questions correctly suggests verification of identity against valid data. One of the issues that impact upon this model includes the availability of other sources of data to establish the answers needed to provide correct responses. For example the Land Registry provides details about mortgage providers, the HPI and Car Data Check systems provide information about car finance creditors. Thus an individual’s knowledge of lower level details of their data references is probably more persuasive in establishing verification. In addition, where a person has few commercial data references, the process of identification is starved of data on which to mount the assessment.

53. Do these challenger models offer greater credibility than any paper proof collection exercise? And are they more useful for the digital age than their real world counterparts? It is arguable that they are just these things for a variety of reasons, including:

- Processes and systems have been designed from the outset to meet the validity and verification requirements. Consequently there is an absence of ‘function creep’.
- The systems utilise data - a source of validity that is difficult to corrupt, cannot be lost or stolen, nor counterfeited.
- Using data provides for powerful fraud prevention processing, and this largely sets aside fraud risks.
- Subject to applicant and data owner consents, data does not limit the number of proofs or events that can be factored into the models.
- Applicant’s identity is measured for validity and verification, a qualitative process, and not assumed because a cumulative threshold has been reached.
- As more data becomes available for the re-identification of an individual, it is possible to re-evaluate the identity score or trust level in a contemporaneous time frame with the existence

of the relationship. This caters for fraud risks that mature after the formation of a relationship.

54. The single gap is collusive impersonation. Here the 'victim' of the identity theft provides the necessary answers to get around the 'verification' processes. The only consolation is that this would be no different in the real world of paper documents. The style of the fraud requires the suspect and victim to connive to defraud together, and the victim pretends to have 'lost' or had stolen the relevant documents, denying culpability despite having given them to the suspect. The good news is that what appears at face value to be an 'exact current address impersonation' is often interpreted by fraud investigators as a potential 'collusive impersonation'. The involvement of the victim is often hard to prove, but with a reliable fraud outcome-sharing system in place, should occur just once. Where similar 'in family' exact impersonations occur, the 'victim' on discovering the fraud, often names the disenfranchised family member suspect, and the matter is resolved.

55. In summary, innovation in the area of identification provides the opportunity for customers to be easily identified, negate the real world problems and compromises created through legacy processes, and creates a platform for building new customer relationships with confidence.

56. This begs the question of how often we really need to be identified. Is it not the right of the individual to be anonymous – should they want to be? Real world face to face purchases are nearly entirely anonymous – save for instances requiring delivery or credit terms. Generally the individual is not expected to make themselves known to the vendors, and rightly feels comfortable about this. In the virtual world registration can be anonymous by using an innocent pseudonym, but if an e-commerce transaction is anticipated this would conflict with payment details and genuine registrations are probable.

57. There are occasions when pseudonyms would not be contemplated – for example:

- Transacting with central, regional or local Government,
- Formal liaison with law enforcement
- Entering into and executing contracts
- Entering into a relationship that was regulated – such as financial services or insurance
- E-commerce transactions

58. In all other cases, unless the vendor openly prohibits anonymity, the use of a pseudonym is acceptable. This ensures that a subject's privacy is not eroded unnecessarily. But the reliability of the customer need not be mundanely assessed through identification procedures time and time again, providing that the identity score is acceptable and the risk of identity fraud is catered for. In many cases it would be acceptable to an e-world vendor for a new customer to evince them of their credibility through trust, setting aside the need for repeated full identifications. This will become a necessary model for interaction, as the greatest threat to an individual's identity is compromise through proliferating use. Therefore, what can replace identification to fill the confidence space between parties that do not know each other? The Electronic Communications Act 2000 created a legal parity between real and digital signatures. Given the robustness of the identification processes used in the issue of higher level trust devices and the adoption of common standards, such devices are ideal for creating confidence between remote parties. Indeed, they are equally capable in a

face to face interactions. It should be mentioned that the tScheme profiles for the identification of registrants are presently in draft, but these are close to ratification.

59. There is a line of thought within the tScheme that trust need not find its roots in historical identification through examining evidence of life events, but is capable of being assumed from transactional patterns that have accumulated over time. If such a model is reliable, then this could easily change the face of identification as we know it today. This separates trust, which could be seen as a variable value attributed from performance, from the historical view of a person's identity that is linked to evidence of life events, and has a more absolute value. In most cases it is reasonable to hypothesise that performance engenders trust, but does it necessarily follow that identity is confirmed from this progression? What if the individual's performance declines - does it mean that their identity is of any lesser value? In a transactional situation it may not matter as what is required is trust more than identity. Thus the usage of trust devices should grow with identification being assumed from trust, and less frequent identification episodes in the future. This bodes well for reducing the opportunity for identity information to be compromised. There are other issues that need to be considered though. These include:

