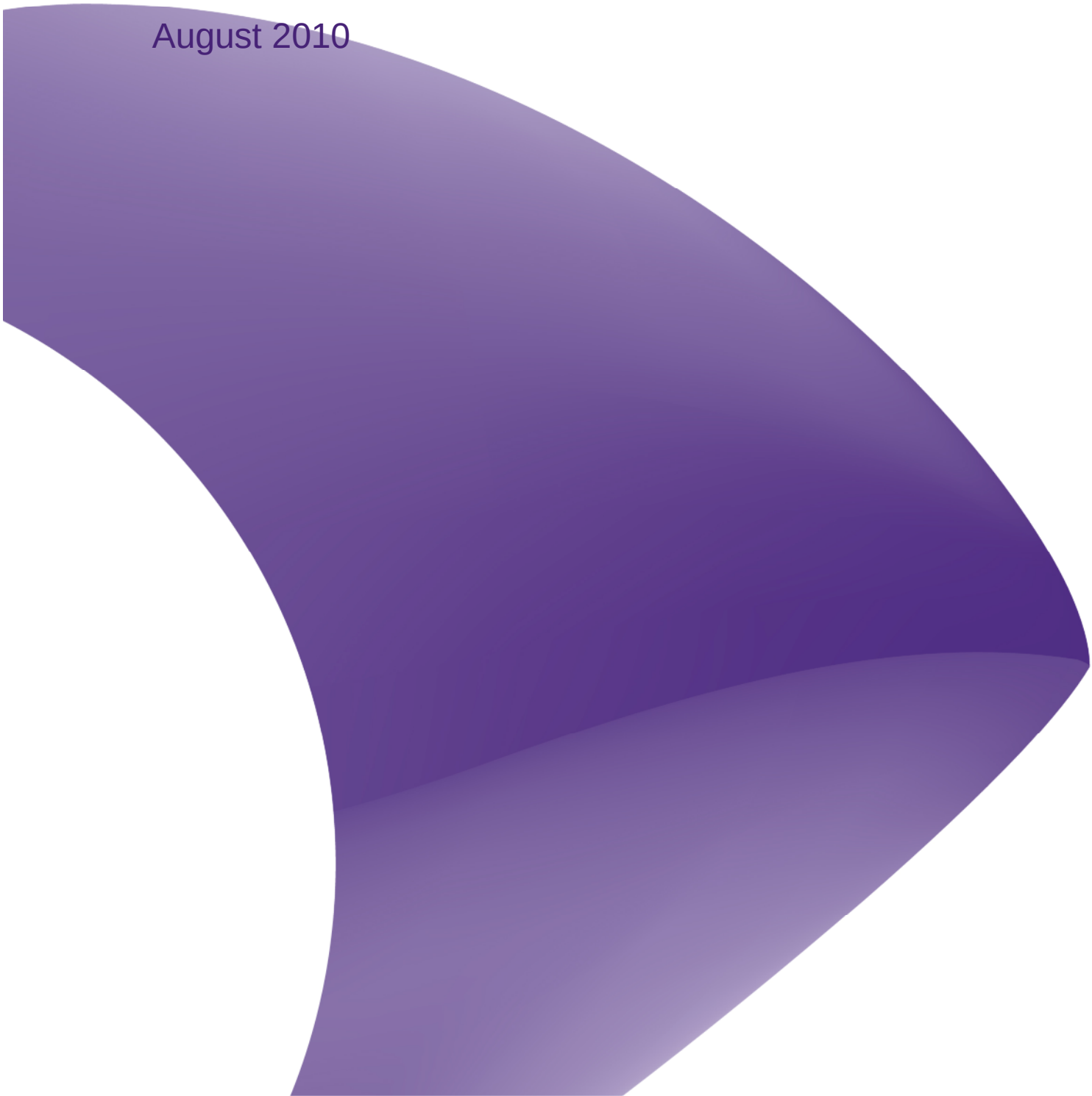
National Fraud Authority

INFORMATION SHARING REPORT

PROGRESS UPDATE

August 2010



CONTENTS

EXECUTIVE SUMMARY

The NFA Information Sharing Task Force is working hard to identify, assess and remove barriers to allow effective and legal sharing of information, enabling public and private sector organisations to better prevent and detect fraud.

