IDENTITY DOCUMENT FRAUD INTELLIGENCE AND ITS BENEFIT TO UK SOCIETY

Trilateral Research

Index

Introduction

The objectives of this report are to:

1

EXPLAIN the societal importance of identity document fraud in the UK

2

PROVIDE evidence that intelligence sharing among private sector practitioners as well as between private sector practitioners and the public sector would provide a significant boost to document fraud detection and prevention

3

EXPLAIN the legal and ethical restrictions and opportunities for this intelligence sharing

4

IDENTIFY future trends in identity document fraud and to explain innovative solutions for their detection and prevention

Identity document fraud enables significant financial crime as well as serious and organised crime such as terrorism and human trafficking. In addition, fake and counterfeit documents used to gain employment facilitates illegal immigration and allows unskilled or dangerous individuals to take up safeguarding roles thereby providing access to the vulnerable.

As a consequence, enhancing its detection and prevention is of considerable benefit to UK society.

The Importance of Identity Document Fraud

In July 2020, arrests were made as part of an investigation into a suspected **£495,000** Coronavirus Job Retention Scheme ("CJRS") fraud[1], as well as in connection with fraudulent applications to the Coronavirus Bounce Back Loan Scheme ("BBLS") in excess of **£550,000**.[2]

However, £1m in a single month is only a small percentage of the cost of fraud annually in the UK. In 2017, experts calculated the total annual cost of fraud in the UK at over **£190bn**.[3] This amount is more than the government spends on health and defence combined, creating immense losses for both the public and private sectors.

Of this **£190bn**, **74%** of the fraud is committed against the private sector, **21.2%** against public sector, **3.6%** is against individuals and the smallest proportion at **1.2%**, is against charities.

Translating these percentages into financial costs:

- The private sector losses are estimated to cost **£140bn**;
- The public sector loss is an estimated **£40.3bn**;
- The loss to individuals is £6.8bn—an average of **£10,000** per UK family;
- The loss to charities (including charitable trusts) is **£2.3bn**.[4]

Substantial financial losses are not the only consequence of fraud. According to several sources, the production and use of fraudulent identity documents is a significant crime enabler facilitating a broad spectrum of forms of crime.[5] In fact, Europol has identified identity document fraud as a principal enabler of serious and organized crime such as terrorism, human trafficking and modern slavery, drug crimes, smuggling and irregular migration.[6,7,8] The perpetrators of the attack on the offices of Charlie Hebdo and a Jewish supermarket in Paris in 2015 used forged identity documents to obtain a consumer loan prior to the attacks.[9] Several of the terrorists involved in the 9/11 attacks in the US used doctored passports to enter the country.[10,11] Europol reports that organised crime groups make frequent use of forged or altered documents to traffic people into the UK and EU for the purpose of sexual exploitation, forced labour, and the removal of vital organs.[12]

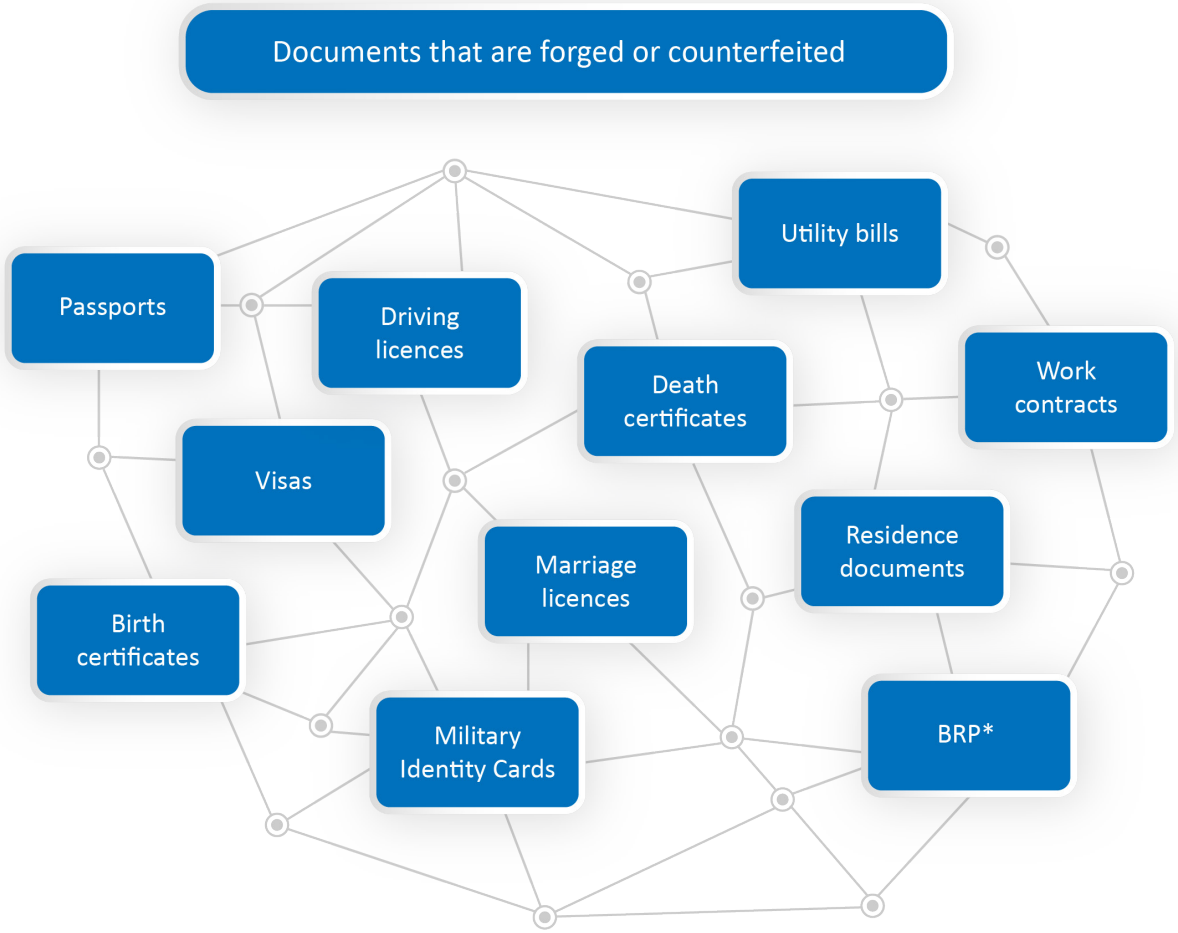
In addition to contributing to both sizeable financial loss as well as enabling serious organised and international crimes, identity document fraud poses a critical threat to UK domestic society. Individuals seeking victims among vulnerable populations can use fake and forged documents to apply for employment in safeguarding sectors such as the medical sector and childcare. A considerable amount of identity document fraud occurs in the construction sector[13] prompting concerns that workers without the requisite training and education are trusted with worksite safety as well as the safety of the wider public. This in turn has long term effects on the security of dwellings in which communities live and work.