- the use of documents that can be obtained in a false name, counterfeited, or stolen without a method for communicating such a risk will undermine any system
- the incidence and methodology of 'sleeper fraud' – a transactional pattern may not be what it seems, and created to provide the illusion of trust
- the measurement of identity necessarily needs to extend beyond volume of paper evidence to include provenance and quality. Without this developed identity fraud will not be exposed at the point of enrolment. Lessons can be learned from both fraud ring and determined individual fraudsters activity in the commercial sector.
- the regularised use of a known fraud file to prevent repeated identity fraud where the same attributes are used

60. Ultimately criminals will find ways through systems and procedures, so it is realistic to expect some degree of unlawful assimilation of knowledge about identity from organised crime groups infiltrating trust service providers, and the growth of first parties selling their identities for others to use. The standard adoption of the use of Criminal Record Bureau certificates to show clean antecedents of those in a position to acquire knowledge about identity is recommended. This separates known criminals from information that they might then use for unlawful purposes, though adults without prior criminal records can be corrupted.

61. We often rightly associate trust services with the use of smart cards. Smart cards are ideal because they are portable, invoked by a password, and these things provide for good security – the user has something physical in their possession, and is required to know something as well. Given that the present model for the use of trust services can involve the user possessing a smart card, where might this establishing of trust move to in the future? Biometric linkage is feasible if the false acceptance and false reject rates are reduced to the point that the false rates are not inconvenient. (Except where it leads to catastrophe, one learns about false rejection faster than about false acceptance.) But there remain privacy issues.

62. There are advantages in looking forward to a biometric trust model - biometric identifiers cannot be lost, provide for unique authentication, and are convenient to use. Biometrically authorised access control to buildings and passage through borders is likely to grow, partly

through general fear of crime and partly from concern about unauthorised access to work terminals. The biometric industry expects its revenues to grow ten fold between 1999 and 2003. Currently the greatest revenues are being earned in finger scan, followed by hand scan technology projects. Clearly there is an optimistic view that biometrics will be used to indicate identity, and in turn there will be more occasions when identity will determine rights and privileges as the technology becomes more widely adopted.

The impact of changes in plan or reasonably likely to occur.

63. There is a significant distinction between the pace of innovation and the delivery and adoption of widespread change. Consequently there is a probability that certain advancements will be leapfrogged. It seems likely that identity will be referenced initially through trust services, and latterly through biometrics. The channels through which identity is displayed are likely to be digital TV, the Internet and mobile communications, (1) because digital TV is already planned to be nationally adopted, and is a capable and secure link between individuals and a particular service; (2) because the Internet is so widespread and has the ability for hardware devices such as smart card and biometric readers to be cheaply and retrospectively added in the home; (3) because of the development of handset technology, integration with the Internet, together with user acceptance, portability and cross socio-economic group penetration. That said, there is a strong presumption here that society will adopt the new opportunities for change. Many will choose not to, because they do not understand it or cannot afford it, and it is for these sorts – ‘the technical underclass’ - that special provision needs to be remembered to avoid them being marginalized. This is a familiar problem facing e-government also.
64. It is probable that the role of face to face interaction with the public sector and commerce alike will alter substantially, and most people will care less about human direct interaction. One consequence is that the cost to benefit ratio of face to face communication centres will grow, and provision will deteriorate because it is too costly. We can see this already with differential interest rates for internet-only banking.
65. Currently, e-tailers run serious risks of impersonation and often have to choose between accepting high fraud risks and losing sales. However, as identification becomes a more exact science and transaction fraud reduces through the use of new layers of fraud prevention coupled with authentication, the attraction of direct selling will grow. It will become increasingly difficult for certain bricks and mortar retailers to retain expensive outlets. This is because they will invariably have higher costs than direct selling models, which will become less susceptible to fraud, operate from less expensive premises with lower overheads, and offer the advantages of price and delivery. There is a chance that certain types of retailers will find more of their customers looking but not buying. Might the shift be so dramatic to force manufacturers to pay for the display of their goods in physical locations to supplement falling sales and retain a high street presence?
66. There is likely to be a sea change in how we are identified when opening new financial service facilities. The present system has been strongly criticised (Cruikshank Report - Competition in UK Banking, March 2000), and it has been advanced that new technologies such as digital certificates and cross sector reliance upon identity should be introduced. Thus those who have facilities have an opportunity to open more accounts, widening their relationships. For those that don't – the socially excluded - less onerous processes have

been recommended, with correspondingly more opportunity for the formerly excluded to have access to accounts that may generate substantial crime income.