The Task Force has identified numerous websites that provide possible solutions to a wide variety of data sharing issues. This Report highlights solutions that could be of assistance in the wider counter fraud community; examples include:

- *Right to work verification* – Providing details on the Employer Checking Service and hotline available for sponsorship and employers;

- *Financial Services Authority regulations* – Addressing the concerns organisations may have when reporting suspected fraud due to potential financial and legal ramifications by clarifying the FSA's position and highlighting websites that can provide guidance to organisations;

- *Financial fraud information* – Explaining the complex and legal background to sharing financial fraud information, helping organisations understand the data sharing framework which all banks must abide by. Providing information on guidance published by the British Bankers Association to help organisations understand the circumstances governing the disclosure of information;

- *Criminal record checks* – Explaining the services offered and costs and timescales involved in criminal record checks to help organisations understand the system and assess the options available according to their time and financial budgets;

- *Fuel station fraud data* – Highlighting schemes launched, such as "No Means of Payment Recovery" and the data available to help organisations get information to protect themselves against this type of fraud.

This Report also provides an outline of some of the ongoing information sharing work that the Information Sharing Task Force is currently involved in; such as access to DVLA data, death data and identity document verification.

The final section of the Report contains a summary on the role of the Information Commissioner's Office, highlighting good practice notes and framework codes they have published in relation to information sharing.

INTRODUCTION

The National Fraud Authority (NFA) established in 2008, is the Government's strategic lead organisation on counter-fraud activity in the United Kingdom. It works with a wide range of stakeholders across the private, public and third sector. One of the NFA's first actions was to publish a National Fraud Strategy, which outlined how the counter-fraud community could work together to better detect, deter and prevent fraud in the UK[1]. The importance of sharing information across both the public and private sectors to combat the harm caused by fraud is a main cornerstone within the strategy.

The NFA employs a team to look at specific information sharing issues between and within the public and private sector. The team's key aims and objectives are to work with stakeholders in the public and private sector to resolve information sharing barriers and to identify and promote good practice in information sharing in the fraud arena. This Report sets out the progress that the NFA Information Sharing team, together with the NFA's Information Sharing Task Force, has made to date and contains some helpful pointers to specific information organisations can access directly.

The Information Sharing Task Force is a group of 25 organisations covering the public and private sectors, established specifically to identify and remove barriers preventing sharing data to minimise harm caused by fraud. Current members include:

- Public Sector: Charity Commission, City of London Police, DWP, HMRC, Information Commissioner's Office, Identity and Passport Service, Ministry of Justice, National Anti-Fraud Network, Audit Commission/National Fraud Initiative, NFA, SOCA.
- Private Sector: Aviva, British Telecom, Call Credit, CIFAS, Detica, Equifax, Experian, HSBC, Insurance Fraud Bureau, Lloyds Banking Group, National Hunter, RBS, Synectics Solutions, UK Cards Association, Financial Fraud Action UK.

The NFA Information Sharing Team is always looking for details of information sharing barriers which may be hindering an organisation's ability to reduce the harm caused by fraud to itself, its clients and the wider public. Any organisation facing these barriers is encouraged to get in contact with the team. The following is a list of essential information the team would require to be able to provide assistance:

- what data you wish to access and why;
- a description of the barrier(s) faced; and
- the benefits/ values you anticipate will flow from access to the data (ideally specifying how much fraud could be prevented or detected).

The NFA Information Sharing team would also appreciate your feedback on this Report, in particular whether you have made use of any of the solutions identified in your counter-fraud activity.

To report an information sharing problem or for clarification of any of the information contained in this Report, contact the team at: information.sharing@attorneygeneral.gsi.gov.uk.

