Home Office

Guidance on the use of document scanners

Contents

Introduction

Document scanners provide a quick and easy way to establish the authenticity of documents presented for identity verification purposes. Scanners can play an important role in supporting front line staff to screen out counterfeit documents.

Scanners work by taking a high resolution image of an original document, using a dedicated reader, and comparing the facial image and security features embedded within the document to a database with data from many countries. They can be used, depending on the contents of the database, to authenticate Government issued documents, European ID cards and commercial documents such as concert tickets.

This paper sets out a consistent framework across Government departments and public sector bodies for the use of scanners and how organisations can gain the most benefit from this technology.

It is important for all organisations to comply with their own legal responsibilities, under the Data Protection Act, the Human Rights Act or any other relevant law. This guidance is not intended to provide legal advice to individuals or organisations. In case of any doubt legal advice should be obtained to cover individual circumstances. Some general guidance on the likely relevant law is set out in Annex C.

The Government is unable to endorse any particular product or type of product. It is important for organisations or individuals to ensure that any product they may use is appropriate for their needs.

Background

Counterfeit documents can be used for identity purposes and continue to be illegally manufactured, many to a very high standard, by professional fraudsters. Counterfeit documents have been successfully used by criminals to defraud private and public sector organisations of very large amounts of money and to create bank accounts which can be used as enablers to launder or hide unlawfully gained assets.

The exploitation of identity by criminals has a major role in underpinning a wide variety of organised criminal activity. Much of this crime targets the public sector and therefore the taxpayer through the falsifying of documents such as passports and driving licences in order to facilitate crime. This is a lucrative trade for criminals and there are highly organised operations exploiting state of the art technology. There are identity factories in most major cities and towns in the UK acquiring printing equipment to produce high quality counterfeits of official documents.

Scanners are already being used to authenticate documents presented to assert and prove an identity within parts of the NHS, a number of local authorities, the police and the private sector. Routinely sharing data detected by the use of scanners could significantly improve the fight to combat identity crime. Collation of false identity data would inform law enforcement activity to reduce the financial loss to both the private and public sectors. The use of scanners could enable more effective identification of counterfeit documents at the point of presentation, and sharing this data would further reduce public and private sector fraud.

How will scanners help?

Scanners should be seen as complementary to existing systems that departments and agencies have in place to tackle fraud. They broadly fall into two categories: those that provide an indication of whether the document is genuine or false, and those that provide information to the user but leave it to them to make the decision.

A key identity crime objective is to prevent and detect crime through data sharing of recovered fraudulent documents. Consultation with manufacturers, retailers and customers of scanner technology suggested that the appropriate use of scanners has the potential to detect fraudulent documents and generate data, which could then be shared to prevent crime.

Scanners may not identify some of the more sophisticated forgeries or photo substitutions and are unlikely to identify imposters (lookalikes). Scanners will never be a substitute for trained forgery officers, however, as a first line of defence, they are a useful tool for identifying fraudulent documents, are relatively easy to use and have proved to be a useful deterrent to criminals.

Scanners cannot be used as evidence for prosecution purposes but they can act as a filter which helps the user to decide how to handle a document or its applicant. In some cases this may involve referring the documents to law enforcement agencies such as the police, or the Home Office, where the user suspects that an offence has been committed under the Identity Documents Act 2010. The law enforcement agency would then obtain further evidence. Where a scanner is automatically linked to the Amberhill database, (which collates and shares information on false documents used for identity purposes), this is regarded as a ‘crime in action’ and can in itself generate a subsequent police response.

Some types of scanner offer more enhanced checking facilities than others. This can leave a margin for error and places greater responsibility for the decision on the user. When considering whether to utilise scanner technology, agencies and departments should ensure the functions of the particular scanner being considered delivers the required benefit, and weigh this against the purchase and ancillary costs. They would need to consider the purpose for which the scanner would be used and the level of knowledge of fraudulent documents amongst staff within their organisation.

Scanners are very effective when compared to a basic visual inspection by a person with no or limited training in examining documents. This is especially useful in front line functions where documents are produced to assert identity to staff who are not trained to a high level to recognise fraudulent documents.

Recommendation

The use of scanner technology by public and private sector organisations should be encouraged. Organisations can use this guidance to help decide whether to incorporate scanner technology to their existing processes. More detailed information is contained in the annexes to this policy.

List of Annexes

Annex A: Adopting scanner technology – issues to consider
Annex B: Implications of implementing this guidance
Annex C: Relevant legislation guide
Annex D: Example public sector data sharing agreement

Annex A

Adopting scanner technology – issues to consider:

How the technology may help them to protect themselves against fraud

There are systems available where:

- A database of all information captured which can be used for management reports and trend detection could be created.
- It may be possible for some Public Sector agencies to perform checks against other data sources that may be relevant to the department or agency such as the Interpol or crime stoppers lists.
- Users can create their own watch lists and, if the system allows, share these watch lists among other systems in their user groups at the touch of a button.
- It is also possible to create alerts that will help to enforce policy. It is possible for a system to provide a definitive response on the authenticity of the document in less than 3 seconds, which may be beneficial in high volume customer serving environments, particularly where exposed to high volumes requiring a yes/no approach.

Sharing of scanned false identity data

Confirmed false documents could be shared with a central database. The Amberhill database in the Metropolitan Police draws together data relating to false documents. Amberhill utilises identity scanner technology as part of its work and can receive data from identity scanners into its database for matching against other databases. Where this receipt of data identifies evidence of false or fraudulent documentation, it is treated as a ‘crime in action’. Amberhill is responsible for the management of the accuracy of its database in terms of complying with Data Protection principles. *(See also Section 5)*

This data is cross checked against other databases to identify fraud and deception in both the public and private sectors. The data is available to public and private sector organisations where a data sharing agreement exists, and thus supports existing systems that organisations have in place to tackle fraud.