Unlawful employment, benefit fraud and undeclared work cause major shortfalls in tax revenue and social security contributions. For example, in the UK in 2018/19 the net Government loss from benefits overpayments was 1.6% of benefit expenditure totalling £3.0bn.[14] In addition, these forms of identity fraud harm law-abiding employers and all of the workers who have to pay higher social security contributions in order to compensate for these losses. The workers who participate in such arrangements also suffer: they have to work under poor conditions, their employers do not comply with occupational safety rules and minimum wage rules, and they receive less protection and fewer social benefits. Finally, these harmful activities undercut competition: fraudulent practices allow companies to offer significantly cheaper products and services, which can crowd out law-abiding companies, precipitate the loss of legal jobs and hamper job creation.[15]

(A vendor sells fraudulent identity documents. Location unknown.] [Images taken from https://www.icao.int/meetings/mrtd-zimbabwe2012/documents/2-11-esteves_portugal-forensic.pdf)

Critically, the fraud stemming from right-to-work as well as right-to-rent applications is not isolated from financial fraud and fraud enabling serious organised crime. For example, migrants can be trafficked in order to provide labour, forced or underpaid, and organised crime organisations have been known to extort employers into engaging in fraudulent financial schemes.[16] For example, the recent Operation Fort, run by West Midlands police, uncovered the largest modern slavery network ever in the UK. It was revealed that gang members trafficked men for forced labour. The gang members also accompanied victims to banks to open one or more accounts, accompanied victims to job centres, applying for National Insurance numbers on their behalf, used forged utility bills, bank statements and other fake forms of identification to provide alternative addresses to where the victims were living, made fraudulent applications for benefits on behalf of the victims.[17] This also has long term impacts on the victims, whose credit history will have been impacted and consequently even when “rescued” from the traffickers, they may struggle to open up bank accounts or apply for benefits.

Which documents are most commonly faked and why are they difficult to detect?



*Biometric Residence Permits and Biometric Residence Cards issued by the UK

Graphic 1 : Documents that are forged or counterfeited

The geographic origins of fraudulent identity documents are diverse. This diversity creates a challenge in identifying fraudulent identity documents.

A single member of The Association of Document Validation Professionals (ADVP) in the UK reported the following results for checks performed over an 18-month period in 2018 and the first half of 2019.

Claimed Nationality	Jan 18-Jun 20
France	18%
Nigeria	15%
India	11%
Portugal	10%
Spain	7%

(Most common claimed nationalities found by an ADVP member 2018-2020.) (Data and graphics provided by ADVP)

In addition, several studies indicate that owing to internet and general technological accessibility and the prevalence of e-commerce transactions, identity document fraud has expanded.[18] Identity document traffickers have taken advantage of the ubiquity of internet sites and online markets in order to sell their products and reach customers around the world.[19]

Will the continued implementation of digital IDs and documents help?

With activities and debate concerning the creation and use of digital identities increasing, the digital identification of identity documents is pivotal to the development and enhancement of a UK digital ecosystem. By virtue of the identity document validation methodology being electronic, the following intelligence can be developed:

- The number of fake documents being detected.
- What type of documents are being detected.
- What security features are being defeated.
- What purported nationalities are being used.

At a strategic level, if multiple digital identity providers shared this intelligence via their electronic identity document validation provider, the intelligence could determine:

- Specific weaknesses in the ecosystem.
- Digital identity providers at higher risk.
- Variations in detection rates across different electronic validation solutions.

Although the further development and use of digital identity is a priority for the UK government[20], the digitisation of identity documents cannot be seen as a panacea for document fraud and its corresponding societal challenges. Even if the UK were to roll out a system to produce and check all digital IDs domestically for its residents and citizens, fraud associated with identity is an international problem involving people from foreign countries arriving, living, studying and working in the UK. It will take a significant amount of time for fully digitised IDs to be implemented across the globe. Authorities and document fraud specialists ought to expect a world in which a blend of paper and paperless identity verification is the status quo. A similar scenario has developed with money. Some societies have gone fully cashless (e.g. Norway); but owing to the international aspect of business transactions even these cashless societies must still be prepared to accept and process cash transactions.[21] Similarly, the UK ought to be equipped to continue to carry out document checks on paper documents for immigration, right to work and right to rent and other relevant checks.