[1] www.attorneygeneral.gov.uk/nfa/GuidetoInformation/Documents/National%20Fraud%20Strategy.pdf

IDENTIFIED SOLUTIONS

This section highlights available solutions for a variety of data sharing issues raised with us that we believe may assist others in the counter fraud community.

Company and Foreign Property Data
Certain records at Companies House are hand written making real time verification and / or searching resource intensive and time consuming.

UK businesses are unable to obtain companies register data for overseas businesses to enhance investigations into suspect dealings.

Organisations are unable to check property ownership on foreign properties. This limits their understanding of a suspect individual's capital worth.

Companies House has accepted company filing documents electronically since 1999. Currently 95% of documents are received in this format and any documents received on paper are scanned and made available on their free Webcheck Service. Due to resource and cost constraints they have not yet been able to transfer retrospective records online.

Not all jurisdictions make their company register details available to the public. The relevant national register is best placed to assist with any questions relating to companies within their jurisdiction that are not registered within the UK. Companies House's website provides a list of links to Registers worldwide.

In addition, there are websites available that enable access to company business information, such as the European Business Register which provides access to 25 European country's official registers, and the list of court information systems and public registers on the Council of Europe's website for 13 European countries.

There is no centralised UK access point for details about foreign property ownership. These details need to be obtained from the responsible organisation in the particular jurisdiction. HM Land Registry publishes an Inventory of Land Administrations in Europe and North America on its website which provides the contact details for land title registration organisations in 41 countries, and the European Land Information System (EULIS) provides direct online access to official land registers in Europe. Many registries also provide online services to access information on property ownership within their own jurisdiction.

Credit Reference Agencies (CRAs) also provide services to assist UK businesses to access overseas data.

Further Information:

Companies House Webcheck service:
wck2.companieshouse.gov.uk/339094a284dded28ccc1314d2225dc0d/wcframe?name=accessCompanyInfo

Companies House list of international registers: www.companieshouse.gov.uk/links/introduction.shtml#reg

European Business Register: www.ebr.org/

Council of Europe Court and Registry information: www.coe.int/T/E/Legal_Affairs/Legal_co-operation/Operation_of_justice/Information_technology/Links/3_court_info_registers_ENG.asp

Inventory of Land Administration Systems in Europe and North America (HM Land Registry, July 2005): www1.landregistry.gov.uk/publications/default.asp?pubtype=56&f=5&o=u

EULIS: www.eulis.eu/

Right to Work Verification
Access to information to ensure potential employees have a 'right to work' in the UK.

It is the legal responsibility of an employer to ensure the staff they employ are legally entitled to work in the UK. Assistance is available from the UK Border Agency (UKBA) to provide information and support to employers including:

- information for employers and education providers about sponsorship under the points-based system;
- a service to employers who want to verify the entitlement to work for people who are awaiting the outcome of an application made to the Home Office (the Employer Checking Service);
- advice to employers about preventing illegal working; particularly about carrying out the document checks necessary to attain a defence against conviction;

The Employer Checking Service can be used to check the status of individuals' right to work in the UK where:

- the individual has an outstanding application or appeal with UKBA;
- the individual has presented an Application Registration Card (ARC) requiring validation;
- the individual has presented a certificate of application which requires validation.

Further Information:

www.ukba.homeoffice.gov.uk/employers/preventingillegalworking/support/

Sponsorship and Employers hotline: 0300 123 4699 (weekdays 0900h-1700h).

Financial Services Authority (FSA) Regulatory Disincentives
Reporting suspected and / or confirmed fraud to the FSA could pose potential legal and financial ramifications. This may lead to under-reporting of fraud and subsequent lack of preventative action.

The FSA website provides a comprehensive breakdown on subjects such as 'Regulatory Requirements', 'Treating Customers Fairly' and 'Good Practice'. It also has a whistle-blowing section which allows concerns to be reported in confidence, and information specifically designed to help Small or Medium Enterprises meet their fraud-reporting obligations.