Legal advice from the Information Commissioner’s Office on the use of scanners and the sharing of information

Prevention through collaboration by improving data sharing is encouraged. This includes the use of scanners to prevent individuals using false identities for criminal purposes and sharing false identity data obtained from scanners.

However each department or agency will need to ensure that it has addressed any potential legal issues regarding the data sharing of false identities, including any Human Rights considerations.

What to do when encountering potential false documents

a. When the individual is present

Only certain categories of person (for example a police constable) have legal powers to seize false documents. However, members of staff may request to retain a document identified as potentially false, and can advise the person that the police will or are being contacted. The health and safety of staff is paramount and where an individual insists, the produced documents should be returned.

Although the sharing of data with Amberhill may initiate a police investigation, the identification of a potentially false document should always be managed by contacting the local police, in accordance with each agency's locally developed best practice and guidance.

When involving the police, staff should hand to the police any original documentation, and any print outs from the scanner. The police would require a witness statement to support any arrest and/or prosecution.

The joint protocol for the delivery and presentation of evidence regarding travel document fraud is an agreed practice between the Home Office, the Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO). It sets out a process commencing at the point at which a suspect is arrested on suspicion of committing an offence involving a falsified travel document. A copy of this guidance is reproduced as **Annex C**.

b. When no persons are present

Scan data should be sent to Amberhill and physical documents should be securely stored and subsequently forwarded to the police. Ultimately, when the document is a genuine UK issued document, whether falsified or fraudulently obtained, it should eventually be returned to the issuing authority unless that authority gives permission for it to be retained by a third party.

Annex B

Implications of implementing this guidance

Procurement

No particular product, system or company can be officially endorsed. For the public sector, Government Procurement Policy and Procedures apply.

All procurement of information and communications technology goods and/or services that are considered to be a major project or are provided under an existing contract, should be undertaken through approved framework agreements. The final decision will be up to the contract issuing department. However, to ensure that common standards are adhered to across the Government and public sector, the Home Office will consider the feasibility of sharing details with partners of the minimum standards required for identity document scanners that have previously been used by public sector bodies running procurement exercises for these scanners.

Procurement departments should consider ensuring that the contract for an identity document scanner includes routine updating of the database as new documents are released, and the costs of this should be built into the business case. The scanners would also need periodic checks to ensure they are still operating within their requirements.

Financial

It is for each agency or department to consider what arrangement is most suitable when exploring the identity scanner market place. Suppliers may offer a variety of options ranging from outright purchase with licensing and support, through to a range of rental options.

Some scanner technologies allow information to be collected at source (the scanner suppliers). This can then be electronically supplied to Amberhill and such data sharing is encouraged. The advantage of this is that it is a wholly automated process and does not impose any administrative burden on the identity scanner customer and effectively take a false document out of circulation where document scanners are used.

Training and Guidance

Guidance and training on the day to day use of identity document scanners should be given to all staff with responsibility for using them. This should include:

1) What to do if there are concerns about the match of a person's face to the image in a document.
2) What to do about false alerts, for example, when an authentic document is flagged as suspect because it is damaged.
3) Guidance on how to identify lookalikes.

When purchasing or leasing a scanner, suppliers can provide training at the client site, at the suppliers HQ or remotely, as appropriate, to meet individual requirements. Initial, basic user training is provided upon installation and delivery and typically will last one to two hours providing a general system overview and 'how to scan' capability. In addition, some suppliers can offer more in-depth training for managers and advanced users.

Presentational

Encouraging the widespread use of identity scanners throughout Government will have a hugely positive benefit in terms of demonstrating the Government's commitment to reducing fraud in the public sector and its cost to the taxpayer. However, there may be concerns in Parliament and amongst the public, over the purposes of the increased sharing of identity information that would be entailed by more widespread use of identity scanners. There are also concerns amongst document experts that scanners do not provide a sufficiently high level of certainty as to whether a document is genuine or not:

- **Increased sharing of data** - The Government abolished identity cards and the National Identity Register in 2010 and has no intention of re-introducing a central system of recording and sharing the identity of all citizens due to its commitment to protecting individual privacy. Identity information could therefore only be shared if scanning technology first detected a counterfeit document in a person's possession. This 'false identity' data would then be shared through the existing central hub of information operated by Amberhill for crime prevention purposes only.

- **Reliability of scanners** – The limitations of scanners should be taken into account in their use. They are only ever a supplement to the experience of document experts, such as those in the National Document Fraud Unit in the Home Office, who would need to be called upon to adjudicate if there is doubt over whether a document is genuine or not, as part of an official investigation for prosecution purposes. However, scanners would provide an important first line of defence in the fight against document fraud. They will enable a much wider and consistent scrutiny of documents than is currently possible and where many staff handling a wide range of official documents cannot have sufficient expertise to recognise all kinds of fraudulent documents.

Legal

There are generally no major legal barriers to the sharing of fraudulent document data identified through the use of scanners as long as there are **adequate data sharing agreements** in place and the information is being shared for a specific purpose, namely for the prevention and detection of crime.

It is highly important that systems comply with codes of practice that have already been issued by the Home Office and the Information Commissioner's Office (ICO). Guidance is available on the ICO website via this link:
http://www.ico.gov.uk/for_organisations/guidance_index/data_protection_and_privacy_and_electronic_communications.aspx

Particularly relevant under the heading "Identity Scanning" is the following:
Restrict access to scanning system records to those whose duties require it i.e. Different user levels, with passwords that limit front line staff to only seeing the photograph of the ID and an easy to read interpretation on the documents authenticity. Detailed information and in depth analysis of documents should be restricted to senior management only.

However, it should be noted that The Data Protection Act 1998 does not cover false identity data. The presentation of a false identity to a public sector service is a crime. In effect, where a false identity has been captured, relaying that information to the police is equivalent to reporting the facts of a crime. It is recommended that a Data Sharing Agreement is always put in place where a Government department or agency wishes to share its false identity data with Amberhill.