Additionally, the digitisation of identity documents does not necessarily entail a decrease in fraud-related crime. Evidence has shown that as identity documents come to possess more technologically advanced security features, criminals change their modus operandi from forgery to counterfeiting.[22] Paper-based documents are easier to forge, e.g. by changing the name, dates or other numbers on

the document, but more difficult to counterfeit due to the watermark in the paper. New advances in ID documents make the documents more difficult to alter or forge, resulting in criminals counterfeiting the entire document (or card).[23]

How are these challenges currently being faced in the UK?

Employers have a legal obligation to check that prospective employees have a Right to Work in the UK. The rules related to preventing illegal working are set out in sections 15 to 25 of the Immigration, Asylum and Nationality Act 2006 (the 2006 Act), section 24B of the Immigration Act 1971, and Schedule 6 of the Immigration Act 2016.

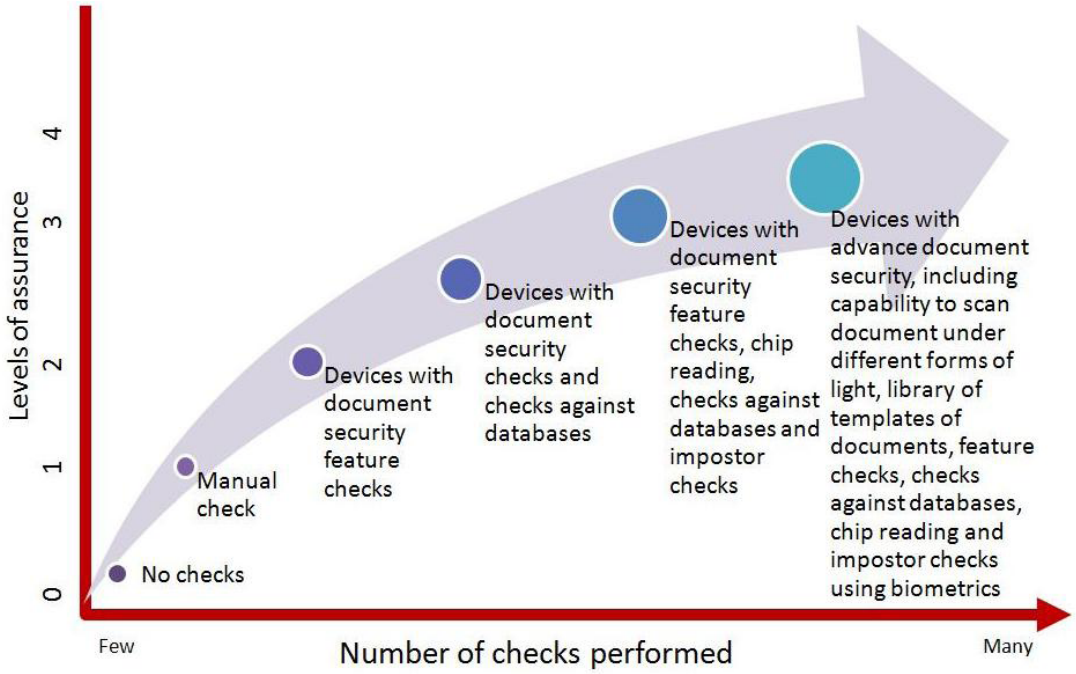
Failure to comply can result in a fine of up to £20,000 per person for each member of staff found not to have full right to work in the UK.[24] Criminal punishment might also follow. Serious or persistently non-compliant employers may face temporary closure of their business by immigration officers. The employer is then placed under special conditions to support compliance, as directed by the Court, and may be inspected by immigration officers.[25] Conducting the prescribed process appropriately establishes a statutory excuse in favour of the employer, protecting them from liability, even if the documents are later found to be fraudulent.[26]

Crucially the Home Office further clarifies that validation technology may be, and even ought to be, utilised:

> *"You may also wish to consider using commercially available document validation technology to help check the authenticity of biometric documents presented to you, notably passports and biometric residence permits (BRPs). There is no requirement that you do this in order to have a statutory excuse against a civil penalty, but using this technology is likely to increase the security of your checking procedures.[27]"*

Quote from the Home Office

The below diagram from the UK Home Office illustrates the importance of innovative technology to detecting document fraud.[28] The levels of assurance increase significantly as more advanced technology is used.



[A representative comparison of identity document validation technology and assurance levels provided by UK Home Office (2018)]

Despite these clear guidelines and significant punitive measures for noncompliance, as the above statistics make clear, the current system is not fully adequate to identify and detect a sufficient proportion of fraudulent documents for right to work application and in the public sector more generally. There are several factors that allow for significant gaps in the process.

01. There is no single effective database

There is no single effective database that collects fraudulent identity documents and that can be used as a resource to compare against new submissions of fraudulent identity documents for right to work, right to rent, or wherever documents are presented. Instead, the public sector has a number of intelligence databases with varying degrees of national coverage, each with a different dataset and different sources of updates.[29]

02. Excess Records

Records for individuals who are deceased, living abroad, or get divorced and change their names are not always cleaned and deleted from the national databases. In addition, human and technological error often result in duplicate records.[30]

03. Insufficient Sharing of Intelligence

In their report on ID fraud, the Cabinet Office emphasises several times that, "more data sharing within government could be a significant step to minimising fraud through the early prevention and detection of fraud."[31] Government offices are often too siloed creating obstacles to the detection and prevention of fraud.
For example, the National Audit Office (NAO) report on UK immigration enforcement found significant inefficiencies, redundancies and obstacles to immigration enforcement owing to the Immigration Office not routinely sharing intelligence among branches and teams.[32]

04. Under reporting

ADVP reports[33] that public sector checks account for around 30% of all of its checks performed. Despite making 244,000 checks, only 3 fakes were reported in H1 2019. Applying a Fake Rate of 0.10% (lower than any other sector) would result in 244 fakes. Hence, it is reasonable to conclude that not all forgeries and fakes are being reported by public sector clients or are being reported along multiple separate reporting channels.