The effectiveness of the FSA's regulatory regime depends to a significant extent on maintaining an open and co-operative relationship between the FSA and those it regulates. Firms authorised by the FSA are required to tell the FSA anything relating to the firm of which the FSA would reasonably expect notice (Principle 11 of the Principles for Business). Authorised firms are also required to report significant fraud to the FSA (SUP 15.3.17R).

Proactive supervision and monitoring of firms, and an open and cooperative relationship between firms and their supervisors, may lead the FSA to decide against taking formal disciplinary action in certain cases. However, in such cases the FSA will expect the firm to act promptly in taking the necessary remedial action (agreed with its supervisors) to deal with the FSA's concerns. If the firm does not do this the FSA may take disciplinary or other enforcement action in respect of the original contravention. When deciding whether to commence a formal investigation or exercise certain powers against an authorised firm, the FSA will consider whether the firm/ issuer/ individual proactively brought the actions or potential breaches to the attention of the FSA.

The FSA resolves many enforcement cases by settlement and, in recognition of the value of early settlement, the FSA operates a scheme to award explicit discounts for early settlement of cases involving financial penalties. If a firm brings an issue to the attention of the FSA, and it is decided that enforcement action is appropriate, the firm could benefit from agreeing to early settlement.

Further Information:

www.fsa.gov.uk/smallfirms/new_to_regulation/index.shtml

www.fsa.gov.uk/Pages/Doing/Contact/Whistle/index.shtml

www.fsa.gov.uk/smallfirms/your_firm_type/mortgage/fraud/report.shtml

Human Resources
Quality of staff databases limits employee information data-sharing. This creates an opportunity for fraudsters to re-commit fraud against numerous employers.

Commercially, databases exist to ensure that information about employees dismissed for fraud is shared to minimise the potential for such staff to move to another unsuspecting employer to commit further fraud[2]. Examples are both industry-specific (via TUFF) and cross-sector (via the CIFAS Staff Fraud database where members can ensure that information is shared about their employees dismissed for fraud, employees who have resigned and then been

[2] The process for collecting, sharing and disseminating this data generally requires the approval of the Information Commissioner's Office.

identified as involved in fraud, and potential staff fraudsters who are/ were supplied by third parties).

If organisations are interested in comprehensive employment history or criminal record checks, credit reference agencies (CRAs) or the Criminal Records Bureau (CRB) may be able to assist. CRAs offer specifically designed services to help ensure that the people you employ are who they say they are, and have the stated qualifications and experience to do the job.

The Information Commissioners Office also publishes a 'Personal information online small business checklist' which offers guidance on how small and medium sized businesses can collect and use information about the people they employ within the proper constraints outlined in law. (For further information please refer to the ICO chapter at the end of this report).

Criminal Record Checks
Criminal Records Bureau (CRB) checks are long and costly. This significantly reduces the likelihood of completing searches prior to recruiting employees.

The CRB provides wide access to criminal record information through its Checking Service. It enables organisations in all sectors to make safer recruitment decisions by identifying candidates who may be unsuitable for certain work.

The cost of a CRB check is prescribed in regulations. The regulations were reviewed and amended last year, reducing the cost of a standard check (which shows current and spent convictions, cautions, reprimands and warnings held on the Police National Computer) from £31 to £26.

An Enhanced Check, which includes a review of lists held by the Independent Safeguarding Authority[3] and other data sources such as the British Transport Police and the Royal Military Police, costs £36. Checks for volunteers are free of charge.

The time it takes to complete a CRB check varies on a case-by-case basis, depending on the level of information available on an individual, the number and type of hits that may appear on a system, and the number of systems that a hit may appear on, although the aim is to complete all checks within four weeks.

Further information:

www.crb.homeoffice.gov.uk/default.aspx.

Fuel Station Fraud
Fuel station 'No Means to Pay' data should be shared, especially within the filling station community.

[3] The Independent Safeguarding Authority is responsible for maintaining a register of individuals considered unsuitable for work with children or vulnerable adults. This service is currently being reviewed.