To ensure compliance with Article 8 of the Human Rights Act, legal advice is that the use of scanning technology should be proportional to the threat of fraud it is trying to prevent. This can be done by putting measures in place to ensure that:

- The scanning equipment has been properly assessed against what it is required to do - suppliers could be advised by the Home Office National Document Fraud Unit.
- Staff using the equipment are given the appropriate training for its use and understand how improper procedure may throw up rejected document information. Staff would still need to undertake other manual checks to minimise impostor abuse and check for forged documents.
- Thresholds for what would be identified as a false identity document are set to an appropriate standard.
- Where scanned data contains details of hijacked identities interfering with the right to privacy and this is forwarded to Amberhill, they will help to manage the impact on the individual from these hijacked identities where possible.
- If considered appropriate, organisations wipe all scanned data every 24 hours to avoid any potential data protection breach. Specific policy should be determined by local legal departments.

Attached at **Annex C** is an overview of the relevant legal issues that need to be addressed and complied with. The use of scanners is compatible with existing legislation for the purposes set out in this policy i.e. the detection of counterfeit documents and sharing of false identity data to combat identity crime.

There is a specimen data sharing agreement at **Annex D.** This is a template based on existing data sharing agreements that have previously been successfully utilised by Amberhill. Agencies should seek advice from their own legal departments when entering into such agreements, to ensure the document used is appropriate to their business.

Equality Impact Assessment

It is our assessment that the equality impact of introducing scanners would be neutral. It would not discriminate against any group of people, but neither would it promote equality of opportunity or foster good relations as it is a technical solution which is aimed at existing procedures and the public will not perceive as any different. The effect should be beneficial to all individuals who are potentially subject to identity fraud. The mitigating factor must be that the use of identity scanners is an additional tool that improves or complements (rather than replaces) the existing systems in place to guard against criminal use.

Annex C

Public Sector Data Sharing for Prevention and Detection of Crime

Power to share data

When considering whether a proposal to share data is lawful, it is first necessary to consider whether the parties to the proposed arrangement have the necessary powers.

A public body may only share data if it has power to do so. The power may be set out expressly in statute, or it may be implied from the body's other statutory powers and functions. Government departments headed by a Minister of the Crown may also have common law powers to share data.

Sharing of personal data for statistical purposes

If the data to be shared is fully anonymised, then it will be less likely that problems should arise, though consideration still has to be given to the principles in the Data Protection Act 1998 (DPA). If the data required for statistical purposes contains information which may identify individuals (personal data), then the sharing should be approached in the same way as for any other circumstances.

The Data Protection Act 1998

If it has been established that the parties have the necessary powers, the next step is to consider whether the proposal is compatible with other legal provisions regulating the use of personal data.

The principal legislative provision relating to data protection is the Data Protection Act 1998 (DPA), which implements the Data Protection Directive 95/46/EC. The DPA gives individuals a number of important rights to ensure that personal information covered by the Act is processed lawfully. It regulates the manner in which such information can be collected, used and stored, and so is of prime importance in the context of data sharing.

Express statutory powers

Some legislation includes explicit 'gateways' by which information can be disclosed or received for particular purposes. Such gateways may be permissive (creating a discretionary power to disclose or receive data) or mandatory (requiring data to be transferred in certain circumstances).

Examples of permissive statutory gateways include (not exhaustive):

- section 115 of the Crime and Disorder Act 1998, allowing anyone to pass information to certain authorities if it is necessary or expedient for the purposes of any provision of the Act;

- section 17 of the Anti-Terrorism, Crime and Security Act 2001, allowing disclosures under the statutory provisions specified in Schedule 4 for purposes connected with criminal investigation and prosecution, where such disclosures are proportionate;

Common law powers

If there is no relevant express or implied statutory power to share data, government departments that are headed by a Minister of the Crown may be able to rely on common law powers to share data.

Ministers of the Crown have ordinary common law powers to do whatever a natural person may do, in contrast with bodies which have powers conferred on them by statute and no powers under the common law. Government lawyers have called this principle 'the Ram Doctrine' as it is explained in a memorandum by the then First Parliamentary Counsel Sir Granville Ram dated 2 November 1945. However, Ministers' common law powers may be extinguished by statute and may otherwise be limited by the requirements of public law, the law of confidence or by agreement.

In relation to data collection, use and sharing, reliance on common law powers by public bodies has not often been considered by the courts, so there might be an element of risk in such reliance. The degree of risk would depend on the facts, particularly the nature of the information proposed to be collected and disclosed, the purposes for which it was to be collected and disclosed and the identity of the bodies acting as recipients. It is worth noting that even where common law data sharing powers are compatible with Article 8 of the ECHR, they may still not provide a suitable basis for public sector data sharing for other reasons. Sometimes a statutory framework is necessary in order, for example, to impose criminal sanctions on officials for non-compliance.

Public bodies which are neither central government departments nor organisations which derive their powers from statute will need to analyse carefully what powers (if any) they have to process data and whether there are any explicit or implicit restrictions or limitations upon such processing. Because the powers available to any such body will almost entirely depend upon the specific nature of the body concerned and its legal status, it is impossible to provide general guidance on such cases.

Application of the Data Protection Act

'Data' includes all automatically processed information as well as some manual records.

'Personal data' means data relating to an identified or identifiable living individual. Anonymised data may still be personal data if the data controller can identify who the information relates to.

'Sensitive personal data' are personal data consisting of information as to racial or ethnic origin, political opinions, religious and similar beliefs, trade union membership, physical or mental health, sexual life, and the commission or alleged commission of any offence or criminal proceeding. The DPA imposes additional requirements in relation to the processing (including the sharing) of such data.

The *'processing'* of personal data includes anything which may be done to personal data, such as obtaining, holding, using, disclosing or destroying it. Many types of public sector data sharing will involve information held on computer, so if the information relates to identified or identifiable individuals, it will be clear that the DPA applies.

'Data controllers' are persons who determine the purposes for which, and the manner in which, the personal data are processed.