05. Repeat Offenders

Repeat offenders remain a common occurrence, with fraudulent documents frequently presented at multiple businesses, banks, universities, etc. This implies that offenders are not being reported to police, or if they are being reported, no action is being taken.[34] It is reasonable to conclude that this occurrence is a direct result of problems 1, 3, and 4 listed here. Owing to the use of multiple databases, insufficient sharing of intelligence and under reporting, fraudsters are able to present fraudulent documents multiple times.

06. Insufficient education and training

To detect fraudulent identity documents, stakeholders such as police, employees at companies performing document identity verification, as well as clerks at banks or the post office need to improve their understanding and awareness of fraudulent identity documents as well as their detection capabilities.[35] As many of these individuals are laypersons, they do not always have the expertise necessary to detect fraudulent identity documents, especially those utilising sophisticated methods of forgery or counterfeiting.

07. Inadequate Deployment of Technology

While the deployment of electronic validation technology has become more widespread, it remains unclear whether the correct technology is being deployed to mitigate known risks. ADVP reports that counterfeiters are increasingly able to defeat some basic security checks (such as MRZ algorithmic checks) used by certain Cloud-based validation systems.[36] The validation capability of a Cloud-based system that can check the MRZ against a library of images is lower than that of a physical document being presented to a trained user utilising a three light (visible, UV and infrared) document reader.

However, detection rates can be influenced, not only by the use of differing technologies, but also owing to differing operational settings and differing contexts in which document validation is carried out. First, operational settings such as ease of use, cost and client acceptance of a particular technology can influence detection rates. Second, the quality of fake documents presented to evidence Right to Work in the UK construction sector may be much lower than those potentially used in the contexts of serious organized crime and terrorism. Given these multiple variables affecting detection rates, the sharing of intelligence concerning context, level of risk, quality of fakes and technology employed is necessary to determine whether the most suitable validation technology is being used in a particular environment.

Fraudulent immigration documents are not limited to passports. Verification of travel documents will not be enough to secure the borders, because valid UK and EU travel documents can be obtained with false breeder documents (e.g., marriage record or birth certificates). Thousands of different types and models of breeder documents[37] have been issued in the last 100 years and they usually contain little to no security features. Counterfeiting or forging these documents is relatively easy and may lead to obtaining a genuine EU or UK passport with a forgery, counterfeit or with a stolen identity document. In order to prevent legitimate documents such as passports or residency permits being obtained with fraudulent breeder documents, an integral automated solution will be required that includes breeder document authentication and verification.[38] As of today, no such automated solution for breeder documents exists.

08. New Threats

The current system for preventing and detecting identity document fraud must either be already equipped to confront new and emerging threats, or be flexible enough to adapt to such threats. One of the most critical challenges regarding the market for fraudulent identity documents is that the majority of transactions occur on the darknet.[39] The international scope combined with the anonymity of the sellers and buyers has established a lucrative market for fraudulent documents on the darknet.

09. Public Sector Lack of Agility

Researchers at McKinsey & Company found that public sector agencies lack the agility that is required to respond to novel and changing factors in society.[40] Three essential

factors contribute to this incapacity: cultural aversion to risk, functional silos and organisational complexity. "In essence, bureaucratic public-sector institutions lack the speed and nimbleness to keep pace in a rapidly changing world."[41] As new modus operandi of identity document fraudsters and new technological means for forging and counterfeiting identity documents become increasingly apparent, the ability to develop prevention and detection methods rapidly and with agility is critical.

Responses to these challenges: A Roadmap

01. A Single Intelligence Database

If the use of multiple separate databases entails multiple separate datasets and varying degrees of national coverage, then a single intelligence database that collates the intelligence from these multiple databases would make significant progress towards verifying documents and identities and preventing fraud. Especially significant would be that a single intelligence database could receive updates and technological advances avoiding the problem of multiple siloed databases with varying levels of technological readiness. Furthermore, the existence of a single intelligence database might also mitigate the problem of under reporting as employers and other identity document checkers will have a single point of contact to report their findings.

02. Sharing Intelligence

This solution helps facilitate the establishment of a single comprehensive intelligence database, it provides the solution to excess and incomplete records, repeat offenders, facilitates the sharing of training thereby lowering cost per agency, and, as a direct result, proves to be of considerable benefit both to practitioners of identity document checks, and, most importantly, to the public sector and society more generally.