The British Oil Security Syndicate (BOSS) recently launched a 'No Means of Payment Recovery' scheme, designed to put in place a co-ordinated system for combating this crime and recovering financial losses incurred by incidents where drivers fill up, claim to have 'No Means of Payment' and subsequently fail to return to pay.

Access to DVLA data to help combat 'No Means to Pay', and assist fuel stations in the recovery of their losses is available either directly from DVLA or via the BOSS[4], which has been accepted as a DVLA Accredited Trade Association and is therefore able to access DVLA data via a secure electronic link for these purposes.

Further information:

www.bossuk.org

www.dft.gov.uk/dvla/data/rc.aspx

Financial Fraud Information

Banks are reluctant to share data with other financial institutions on fraud attacks.

Banks are unable to verify information with other financial institutions.

Investigators and victims have difficulty obtaining suspected and confirmed financial fraud information from Banks and Insurers.

The British Bankers Association (BBA) publishes practical guidance on data protection both generally and specifically. For financial fraud investigators and managers[5], this provides details of the legal and regulatory framework of the main fraud risk areas, and outlines the complex data protection rules within the financial services industry in a practical context.

The circumstances governing the disclosure and exchange of information in the financial services sector are complex and very carefully managed but disclosure of information does, and can, legally occur. The 2006 Fraud Review stated that, "*effective sharing of data on actual and suspected frauds is a key strand to improving the quality of the UK's response to the threat from financial crime*". Ultimately any data sharing proposal in the banking sector must have due and proper regard to the duty of confidentiality owed by a bank to its customer as required by law. This duty applies to the extent that it may even prevent a bank from communicating information to other companies in the same group, including its own subsidiaries.

However, a banker's duty of confidentiality is not absolute. There are four key circumstances where a bank can legally disclose information about its customer. These are:

[4] BOSS is an independent organisation formed in 1991 by the oil industry, together with the Petrol Retailers Association, the Home Office Crime Reduction Centre, and the Association of Chief Police Officers, to reduce the amount of crime taking place on Britain's petrol forecourts in partnership with the police.

1. Under compulsion of law;
2. Where there is a duty to the public to disclose;
3. Where the interests of the bank require disclosure; or
4. Where the disclosure is made by the express or implied consent of the customer.

Thus it is not necessarily accurate to say that Banks are 'reluctant' to share data but rather that there is a complex regime and procedural requirements that need to be addressed prior to approving any requests.

Banks generally provide information only in response to a court order. This ensures that they have not breached their duty of confidentiality to their clients as they are supplying the information under legal compulsion. Over recent years, the powers available to law enforcement agencies to require provision of information without a court order has expanded under legislative regimes such as the Serious Organised Crime and Police Act (SOCPA) 2005 and the Serious Organised Crime Act (SOCA) 2007. Thus the use of legislative information gathering powers by law enforcement has increased ten-fold, with little or no matched increase in resource to process them. In order to efficiently manage the handling of such requests from law enforcement, all requests are prioritised to ensure that the bank meets its statutory and regulatory obligations.

Banks are also obliged to report suspected money laundering activity to SOCA under the Proceeds of Crime Act (POCA) 2002. The BBA encourages its members to share data with other financial organisations and CRA's on suspected fraud typologies and 'fraud' data. However, internal guidance to report attempted fraud is a matter for individual corporate policy and until this point is addressed at higher levels the industry will need to rely on the cooperative working of all organisations using agreed and lawful methods.

Further information:

www.financial-ombudsman.org.uk/publications/ombudsman-news/45/45_bankers_duty.htm

www.bba.org.uk/bba/jsp/polopoly.jsp?d=146

www.bba.org.uk/bba/jsp/polopoly.jsp?d=155&a=7818&view=print

Information Sharing with and between DWP and HMRC
DWP staff needed to be reminded of changes to the process for internal data sharing following the introduction of a central reference point in Shoreham.