'Data processors' are persons who process personal data on behalf of a data controller, rather than on their own behalf.

'Data subjects' are the individuals to whom the personal data relate.

The data protection principles

The eight data protection principles set out in Schedule 1 Part I of the DPA form the core of data protection regulation.

The first principle: fairness and lawfulness

This requires that "Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless— (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met".

The second principle: purposes

"Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes."

The third principle: adequate, relevant and not excessive

"Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed."

The fourth principle: accurate and up to date

"Personal data shall be accurate and, where necessary, kept up to date."

The fifth principle: information not to be kept longer than necessary

"Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes".

The sixth principle: rights of data subjects

"Personal data shall be processed in accordance with the rights of data subjects under this Act."

The seventh principle: keeping personal data secure

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

The eighth principle: transfer outside the EEA

"Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."

The Human Rights Act 1998 and the European Convention on Human Rights

Data sharing by public authorities must comply with the European Convention of Human Rights (now part of the UK domestic law as a result of the Human Rights Act 1998), and in particular Article 8, which provides:

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

Data Sharing Agreements

It is strongly advisable to have in place a Data Sharing Agreement or Memorandum of Understanding to formally define the project, ensure that relevant considerations have been considered, and record the respective obligations of the parties.

Clauses that it may be appropriate to include in such an agreement are:

Shared data: a description of the information to be shared.

Purpose(s): the purpose(s) for which the sharing is taking place and consideration of why the sharing is proportionate to the purpose(s).

Further use of shared data: consideration should be given to what further use could be made of the data shared by those who receive it. Provisions may include preventing the recipient from processing the data for purposes other than those for which it is shared without the data controller's consent or for purposes which are incompatible with the purposes for which it was shared.

Roles: In most cases where public sector bodies share data, both the sending and receiving organisations will be using some or all of the data for their own purposes and both will therefore be data controllers of at least some of the data. The agreement should state which body is the controller of which data and how it will be shared and used. Where one body is a data controller and the other is a data processor in relation to all or part of the data, their respective roles should be defined. This approach will in part determine the responsibilities each party has under the DPA.

Legal basis on which data is being shared: a description of the legal powers that both organisations rely upon in order to share the data.

Security of shared data:

- Data controllers are responsible for the security of the data they hold. This responsibility requires the sending organisation to ensure that the information is kept secure during the sharing process, and they must also take reasonable steps to ensure it will be kept secure by the recipient.
- The agreement should set out an explanation of the security arrangements that will be in place in relation to the shared data such as any applicable security standard, permissible copies, confidentiality, the means of access to the information, storage facilities and encryption of data.
- Where data is sent to a data processor who will process data on the data controller's behalf, there must be a written contract in place which provides for the 7th data protection principle to be observed by the data processor as well as requiring the data processor to act only on the instructions of the data controller. (As previously mentioned, such data processing transfers are not usually considered data sharing).

Integrity of shared data: the obligations of the recipient of the data to preserve its integrity.

Freedom of Information: where one or more of the parties to the data share are subject to the Freedom of Information Act or the Environmental Information Regulations the agreement should provide for the parties to assist each other in responding to requests, e.g. by providing information where appropriate if it is in their possession, and for the co-ordination of any responses to such requests to ensure consistency.

Inspection: the data provider may want to retain oversight of how the data is being held and used.

Loss and unauthorised release: the steps to be taken if data is lost or released without authorisation. They could include a requirement for the recipient to report any loss as soon as possible and an obligation to conduct an investigation. The agreement may require the recipient to indemnify the provider of the data for all financial liability that may arise as a result.

Annex D

Specimen data sharing agreement

Title & Version	A purpose specific information sharing agreement between xx and xy.
Author	
Organisation	
Summary/Purpose	An agreement to formalise information sharing arrangements between xx and xy for the purpose of identifying criminal offence being committed by the use of false and fraudulently obtained genuine identity documents.

Information Sharing Agreement (ISA)

Between

xx

And

xy

For the purpose of identifying criminal offence being committed by the use of false and fraudulently obtained genuine identity documents.

Section 1. Purpose of the Agreement

This Agreement has been developed to:

- Define the specific purposes for which the signatory agencies have agreed to share information.
- Describe the roles and structures that will support the exchange of information between agencies.

- Set out the legal gateway through which the information is shared, including reference to the Human Rights Act 1998 and the common law duty of confidentiality.
- Describe the security procedures necessary to ensure that compliance with responsibilities under the Data Protection Act and agency specific security requirements.
- Describe how this arrangement will be monitored and reviewed. This should be after six months initially and annually thereafter**.**

In addition, completion of this document will ensure that the [name of organisation] can meet the information sharing requirements of [relevant departmental guidance].

This Agreement relates only to the sharing of the information for the Purpose, and is without prejudice to any other agreement that might exist between xy and xx.

The signatories to this Agreement will represent the following agencies/bodies:

xx

And

xy

Section 2. Specific purpose for sharing information

2.0 Introduction

2.1 Details of 1st party (known as xx) in this agreement (their remit, the background to how they are in possession of data that they are willing to share etc)

2.2 Details of 2nd party (known as xy) in this agreement (their remit and requirements for accepting data)

2.3 The purpose and scope of the information sharing arrangement:

The purpose of this arrangement is to determine the appropriate and mutual exchange of relevant information between xx and xy to protect the Public by enabling the respective agencies to discharge their responsibilities and fulfil their objectives.

This arrangement is necessary to ensure a shared understanding of the responsibilities of the respective partners, provide a substantive basis for the sharing of relevant information to the parties involved, and outline the process and mechanism for the provision of information at the appropriate time.

The arrangement will manage the results discovered by xx on comparing the data and the results discovered from sharing the data. These results could identify potential criminal offences and offenders whilst also disrupting other applicants for posts in sensitive employment.