In most contexts, empirical research has shown the market and economic benefits of sharing both knowledge and know-how. Forbes reports that Fortune 500 companies lose at least $31.5 billion a year by failing to share knowledge.[42] When a knowledge sharing structure is working well, the right people receive the right information at the right time. Also, they know where to look and how to share. From a management perspective, this means streaming information cleverly, to maximise its value without overwhelming the company's staff.[43]

The benefits of sharing knowledge and know-how within a single company are analogous to those in the context of business consortia as well. These include:[44]

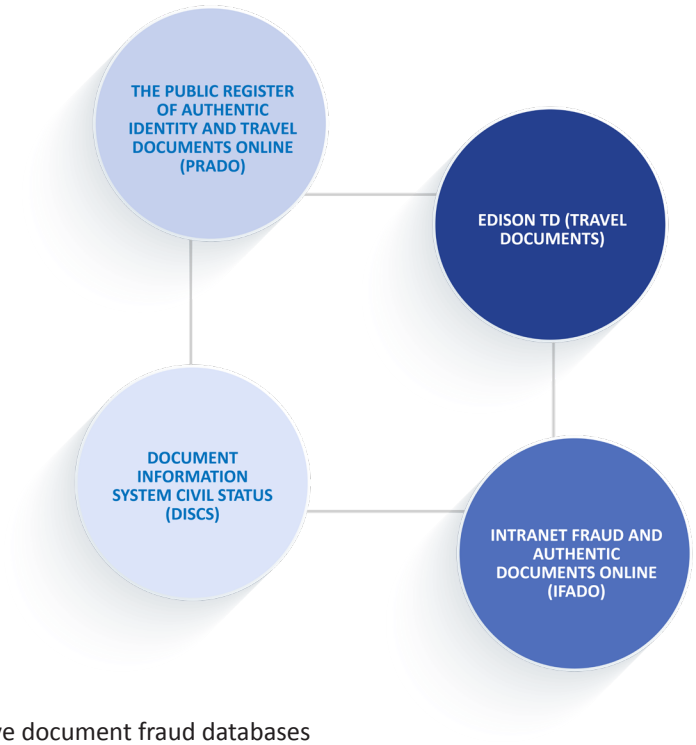
- Innovation & development
- Alignment among partners
- Faster response time
- More efficient communication
- Reduction of redundancies

The benefits of sharing and cooperation are supported by game theory.[45] In the classic prisoners' dilemma (PD) scenario, two individuals are arrested and suspected of committing a crime. Each suspect has two options; to confess to committing the crime or to remain silent. Each suspect must choose one of these two options without knowing which option the other suspect has chosen. The dilemma is that the fate of both of the individuals is dependent on their own choice as well as that of the other. If one remains silent and the other confesses, the sentence could be harsher for the one who was silent. Conversely, if only one confesses, the sentence may be lighter—as long as the other does not confess. If both remain silent, the suspects might be released owing to lack of evidence.

The question of whether to cooperate in sharing intelligence among businesses shares some characteristics with the classic PD scenario. Even with a contractual agreement in place, one business might not trust that its potential partner will reciprocate. As a consequence, the outcome of the decision to cooperate also depends on the decision of the potential partner, hence the bilateral game. As with the PD scenario, absent the actions of the potential partner, a business has more to gain if it acts only to protect its own interests. Acting unilaterally increases gain and decreases risk only if a business can manage to keep its own intelligence for itself while also receiving intelligence from others. However, this ideal situation is not realistic. In reality, siloed intelligence remains incomplete, or, even worse, erroneous. As a result, by acting unilaterally a business has more to lose. Consequently, if both businesses cooperate with one another, each maximises its gains and mitigates its risks for loss.[46] Moreover, if private sector companies collaborate with public sector agencies, the public sector entities can serve as a guarantor of cooperation thereby further promoting advantageous results for all parties involved.

Excess and incomplete identity records and repeat offenders: By sharing intelligence and even compiling shared intelligence into a single database, excess and incomplete identity records as well as repeat offenders of fraud have a significantly higher chance of being detected.

Several EU countries as well as the United States and Canada, have already proven that such shared databases of fraudulent documents are effective for detecting and preventing document fraud. Interpol reports that these databases provide essential help to their law enforcement officers in preventing document fraud in real-time.[47] Recognising the efficacy of such databases, the European Council adopted conclusions on 18 December 2017, which prioritise continued cooperation and information exchange among Member States to align practices concerning document fraud and identity management.[48] The collaborative databases include:



Graphic 2: Current collaborative document fraud databases

The Public Register of Authentic Identity and Travel Documents Online (PRADO)

is a database created by the Council of the European Union, contains information on travel and ID documents and selected security features. The database is maintained by experts of EU countries together with experts from Iceland, Norway and Switzerland.

Edison TD (Travel Documents)

is a database of travel documents and other travel-related documents from most countries in the world. The database is developed by the Dutch authorities in cooperation with the authorities in Canada, Australia, USA, United Arab Emirates and Interpol. The content is available in English, German, French, Spanish, Dutch and Arabic.

Document Information System Civil Status (DISCS)

is a web-based reference database developed by the authorities in the Netherlands, Canada, Australia, United Arab Emirates and Norway (the Norwegian National ID Centre). DISCS aims to support the verification of foreign and national documents containing information on civil status, identity, nationality as well as other matters concerning the holder of the document. DISCS includes information on genuine and forged breeder documents, amongst others identity cards, birth, marriage and death certificates, citizen's certificate and driving licence etc.

Intranet Fraud and Authentic Documents Online (iFADO)

is owned and operated by the Council of the European Union and the information is published by EU Member States, Iceland, Norway and Switzerland. The website contains key information on security features in genuine identity and travel documents, visas and stamp printing in the EU as well as in a number of third country documents. The database also contains information about false documents.

03.

Collaboration with Law Enforcement and wider UKGOV Agencies

Not only sharing intelligence, but particularly the sharing of intelligence between private sector companies that provide identity document fraud detection and public sector agencies including law enforcement agencies is a crucial step towards detecting and preventing identity document fraud for several reasons.