Guidance given to Local Authority investigators working on behalf of DWP needed clarification on how to access HMRC information. Previously data requests had been unnecessarily rejected by HMRC.

To address the concerns raised, DWP will issue clarification to staff on the process of disclosing information explaining the reasons why the system was centralised and the role of the Shoreham office. In addition DWP and HMRC are reviewing the guidance on their websites to provide a clearer definition of

information sharing gateways available, the processes, and the level of evidence required for data request approval.

In relation to Local Authority access to HMRC data, guidance will be issued to clarify the process. In this situation the legal gateway is between HMRC and DWP therefore Local Authority investigators should use this process and access HMRC data via DWP.

Bank Identification Number (BIN) Lists

Organisations cannot access BIN Lists from Banks. This information would be used to help detect and prevent 'card not present' fraud.

BIN numbers are represented by the first six digits on the front of a plastic payment card. This number is used to identify the party who issued the card to you. Every time you use a plastic payment card to make a payment the BIN is system is activated.

The NFA met with representatives from UK Payments and BBA to discuss access to BIN data. During this meeting it was clarified that BIN numbers are owned by the card schemes (Visa/ Mastercard); not, as is commonly perceived, banks.

BIN Books are available to members of the card schemes. If an organisation is not a member of a card scheme, but collects payments by card, they can approach card schemes for access to BIN lists. If an organisation is not a member and does not collect card payments, requests for BIN data can be made via an approved members' sponsorship. When making a request of this nature details on how and to whom the information will be disseminated must be provided.

Further information:

en.wikipedia.org/wiki/List_of_Bank_Identification_Numbers

www.binbase.com/csv.php

Telephone Number Validation

To validate whether telephone applicant/ owner and telephone number in use match i.e. that the quoted owners' name matches the documented owners' name.

Discussions with British Telecom (BT) and the Telecommunications UK Fraud Forum (TUFF) regarding Landline Verification Services identified data stored in BT's OSIS database which is held by British Telecom Wholesale Directory Solutions (BTWDS) Licensees.

To access OSIS data[6], BTWDS Licensees need to be approached directly. Some licensees offer services whereby queried ('searched') names and addresses return a telephone number. They can then compare that telephone number to the telephone number for the name and address of the applicant.

Regarding validating a mobile phone number, there is currently no central location for data associated with mobile phone numbers. All network providers operate their own disclosure departments who service requests for this type of information (such requests must have a basis in law, e.g. under the Regulation of Investigatory Powers Act 2000 [RIPA]). Websites are available to locate Telecom providers for mobile numbers which allow organisations to direct requests for information where fraud is suspected.

Further information:

BWTDS Licensee details:
www.btwholesale.com/pages/static/Products/Managed_Network_Solutions/Directory_Solutions/About_Us/OSIS_Customers.html

www.ukphoneinfo.com/section/home/introduction.shtml

www.wtng.info/

www.magsys.co.uk/telecom/codelook.asp

www.simplcom.ca/telrusca/html/infosat.html

[6] OSIS data is a complete list of all UK subscribers who have requested directory listings, including ex-directory listings. When BTWDS supply ex-directory listings to licensees, the name and address is provided but the telephone number is withheld.

WORK IN PROGRESS ON KEY INFORMATION SHARING BARRIERS

This section outlines some of the ongoing information sharing work that the NFA and the Information Sharing Task Force are currently involved in which we believe will be of interest to you. Within each work area we have highlighted data sharing blockages and provided a summary of current progress.

Access to DVLA Data
Enhancing access and providing a verification service to DVLA datasets outside the framework of road traffic crime.

The Driver and Vehicle Licensing Agency (DVLA) maintains two separate databases:

- ***Vehicle Register***: maintained to identify vehicles used on public roads, assist law enforcement and the collection of taxes, and to facilitate improved road safety. It holds relevant information about each motor vehicle e.g. registration mark, Vehicle Identification Number, make/ model, emissions rate etc. and includes the name and address of the registered keeper, dates of acquisition and disposal, and the vehicle's tax status.
- ***Driver Register***: holds each driver's name, address, date of birth, photograph, entitlement, endorsements, convictions and relevant medical information that may affect a person's ability to drive.