The information that will be supplied both ways will be:

- xxxx

[Provide details of how the information will be shared]
[Provide details of what will happen to the shared data]

2.4 Objectives

This information sharing agreement will help to identify [e.g. criminal activity] with false identity documents. This will prevent persons form using these documents to:

- to gain by employment possibly with vulnerable adults or children by fraudulent representation in breach of the Fraud Act 2006;
- to commit offences under the Identity Documents Act 2010.
- to use fraudulently obtained genuine documents to commit Fraud and other related offences.

2.5 Benefits to 1st party

The benefits to the 1st party are as follows:
[For example]

- Crime, disorder, vulnerability and harm are prevented, disrupted and reduced;
- Improvement in security;
- Improvement in public confidence;
- Offenders are identified and brought to justice

2.6 Benefits to 2nd party

The benefits to 2nd party are:
[For example]

- Improvement to security and public reassurance;
- Assisting with the detection of crime;
- Reduced economic loss;
- Reduced crime.

2.7 Citizen Benefits

[For example]

- Ensuring the integrity of systems;
- Ensuring the integrity of the criminal justice system by showing the public that criminal offences and serious breaches of trust are identified, investigated and prosecuted giving full consideration as to whether criminal proceedings are necessary;
- Ensuring the prevention and detection of crimes.

2.8 How will this information sharing arrangement further those objectives?

[For example]
This arrangement will ensure that possible offenders who use forged, fraudulent and FOG identity documents to commit criminal offences are identified at the earliest possible opportunity, thus preventing them from causing harm to individuals and systems.

The information can be matched and potential abusers of systems identified and investigated and subsequently prosecuted/disrupted.

The sharing will detect a number of criminal offences i.e. S2 Fraud Act by False Representation, S3 Fraud Act of failing to disclose information, S4 Abuse of position and S6 Possession of an article for use in Fraud, that have been committed and will detect and disrupt future offences. This will reduce the risk of harm against individuals and financial companies.

This arrangement is necessary to provide an accountable management process to enable the partners in this information sharing agreement to distribute personal material in a lawful and proportionate manner. This agreement will establish the lawful purpose for the sharing of information and establish by which it will be defined.

The two-way sharing of Information between xx and xy will present opportunities to identify people who present a clear and present risk to the Public.

2.9 Information to be shared

1st party (describe)

2nd party (describe)

2.10 Does this information include personal data under the Data Protection Act 1998?

Yes

It is anticipated that part of this agreement will include that once the information has been passed to the relevant party they will become responsible for it. At the same time agreement will be sought regarding the following:

- They are clear as to what they are permitted to do with the information.
- They are clear as to how it should be handled (e.g. storing, maintaining accuracy, transmitting and deleting etc.)
-

This will be assured and evidenced in the Baseline Security Assessment later in this process.

Section 3. Legal basis for sharing and what specifically will be shared

Any Information Sharing Arrangement (ISA) must be underpinned by a firm legal basis. This document is intended to establish a legal basis for an operational information sharing agreement between xx and xy

The purpose of this ISA is to enable the appropriate exchange of information between the agencies concerned to enable them to carry out their respective responsibilities in relation to the prevention and detection of crime. This document is structured around the Data Protection Act 1998 (DPA). Where all 8 data protection principles are satisfied, the sharing of information will be lawful.

This ISA is completed for the sharing of Personal Data. This is information relating to an identifiable living individual and includes information that does not mention a name but could easily be linked to a person, like a warrant number or national insurance number.

3.1 First Principle

The first data protection principle states that data must be processed lawfully and fairly.

3.1.1 Lawfully

A public authority must have some legal power entitling it to share the information.
INDICATE: The primary power you are invoking to share this information.

1st Party (give details for example Common Law)

3.1.2 Duty of Confidence

If the 1st party has received any information in confidence, you almost certainly have a Duty of Confidence towards the data subject.

INDICATE: How any duty of confidence might be overridden.

Both sets of data have been received via legitimate means. It is information that contains personal details but these are included upon forged/falsified documents. There is therefore, no likely presumption of confidentiality.

However, any obligation of confidence is not absolute and can be overridden by several factors, one being to demonstrate that to disclose the information would be in the public interest.

In the circumstances outlined in Section 2 of this ISA there is an overwhelming public interest in sharing information in accordance with this agreement to ensure that the agencies involved are able to demonstrate and display the utmost professionalism, integrity and accountability to the law. This is paramount to ensure the trust and confidence of the general public in the xx and xy.

There are a number of potential examples of public interest factors that this agreement brings to the fore, which include; preventing the commission of criminal offences and bringing offenders to justice.

The consideration of proportionality and justification is provided by the serious nature of the potential offences against individuals as well as financial institutions.

3.1.3 Fair Processing

As previously outlined this data has been obtained by legitimate means. The subjects of this information have or have attempted to obtain false/forged/FOG ID documents and there is therefore no intention to issue Fair processing notices to them.

It would not be practicable to do so as to comply with Fair Processing requirements could prejudice the ISA by alerting the potential offenders to Police interest in them and their criminal offences. This could in turn cause them to avoid detection and subsequently prosecution for these offences. It could also bring their attention to the fact that the authorities were aware of their possession of false/forged/altered/FOG ID documents.

Therefore to support this information sharing agreement we would seek to claim an Exemption under Section 29 of The Data Protection Act 1998. If the purpose of the arrangement relates to the prevention or detection of crime or the apprehension or prosecution of offenders, it may operate under the exemption made available by Section 29(1) DPA 1998.

This removes the need to apply the fair processing conditions. The exemption applies where:

- To comply with the fair processing conditions would be likely to prejudice the purposes of the prevention or detection of crime and/or the apprehension and prosecution of offenders

The exemption is <u>not</u> a blanket one but it can be claimed in relation to the ISA as a whole and in relation to multiple transfers of information within the arrangement. However, the transfer of each category of information, on each occasion, must be shown to be for the purpose of preventing/detecting crime and/or apprehending or prosecuting offenders.