67. Turning to governance, the ability for individuals to be identified remotely through authentication – digitally or through biometrics, means that online voting is probable. No longer will we need to attend a polling station, instead we might call up our digital voting paper and select our candidate. This may generate a higher percentage voting, but conventional methods will have to be retained for the ‘information poor’, or else there will be voting distortions.
68. What other things could be linked to our identity? The technology clearly exists for the bearer to use a digital certificate in one to one social interactions and this provides for trust to be awarded. This could spark a growth in the proactive use of identity, not just to create a position of trust between two parties, but so that relevant references can be accessed to build upon that identity with attributes and information. These might include medical information, a Criminal Records Bureau certificate, a photo, creditworthiness, licences to drive, a passport and visa details, licences to purchase certain items that require control, loyalty benefits etc. This would have the advantage of reducing crime through the ability to identify the suspect quickly, easily and unequivocally. These might typically include those offences that are committed in hitherto anonymous remote meetings.
69. So if the criminal becomes aware that they can be identified more easily than ever before, how might this change their behaviour? If they recognise the risk, there could be two effects. They will either be displaced through target hardening into committing other crime where the risk of being identified is less, or exercise leverage upon others to commit crimes for them, for example by kidnapping or blackmail. Identification might not cause them concern, if the short-term gain is worth more to them than the ultimate sanction. The uplift to law enforcement would be more focussed investigations, and less opportunity for judicial errors (see ‘The use of biological data in Fraud Prevention and Detection’ - M Cooper). The sorts of offences that are likely to be reduced are all types of fraud and money laundering (though serious laundering is likely to occur not through impersonation but through simulating legitimate transactions), violence in premises requiring identification upon access – nightclubs and disco’s, and even sporting events. The deterrent, as opposed to deflective, effects of this remains unknown, but opportunities are likely to be reduced if permission to be in certain places can be refused and electronically enforced.

Conclusion

70. This journey through the identification process has revealed certain opportunities that would bring cost savings in the form of reduced fraud and administrative burdens to both the public and commercial sectors. These are necessary to ensure that any future innovations in the area of identification and trust are founded on a reference platform that is more stable than it is today. The most important of these – though as with many current initiatives, it raises data protection and privacy issues - is the introduction of a public sector and commercial sector identity fraud sharing system, that reflects fraud risks at an individual level, document level, and caters for victims of fraud in a sympathetic manner. Document validation processes (including the tricky area of validating e-documents) would be another immediate improvement.

71. Next, the present system of allowing the non-publication of change of name needs to be addressed. There are reasons why change of name will become more common, including the availability to employers of criminal convictions. If the true and often negative attributes linked to an identity cannot be accessed because of this process, there are severe risks for children and vulnerable persons to be victimised by offenders using new names. In addition, fraud will not be identified so readily through data sharing.
72. More work could be done to limit the instances of identity theft. This could be achieved through the cross-referencing of deaths and births to prevent many instances of deceased impersonation fraud. Also the sharing of information about persons who emigrate, which would prevent their identities being used by others that 'replace' them in the UK, even if some of them remain capable of generating new identities and passports in their home or adopted countries.
73. As innovation improves upon the identification process, and enhances the level of validity assigned to life events and the verification of the individual to them, clear methods of accrediting alternative models across all sectors and industries should exist. More work should be done on the measurement of identity beyond volume driven cumulative models, as more refined assessments are possible by adopting a qualitative approach which takes account of provenance, which is important as the socially excluded may through circumstances have fewer life event attributes.
74. The future holds a sea change in the availability of access to identity attributes and trust across a range of personal and commercial forms of interaction. Attributes will be more widely accessible than ever before, and provided that the identification process allows these to be securely linked to the bearer, there will almost certainly be a reduction in a range of offences, from fraud and deception to theft and violence that depend on not being easily identifiable. This will still leave many serious frauds by those apparently entitled to exercise authority by virtue of their position; and it will probably still be possible for those not biometrically authorised to break into homes and motor vehicles, even if it is harder for them to take the vehicle away. This crime reduction will be enhanced further by the inevitable – unless forbidden by the Data Protection Commissioner - introduction of biometric linkage between an individual, their identity, and their attributes. However, if this is a voluntary process, there is sure to be a growing margin of trust and service between adopters and dissenters. It would be equitable to allow the technology to deliver as many or as few attributes as the individual is comfortable in revealing. Circumstances may allow certain bodies to over-ride the access to such information – such as hospitals accessing medical data, the Police accessing identity data and so on. This would make for a comfortable balance between privacy and social utility.
75. As ever, technology and innovation may leap higher than the community around it can reach. However, providing there is a resemblance between things that we do now and future expectations of us, the progression and route of change will be understandable and acceptable to those that choose to adopt it. Thus, providing that we give ourselves the tools to fix the problems that exist today, our identities will surely carry greater value in the future, enhancing speed of service and remote interaction, and the verification of rights to use the identity, its attributes and a measure of trust that will be more firmly assured through well thought out authentication processes than through the current mechanisms that are a legacy of our history.

¹ Acknowledgements: There are many commercial fraud prevention specialists that have provided assistance to us in the way of confirming the facts and in turn shaping the content of this essay. Particular thanks are due to Mr Hugh Norton-Amor of 'CIFAS – the fraud prevention system' for the provision of statistical information about identity fraud. We are also grateful to Mr Chris Binns of tScheme Limited for the provision of material about securing electronic business. Finally, to Ian Stewart and Jon Jones of Experian Ltd for their insightful assessment of identification through data references.

² Gareth Jones is Head of Fraud Control for Experian Ltd. Michael Levi is Professor of Criminology at Cardiff University. The name order is alphabetical.