- Several reports show that to significantly combat document crime, focus ought to be shifted away from prosecution and should instead target enhancing the detection of identity document fraud through intelligence-led policing. Private sector companies engaging in "smart" forensic document examination methods could share their data with law enforcement agencies, thereby providing a crucial boost to law enforcement.

CASE STUDY

A trial collaboration between industry practitioners within the consortium Association of Document Validation Professionals (ADVP) and the Metropolitan Police (MPS) in relation to the Amberhill database on false identities and identity documents has already provided strong evidence to support the importance of continuing such collaborative efforts between the private sector and law enforcement in the future. ADVP placed fake documents into the Amberhill database. Criminals applied for employment at businesses, schools or hospitals. The employers sent the applications to Disclosure and Barring Service (DBS). DBS confirmed with Amberhill, and the applicants were prevented from gaining employment. Critically, the results of this collaboration prevented multiple criminals from taking on safeguarding roles.[49]

04.

Private Sector Agility

The private sector can address the lack of capacity for agility characteristic of the public sector (described under Challenge #9).[50] Through its innovation and ability to respond nimbly and rapidly to changes within the identity document fraud context, private sector companies are pivotal to developing robust solutions to current and new societal and technological challenges.[51] But this advantage held by private sector companies need not stay within the private sector. Applying private sector innovation and agility with the public sector interest in preventing and detecting identity document fraud would create a significant benefit for UK society.

> *"Collaboration between public and private entities creates better and more effective public and private services and products. Collaboration enables the participants to exchange and share knowledge, experiences, know-how and expertise. Collaboration helps to bring a broader set of skills and talents and a more responsive work culture into public sector organisations, along with innovative thinking and creativity; it also helps private companies to innovate more effectively and to achieve their concrete goals in a more efficient way."*[52]

Quote from the Home Office

05.

Training and Education

Rather than relying on the training of company employees and bank and post office clerks to detect identity document fraud, private sector companies can provide this service thereby lowering the cost of training while simultaneously significantly raising the accuracy of detection of fraud. Indeed, the UK Home Office recommends that companies outsource identity document fraud detection to experts in the field.

> *"IDVTs (Identity Document Validation Technologies) can play an important role in preventing the use of fraudulent documentation. Whilst they do not replace forgery experts, they provide higher levels of accuracy and assurance than the manual checking of documents by staff not used to checking different forms of identity documents."*[53]
>
> Quote from the Home Office

Ethical and Legal Considerations of Sharing Intelligence on Document Fraud

- The UK Home Office strongly encourages the sharing of intelligence concerning document fraud to enhance the prevention of crime.

> *"The Information Commissioner's Office (ICO) has confirmed that there are no legal barriers to the sharing of fraudulent document data identified through the use of IDVTs as long as you have adequate data handling procedures in place and that the information is only being shared for a specific purpose, namely for the prevention and detection of crime and/or immigration abuses."*[54]

Quote from the Home Office

> *"Where a fraudulent identity from a document has been captured, relaying that information to the police or Immigration Enforcement is equivalent to reporting the facts of a crime or abuse of immigration laws."*[55]

Quote by Ibid

- The purpose of preventing crime includes preventing people from using false identities for criminal or illegal immigration purposes.

- To be legally and ethically compliant, the sharing of data must be in support of the state's legitimate interest in crime prevention. As a consequence, it is recommended that an explicit agreement be sought after and completed between a law enforcement agency focused on document fraud, such as Metropolitan Police-Amberhill, and any private sector agency performing document checks.

Even if there is an agreement in place with a law enforcement agency, the private sector company is itself not a law enforcement agency and, hence, is not exempt from duties to fulfil data subjects' rights.

The General Data Protection Regulation (GDPR) Art.14[56] states that if personal data has been received from someone other than from the individual data subject, the recipient has the obligations as Controllers to provide the data subject with the following information:

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the data protection officer, where applicable;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data.

Furthermore, it is critical to note that the use of technologies to detect fraud must be proportionate to the intended purpose and must be GDPR compliant.

The Home Office lists the following measures[57] to keep in mind:

- staff using the equipment are given the appropriate training on its use
- you can restrict access to the IDVT records and analysis to those whose duties require it
- there is an audit and access-logging function, which enables tracking of the users who have accessed the data

- you can assess the IDVT to ensure it meets the intended purposes
- where the IDVT is capable of automatically sharing data on fraudulent identity documents with law enforcement, that the service provider has a data sharing agreement in place with them
- the IDVT provider has measures in place to reduce the risk of its technology being misused
- thresholds for what would be identified as a false identity document are set to an appropriate standard, so that the system does not produce too many false positive or negative results
- where scanned data contains details of hijacked identities, Amberhill will help to manage the impact on the genuine owner of that identity where possible
- unless recorded data needs to be retained for a specific purpose, for example as evidence of a right-to-work or right-to-rent check, you should be able to delete data in accordance with local data policies that enable you to comply with relevant legislation on data retention.

The ethical opportunities for establishing a single effective database of fraudulent documents, sharing intelligence and establishing an enduring collaboration with law enforcement are unambiguous.

As described above, document fraud is a crucial enabler for a multitude of serious and organised crime such as terrorism and human trafficking. It is also responsible for significant financial losses including fraudulent applications for social benefits. Finally, it allows unskilled or dangerous individuals to find employment in the medical, childcare, or construction sectors.