If as a result of the sharing, it is identified without doubt that the details shared relate to a subject who has had their identity stolen or hi-jacked then both the xx and xy recognise the duty of care to this person. At this time it is agreed that the fair processing exemption will no longer apply and the parties will accordingly send them a letter advising them of:

- The circumstances of the sharing
- The fact that their identity may have been hi-jacked or stolen
- Actions that they can take to check and protect against this being undertaken in the future.
- Relevant named individuals that they contact for further advice/information

3.1.4 Legitimate Expectation

An individual's expectation as to how information given to a public body will be used will be relevant in determining whether the first data protection principle has been complied with.

INDICATE: How the information sharing arrangement is consistent with the legitimate expectations of the data subject.

There are clear and legitimate policing purposes in the:

- Prevention and detection of Crime;
- Bringing offenders to Justice

This provides a common law basis to the sharing of information in accordance with this ISA. There are also clear Public Interest factors to the sharing of information in accordance with this information sharing agreement. These include:

- Preventing the commission of criminal offences and
- Bringing Offenders to Justice.

There is no objection to the normal xx practice of publishing the details of this ISA on the xx Publication Scheme so that members of the Public can see what is being done with this data.

3.1.5 Human Rights - Article 8: The Right To Respect For Private And Family Life, Home And Correspondence

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

INDICATE: How Article 8 of the Human Rights Act is to be satisfied.

Article 8 (1) rights are not absolute and should be weighed against the public interest, which may justify an interference with those rights. In conducting what is a balancing exercise between the rights of the individual and the interests and the good of the public at large, one must identify how the information sharing is:

- In pursuit of a legitimate aim (e.g. preventing or detecting crime - under statute or common law.
- Proportionate
- Appropriate and necessary to a Democratic Society.

Legitimate Aim

The purpose of this ISA is in pursuit of the legitimate aim of preventing and detecting crime, protecting property, and bringing offenders to Justice. It is also intended to support the public interest in maintaining the confidence of the public in the secure systems.

Proportionate

This agreement is proportionate to the legitimate aims as it ensures that the integrity of data systems are maintained thus ensuring that those involved in serious offences are identified and investigated and as a result prosecuted, prevented or disrupted.

Appropriate and Necessary

It is both appropriate and necessary to have such an information sharing agreement, as the public would expect the xx and xy to cooperate to achieve these goals.

3.1.6 Schedule 2, Data Protection Act 1998

In addition to the legal criteria set out above, the information sharing arrangement must satisfy **at least one** condition in Schedule 2 of the Data Protection Act in relation to personal data.

INDICATE: The Schedule 2 condition satisfied

This information exchange is necessary to achieve a legitimate interest (the investigation, prevention and detection of crime and disorder), therefore satisfying Schedule 2, paragraph 6(1), DPA 1998, which states that the data processing is necessary for:

"The purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms of legitimate interests of the data subject."

It may not always be practical or even possible to obtain consent before sharing information and it is not a pre-requisite, as long as another condition is satisfied. Moreover consent should ideally not be sought unless one is in a position to respect the refusal to grant consent.

3.1.7 Schedule 3, Data Protection Act 1998

If the information is "sensitive" (that is, where it relates to race, ethnic origin, political opinions, religion or belief system, membership of a trades union, physical/mental health or sexual life, the commission or alleged commission of any offence, proceedings relating to the offence) the ISA must satisfy at least one condition in Schedule 3.

INDICATE: How the Schedule 3 Condition is satisfied

As shown earlier the information shared within this ISA may relate to the commission or alleged commission of offences against various statutes and therefore for that reason is sensitive.

The processing of this sensitive personal information is satisfied by the personal data being processed in circumstances specified in an order made by the secretary of State (Schedule 3, Section 10 DPA 1998). These circumstances are defined in Statutory Instrument 217/2000 - The Data protection (processing of sensitive data) Order 2000, which provides for sensitive personal information being processed where:
"The processing is necessary for the exercise of any functions conferred on a constable by any rule of law"

3.2 Second Principle

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

INDICATE: How the agreement complies with this principle.

This information was obtained by legitimate policing techniques and for legitimate Policing purposes. Under this arrangement it will not be processed in any manner contradictory to that purpose. The purpose of the sharing is to allow both partners to identify any potential offenders, thus reducing the risk of harm.

The issue of third party onward transmission will be dealt with in the Baseline Security assessment, thus assuring that both parties are aware of their responsibilities in relation to the data shared and who they can forward the information to.

3.3 Third Principle

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

INDICATE: How the agreement complies with this principle

The information/data to be shared has been obtained by legitimate means. The information has come from xxxx and details of xxxx.

3.4 Fourth Principle

Personal data shall be accurate and, where necessary, kept up to date.

INDICATE: How the agreement complies with this principle.

This data will be subject to standard xx procedures to ensure that it is accurate and relevant. It will be the subject of normal xy procedures and validations intended to ensure data quality.

Both partners are reliant upon the accuracy of the data supplied by each other and therefore would find it difficult to identify any inaccuracies. Therefore any data to be shared with them will the subject of a Quality Assurance process by both teams prior to sharing.

The original information will be kept in an encrypted location and will only be accessible by those that require access. It will be subject to regular review and update to ensure that it is accurate and still relevant. Regular feedback and statistical analysis will be provided by both teams using secure email.

3.5 Fifth Principle

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

INDICATE: How the agreement complies with this principle.

The retention of information, including personal data, legitimately obtained and retained for the purpose of dissemination and investigation will be determined by standard xx policy and procedure.

Both teams are happy to be guided on the period of time that data can be retained. They will retain the data for a six month period to allow the checks to be completed and statistical analysis to be considered and prepared.

Written confirmation should be provided to the xy Contract Manager once secure destruction /deletion is completed.

3.6 Sixth Principle

Personal data shall be processed in accordance with the rights of data subjects under this Act.

INDICATE; How the agreement complies with this principle.