While the law requires the DVLA to protect the privacy of the individual motorists whose details are held on the registers, there are a number of lawful circumstances in which data can be released - including in response to a request under s29 of the Data Protection Act 1998. Where an organisation has a reasonable suspicion about a driver's licence that has been presented to them, they are able to contact DVLA and have that license verified. Because this process relies on s29 – which allows for data sharing for the prevention or detection of crime – such sharing is only available on a case by case basis where there is a reasonable suspicion of criminal activity.

The NFA Information Sharing Task Force has set up a sub-group to consider whether the data held by DVLA could or should be legally and securely available to assist the counter-fraud community. Initial meetings between the NFA and DVLA have been held and work is progressing across the following three categories:

1. Information sought for investigative purposes by public and private sector.
2. Information sought by law enforcement.
3. The ability for the private and public sector to verify information for identity purposes to counter fraud.

This area of work involves many individual strands of information sharing. It closely aligns with larger cross-departmental projects involving identity crime and fraud in the public sector, and as such the NFA envisage this to be a long-term project.

Further information:

www.dft.gov.uk/dvla/data/relinfo.aspx

Foreign Identity Documents
Credit Reference Agencies are unable to validate foreign passports. This hampers their ability to confirm the true identity of credit applicants.

Banks want real time access to foreign passport information. This would enable them to verify the document when foreign customers open a new bank account(s).

The UKBA checks the validity of foreign passports at UK borders and offers its staff specialised training in this area. UKBA's National Document Fraud Unit (NDFU) is involved in ongoing discussions about the potential to market an e-learning product on document fraud to a wider audience.

In addition, the EU's Public Register of Authentic Identity and Travel Documents Online (PRADO) publishes guidelines by individual member states, Iceland and Norway on the security features of authentic identity and travel documents issued by them. Some countries provide an additional tool allowing document numbers to be verified online.

For specific countries, data on reported lost, stolen or invalid passports is published on publicly available databases. Examples of these are:

- Italy: coordinamento.mininterno.it/servpub/ver2/Documenti/cerca_docu_ing.htm
- Lithuania: www.policija.lt/index.php?id=3393
- Belgium: www.checkdoc.be/CheckDoc/

Commercial products such as World Check and Document ID Checker can also assist in checking the validity of foreign travel documents from a variety of countries.

The Information Sharing Task Force will be looking into the available services and how they might best be utilised to assist the public and private sector to reduce the harm caused across all sectors and the community in general by fraudulent use of foreign identity documents.

Further information:

PRADO: www.consilium.europa.eu/prado/EN/homeIndex.html

World Check: www.world-check.com/passport-check/

Experian: www.experian-da.com/solutions/docid.html

Enhanced UK Passport Validation Service

A Passport Validation Service (PVS) is available to any organisation that requires validation of proof of identity. The service operates via phone or secure system to advise clients of the validity of a passport. If a passport is

validated, it is confirmation that it exists, matches the official records, has not been reported lost/ stolen and that there are no concerns over its issue. If a passport is not validated, it may be because the passport is either expired or cancelled (e.g. due to a change of name). A 'not validated - retain if possible' response means that the document is fraudulent. In the event of an attempted fraud, clients are directed to a member of the IPS Fraud Team who can further assist.

Further information

PVS Website: www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/563.htm

Royal Mail Re-direction

Obtaining real time access to the full spectrum of postal re-direct data to enhance risk-profiling, flag potential fraud rings, and prevent, detect and deter fraud.

Royal Mail is currently developing its Redirect Address Check service that provides verification on whether a redirection is set up against a given name and/ or address. This enhanced alert service, known as *National Change of Address* (NCOA), is due to be rolled out very shortly and will enable verification against pending, live, cancelled and expired details.