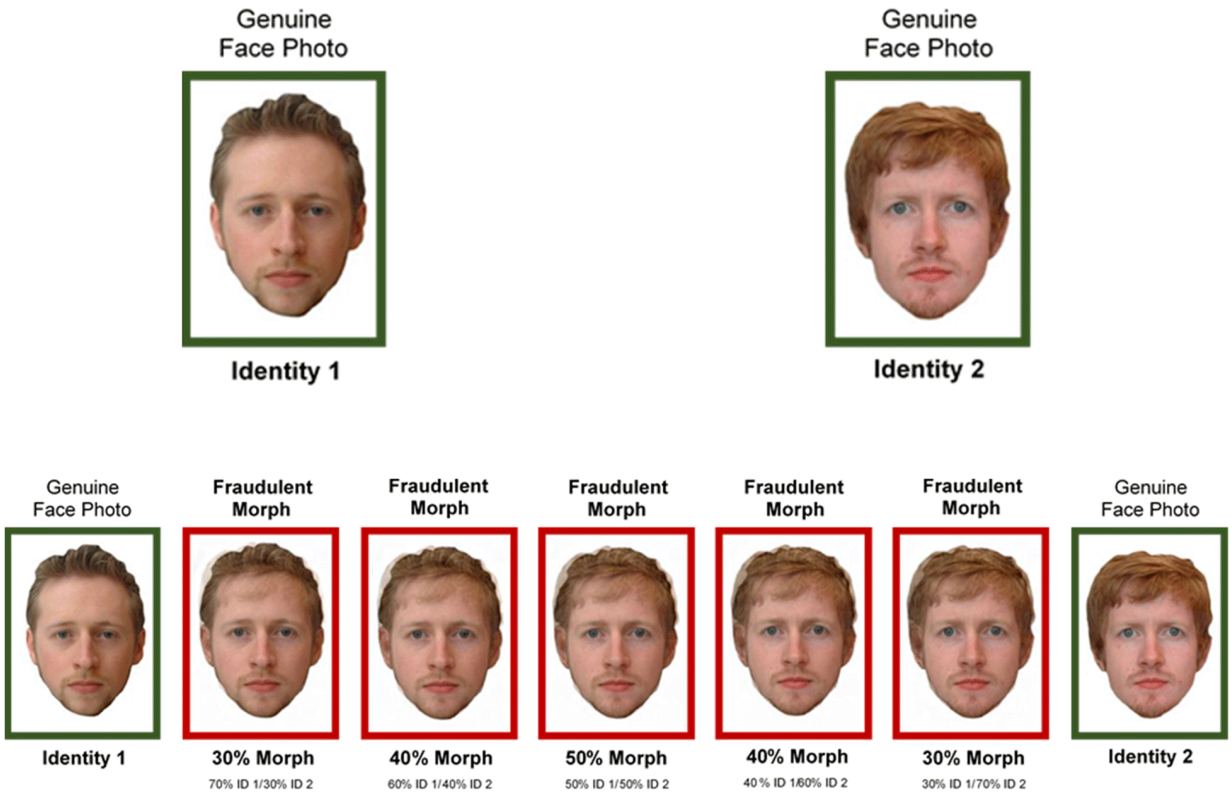
Preventing these crimes from occurring has enormous societal benefit. Improving and increasing document fraud detection will protect and promote the dignity of potential victims of trafficking and forced labour, protect the wellbeing of UK citizens and residents against future acts of terrorism, and save billions of pounds annually in financial fraud that can be used for domestic improvements to infrastructure and education.

The Future

New Challenges

The methods of spoofing identity document validation technologies have become increasingly diverse and difficult to detect. In addition to traditional methods of forgery and counterfeiting, the following newer methods have been detected by authorities:

Picture morphing: Photographs can be manipulated (morphed) in such a way that multiple people can use a single document without being recognised correctly. Recent studies have shown that an intermediate frame in a morphing (transforming and blending) between two face images of different people fools commercial biometric verification systems to match both people with this morphed image[58], and even trained humans can be fooled by such morphed images.[59]
As morphing in itself is not illegal, only when it is used for fraud, there are several commercial websites that provide easy access to photo morphing software.



(Stages of morphing two photos. (Robertson et al. 2018).)

Imposter fraud: A lookalike can use a stolen document to pass a document verification check.

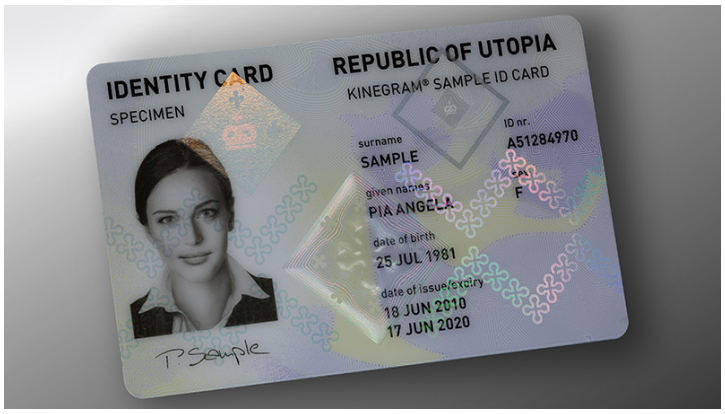
This is the same person.

These are **not** the same person.

(Photos of the same person (above) and different people (below) (UK Home Office 2015).)

Presentation attacks: Even if a stolen document cannot be used for lookalike frauds, offenders may still use the document for verification by an automatic verification system. They could artificially reproduce the biometrics of the former document owner, e.g. using a high-quality mask or elaborate cosmetics.