In order to comply with this principle the following will apply:

Partners to this arrangement will respond to any notices from the Information Commissioner that imposes requirements to cease or change the way in which data is processed.
Partners will comply with subject access requests in compliance with the relevant legislation. Section 29 (2) of the Data Protection Act 1998 enables fraud records to not be released as part of a subject access request in appropriate and restricted circumstances. The data shared as part of this agreement falls under these circumstances and so the data will be suppressed from subject access requests made to either xy or xx. The xx reserves the right to withdraw the right of use of the data at any time.

3.7 Seventh Principle

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

INDICATE: How the agreement complies with this principle

xy will ensure the safe transmission of the Data to xy in accordance with the Seventh Principle of the 1998 Act and the requirements of the Security Policy Framework.
xx will process the Data in accordance with the requirements of the Seventh Principle and the standards set down in the Security Policy Framework [and/or ISO17799]. These same requirements shall apply to the use by xy of any data processor to process the Data on xx's behalf.

Measures to satisfy the Seventh Principle are detailed in the Baseline Security Assessment document - prepared as part of the development of this agreement and included in the final section of the purpose specific agreement, "Description of Arrangements including security matters".

3.8 Eighth Principle

Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.

INDICATE: How the agreement complies with this principle.

The information provided under this agreement is not intended for transfer to any agency not party to this agreement and is not intended for transfer to any agency outside the European Economic Area.

xx agrees not to transfer the Data to any country outside the European Economic Area without the prior consent of xy, whether or not that transfer is to a data processor.

Section 4. Description of arrangements including security matters.

Supply of Information by 1st Party

How 2nd Party will use the information supplied to them

Supply of Information by 2nd Party

xy will share the data for the Purpose under s29 (3) of the Data Protection Act 1998. Xy will share the xxx data with xx as agreed between the parties.

It is an intrinsic condition of this agreement that any data supplied to xx by xy must be stored and utilised in accordance with the Cabinet Office Data Handling Review (June 2008) and any subsequent modifications

xy is obliged to comply with the Mandatory Minimum Measures as set out in the Data Handling Review published by the Cabinet Office. This covers the entire information lifecycle, including use and access under any commercial agreements

For clarity, the Recipient should be aware that guidance within the review stipulates that any source of information relating to 1,000 or more individuals will be deemed to be Protected Personal Data. As such, it must be safeguarded in accordance with the Mandatory Minimum Measures as summarised in Appendix A.

xx needs to be aware of and ensure that they comply with the storage and access of data supplied to them by xy. There are particular conditions surrounding Offshoring the data and also offshore access where it is stored in the UK. Please see Appendix B for more details.

> Where xy consider there to be a breach of these conditions of use xy reserves the right to suspend the service offering until appropriate evidence is supplied to allay concerns.

The terms "data", "data controller" and "data processor" as used in this agreement bear the same meaning as prescribed in section 1 of the 1998 Act.

Section 4(4) of the 1998 Act states that it is the duty of the data controller to comply with the data protection principles as listed in Schedule 1 of the 1998 Act. xx understands that once it is in receipt of the Data from xy it, separately, is a data controller for the Data and is responsible for complying with the principles of the 1998 Act in relation to its further processing of the Data.

By signing this agreement xx undertakes not to use the Data for any purpose other than the Purpose without the prior consent of xy, subject to any exemptions under Part IV of the 1998 Act.

Proportionality

xy is satisfied that the sharing of the Data is adequate, relevant and not excessive in relation to the Purpose.

xx will keep under review the range and volume of the Data that it needs to receive. The intention of the parties is to use the minimum amount of personal data necessary to achieve the Purpose.

Accuracy of the Data

xy will take all reasonable steps to ensure that the Data are accurate and up to date before they are transmitted to xy.

How 1st Party will use the information supplied to them

xx will retain the Data for a period not exceeding [X] years from the date on which xy provided it, subject to any exemptions under Part IV of the 1998 Act. [or specify other basis for retention]

At the end of the retention period, xx will arrange the secure destruction or deletion of the Data in accordance with the requirements of:

(a) the 7th Principle of the 1998 Act, [and]
(b) the Security Policy Framework [and/or]
(c) International Organisation for Standardisation (ISO) 17799 standards and
(d) Cabinet Office Data Handling Review 2008.

Disclosure of Information to individuals, the public or third parties

Either party will answer any subject access or other requests made under Part II of the 1998 Act that it receives for the Data.

Either party will answer any requests made under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004 that it receives for information that it holds solely as a result of, or about, this agreement. In all cases where such a request is received, both parties shall:

(a) Consult the other party before deciding whether or not to disclose the information;
(b) Allow the other party a period of at least 5 working days to respond to that consultation;
(c) Not disclose any personal data that would breach the principles of the 1998 Act; and
(d) Not disclose information that would prejudice either the security of the Data or the security arrangements of either party.

Both parties undertake:

(a) to respect the confidentiality of the Data and not to disclose it to third parties unless required to do so by law,

(b) not to disclose the Data, or any information contained in the Data, to third parties on a discretionary basis without first obtaining the other party's written consent, and

(c) to comply with any conditions that the other party may attach to the giving of such consent.

4.1 Risk controls measures - Countermeasures

4.1.1 Business Continuity

A xx Single Point of Contact (SPOC) will be allocated to maintain and review this agreement. Should the SPOC be unavailable for any length of time then this will be identified by the Office Manager and the responsibility re-allocated to cover for these absences.

The officer responsible at xy will be the first point of contact for the sharing of information.

4.1.2 Confidentiality and Vetting

The members of xx/xy who will be responsible for the receipt and checking of the Data are vetted by their companies and are the subject of a disciplinary code of conduct.

4.1.3 Compliance

Both teams will be responsible for ensuring that security controls are being implemented. Such as:

Only specified staff will be granted access to data
Data will be kept in a secure location when not being accessed by these members.
Data will be stored on a system with security controls and independent from other systems to ensure access is only by necessary and relevant people.
xx will designate which people within their organisation require and are permitted access to the data.