The current service offered - known as Redirect Check - verifies against the 'from' address and provides a yes/ no output result. The NCOA service will continue with this and it is hoped will include additional fields to more accurately verify individuals and provide a more informed output. Redirect Check is already available from a number of CRAs who will also provide NCOA when it goes live.

The primary barrier to sharing the enhanced data (e.g. 'to' address data and more detailed output) as part of NCOA appears to be legal; data of this nature is classified as 'communications data' and as such access and dissemination is governed by RIPA which provides specific legal gateways for public sector investigations to gain access to this data. The NFA Information Sharing Team is currently liaising with Royal Mail Commercial and their legal advisors to clarify the legal issues and identify any possible solutions.

Further Information:

www.royalmail.com/portal/rm/jump2?catId=11800138&mediaId=56100696

Access to Death Data Records

The NFA Information Sharing Team is assessing potential sources of death data records to assist local authorities in preventing and detecting public sector frauds. This work may also benefit the private sector (e.g. combating pension fraud).

The project is currently in its early stages of planning but the NFA hopes to actively pursue this over the coming months.

Identity Crime

The Information Sharing team is currently conducting a strategic review of identity crime across the public, private and law enforcement sectors alongside key stakeholders. The work will focus on:

- identifying and implementing new opportunities for data sharing between public sector stakeholders
- providing the UK's first strategic threat assessment of identity crime and its social impact
- taking action against false ID document production
- addressing criminal abuse of copy birth certificates, driving licenses and passports
- improving personal data protection
- developing advice and guidance for victims of identity theft.

The NFA is pursuing an ambitious Action Plan and has commissioned an initial findings paper that will be used to brief Ministers on the importance of tackling identity crime. The Plan will also lay out a number of measures that should be taken to toughen up the UK's response.

INFORMATION SHARING AND THE INFORMATION COMMISSIONER'S OFFICE

The Information Commissioner's Office is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The role of the ICO is to enforce and oversee the Data Protection Act, the Freedom of Information Act, Environmental Information Regulations, and the Privacy and Electronic Communications Regulations.

Their main functions are:

- educating and influencing;
- promoting good practice;
- giving information and advice;
- resolving problems; and
- enforcing the above using legal sanctions against those who ignore or refuse to accept their obligations.[7]

The ICO publishes good practice notes, providing solutions to everyday questions or problems about how organisations should handle personal information. They also produce more specific Codes of Practice in consultation with trade associations and consumer or representative groups. These are designed to encourage good practice in a particular industry or activity that involves the handling of personal information.

The ICO has created a framework code to help organisations to adopt good practice when sharing information about people. The framework code is intended to be of use to all organisations involved in information sharing throughout the UK, including voluntary bodies, although some of it will be most relevant to public sector organisations.

The ICO has recently been tasked with producing a statutory code of practice for information sharing. Whilst this code will not be legally binding, failure to consider it will be taken into account by Courts or the Commissioner in relation to any breach of data protection law. Consultation on this statutory code is expected to begin by Autumn 2010.

Further information:

The ICO: www.ico.gov.uk/

ICO framework code of practice for sharing information: www.ico.gov.uk/for_organisations/topic_specific_guides/information_sharing.aspx

ICO Guide to data protection: www.ico.gov.uk/for_organisations/data_protection_guide.aspx

[7] It is important to note that the ICO *cannot* award compensation for any breach of the Data Protection Act or the Freedom of Information Act, apply for an injunction to prevent the disclosure of information, make one organisation pass on personal information to another, or stop another individual from keeping or using personal information about you for purely domestic reasons.

ICO Good Practice Notes:
www.ico.gov.uk/what_we_cover/data_protection/guidance/good_practice_notes.aspx

ICO Codes of Practice:
www.ico.gov.uk/what_we_cover/data_protection/guidance/codes_of_practice.aspx

The Personal Information Online Code of Practice:
www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_information_online_cop.pdf

The Personal Information Online Small Business Checklist:
www.ico.gov.uk/upload/documents/library/data_protection/practical_application/personal_information_online_small_business_checklist.pdf