These security controls and compliance with them will be included in the annual review of this Information Sharing Agreement (ISA).

Audit and Inspection

Both parties reserve the right to carry out reviews of the other party's compliance with the terms of this agreement, and both parties agree to cooperate fully with any such review. Both parties will give 28 days notice of such a review.

Both parties agree to share with the other party the outcome of any other audits or reviews that have been carried out on its activities as a data controller, to the extent that they have relevance to the processing of the Data.

Both parties agree to notify the other party immediately if it is the subject of an assessment carried out by the Information Commissioner's Office under sections 41A or 42 of the 1998 Act, to the extent the assessment has relevance to the processing of the Data.

4.1.4. Sanctions

Any breaches in security, losses or misuse of the Data will be immediately informed to either partner by the other and will be covered by their respective disciplinary procedures. Both parties will keep the other party informed of any communications about such incidents with:

- the data subjects whose personal data are affected,
- the Information Commissioner's Office, or
- the media.

The breaches will be informed by telephone and confirmed in writing within 24 hours of it being discovered.

Any breaches of the security protocols will be covered by internal disciplinary processes which once considered and investigated are open to all the normal sanctions.

Both parties understand that when the data controller, it will be responsible for:
taking any action necessary to resolve the incident, and
any claim against them for compensation under section 13 of the 1998 Act that concerns the processing of the Data, and agrees to provide the other party with reasonable information about the substance and conduct of any such claim (such information to be held in confidence by the other party).

4.1.5 Training / Awareness

All members of staff that have access to the data will made aware of the sensitivity, the security protocols and their responsibilities prior to being given access to the material and this will be recorded within personnel processes.

4.1.6 Partner's Building and Perimeter Security

Both partners have secure premises with strong physical controls, which include: -

Security reception area.
Access controls on entrance past reception
Access controls on entry to team responsible for Amberhill data.
Perimeter lighting
CCTV cameras
Alarm system
Security guarding 24 hours a day.

4.1.7 Storage of Papers

Anything not kept on secure system shown at 3.8 below will be secured in locked cabinets or drawers or will be placed in a safe thus limiting access to those with a genuine need to know.

4.1.8 Storage of Information on Partner's System

Assurance have been obtained from both teams the data shared between them will be kept on password protected spreadsheets in a password protected folder, which will control access to those with a genuine need to know.

This system will capture an audit trail of successful and unsuccessful access to the system. There will be regular monitoring of the people who have access and also those who have gained access. The system will be changed as and when any member of staff with access no longer has a "need to know".

4.1.9 Movement of Information (Physically)

Should the need arise for the information to be moved physically, this will be completed by a trusted person in a locked container or package or by Secure Mail or secure courier in a sealed package with no protective marking shown.

4.1.10 Movement of Information (Electronically)

Both partners have access to a secure e-mail system. Any sharing of the information electronically will take place using this system. These emails will also be the subject of the relevant xx/xy Protected Marking System.

4.1.11 Disposal of Electronic Information

After each dissemination has been checked and concluded, or at the end of a six month period from the date of sharing, both partners will return the information l and will erase the material from the system using the standard delete option or overwrite the information using an approved software utility. This disposal will be the subject of review at each annual review of the information sharing agreement.

4.1.12 Disposal of Papers

Both teams have given assurances that once each set of papers have been completed they will be disposed of by use of a shredder.

4.1.13 Review

Each review will consider the following:

Key Contacts

It will be important to ensure that each organisation party to the agreement still holds correct contact details for the key personnel operating or managing the data sharing.

Usefulness/Purpose

All parties will consider whether the information sharing is proving useful, and that the purposes for which it was established are still relevant to the work of the organisations concerned. If the agreement is no longer useful it should be formally terminated.

Fit for Purpose

All parties will consider the range and volume of the Data, and the frequency at which they are shared, and whether the information exchanged is fit for purpose. Is the right information being shared at the right time and in the right way? If the data sharing is not working then the possibility of changing it will be explored, including the security arrangements governing the transmission, safe receipt and further use of the Data.

The arrangements that xx has in place relating to the retention of the Data.

Any audits that have been carried out that have relevance to the way that xx is processing the Data.

Legal Basis

All parties will investigate whether any relevant legislation has been amended, or any new legislation enacted that would impact upon the agreement. If changes have taken place, the agreement may need to be amended to reflect this.

Incidents (Process)

This will be an opportunity for anyone involved to discuss any problems that have arisen regarding the process of exchanging the information (e.g. has the data been exchanged on time, have there been any complaints about its use etc).

Incidents (Security)

This will be the opportunity for anyone involved to discuss any security incidents that have occurred (e.g. unauthorised disclosures, physical/IT security failures). Credible assurances should be provided that any failures have been dealt with. Regular failures in security are likely to lead to the termination of the agreement.

Renewal/Termination

At the conclusion of the Review all parties should either renew the agreement for a further year, or terminate it.

Costs

Both xy and xx are responsible for their own operational running costs relating to staffing, support and maintenance and technical support.

Section 5. Agreement to abide by this arrangement

The agencies signing this agreement accept that the procedures laid down in this document provide a secure framework for the sharing of information between their agencies in a manner compliant with their statutory and professional responsibilities.

As such they undertake to:
Implement and adhere to the procedures and structures set out in this agreement.
Ensure that where these procedures are complied with, then no restriction will be placed on the sharing of information other than those specified within this agreement.
Engage in a review of this agreement with partners six months after its implementation and annually thereafter.

This agreement does not constitute a legally binding contract, and may be terminated by mutual agreement or by either party giving three months notice to the other party of its intention to terminate.

Either party can terminate this agreement with immediate effect if the other does not comply with any of its terms.

Notwithstanding the clause above, any obligations of either party relating to payment of costs, data protection or data security shall remain in effect after termination of this agreement

We the undersigned agree that each agency/organisation that we represent will adopt and adhere to this information sharing agreement:

Agency	Post Held	Name	Signature	Date