(A person wearing a 3D mask. Image taken from http://www.urmesurveillance.com/urme-prosthetic)



Cryptographic weaknesses in security features of passports and other identity documents, e.g. keys associated with embedded chips can be exchanged, Kinegrams altered or destroyed, etc.

(ID Card with Kinegrams and embedded security features. Image taken from https://www.kinegram.com/en/protecting-identities/id-and-dl-cards/)

> *"In order to address the challenges associated with digital transformations, human-machine coupling should become of prime interest to researchers and policy makers, with the aim to combine the best of human expertise with that of machines and artificial intelligence."*

Quote by Baechler 2020

Although these new forgery and counterfeit methods are technologically advanced and difficult to detect with many of the fraud detection methods currently in use, new artificially intelligent (AI) algorithms can be designed to detect them.

Detecting Morphing

Since the discovery of this vulnerability of biometric verification systems, several research groups tackled this method of spoofing under different aspects and developed detection methods. The first detection approaches in this field are often limited to different properties of the data or still highly conceptual, but nevertheless promising.[60] The majority of morphing detection techniques rely on detecting changes of the statistical image characteristics, e.g. image degeneration (loss of high frequency details), or changes caused by JPEG-double compression etc.[61] These can be detected using machine learning methods on a set of fixed features[62] or features learned by a Deep Neural Network (DNN).[63,64]

Currently there exists no representative and publicly available reference data set of morphed face to evaluate and rate morphing detection algorithms. NIST recently announced a call for morphs to create such a dataset.[65] Creating a single and comprehensive database of these images would be of significant benefit.

Detecting Fraudulent Breeder Documents

Practitioners could design an AI algorithm based on Deep Neural Networks (DNNs) to automatically detect anomalies, such as a document number that does not correlate with issuance date, paper quality, printing techniques and ink. To be successful the AI would need to exploit a large digital collection of thousands of reference breeder documents and fraudulent documents. As suggested above, practitioners could build a comprehensive library of document templates suitable for authenticating documents against a library of pre-processed image templates, to apply machine learning for authentication.

3D Face Recognition

3D face comparison has the potential to improve reliability and security over state-of-the-art 2D face recognition systems, which can be manipulated or spoofed with printed photographs, videos or masks; it is also resilient to pose and illumination variations. Prior work has demonstrated the significance of particular facial features for both verification and identification, including both geometrical and topological. Practitioners could develop novel methods to automatically extract such particular facial features based on deep learning. Specifically, recent research[66] can be exploited to process 3D meshes for machine learning.

Cryptographic Fraud Detection

Similarly, anomaly detection through AI to detect cryptographic elements of a document—e.g. which document signer key was used by which country at what time—could significantly enhance the detection and prevention of document fraud. As with the prior solutions, this approach requires a single comprehensive database of templates and documents for the AI to learn from.

Concluding Remarks

This report has outlined the case for continuing and enhancing intelligence on identity document verification to prevent fraud. The detrimental effect of document fraud to UK society is pronounced. Document fraud is an enabler for serious and organised crime such as terrorism, human trafficking, smuggling and forced labour. In addition, it costs the UK approximately £190bn per year. Although it is clear that the production and use of digital IDs and other digital documents continues to rise, predictions of a fully digital society are overstated. It is considerably more realistic that the UK will need to continue to conduct a mix of digital and document checks. Even if the UK society becomes more digitised, authorities and employers will still need to perform identity document checks for applicants coming from other countries with less widespread digitisation. Furthermore, collecting and sharing intelligence concerning identity document fraud and identity verification will play a central role in the evolution of the digital ID ecosystem in the UK and position the industry to face future challenges.

Given the significant importance of the effects of document fraud to UK society, it is of considerable significance to enhance capacities to detect and prevent document fraud. First, practitioners of document checks would benefit from sharing intelligence with each other. Second, the public sector would benefit from collaborating with private sector experts in document checking and intelligence sharing. As evidenced throughout this report, this collaboration is essential to implementing an agile approach to a serious and rapidly changing societal issue. These steps would result in an increase in detection and prevention of current document fraud crimes as well as the design and development of methods to counter new and innovative means of forging and counterfeiting documents.

Author

Zachary J. Goldberg is a Senior Research Analyst and part of the Applied Research and Innovation team at Trilateral Research. His research background and areas of expertise are in applied ethics and moral, political, and social philosophy. His current research interests and projects focus on the ethics of border security and migration including identity document verification, the ethics of surveillance, responsible research innovation, and the value and nature of privacy.

TRILATERAL RESEARCH

Trilateral Research is a UK and IE-based enterprise, founded in 2004. Our rigorous research is at the foundation of our work. We provide regulatory and policy advice; develop new data-driven technologies and contribute to the latest standards in safeguarding privacy, ethics and human rights within the public and private sector. Our teams collaborate across the technology-social disciplinary divide, being able to assess the impact of emerging technologies to avoid adverse and unwanted consequences while delivering sustainable innovation. We focus our efforts on areas where the application of our research can make a difference in enhancing societal wellbeing.

The Association of Document Validation Professionals is a trade association representing companies that provide electronic validation of identity documents in the UK. Its members deploy a wide range of technology solutions that are used across the public and private sectors to check millions of identity documents every year for a multitude of purposes including remote onboarding of customers or employees. The ADVP commissioned Trilateral to undertake this independent study and welcomes its findings.

advp

Notes

[1] *Prytherch and Brown 2020.*

[2] *O'Conner 2020.*

[3] *Mothershaw 2017.*

[4] *Ibid.*

[5] *Delval 1998; Egmont 1999; Friedrich 2001; Gordon and Willox 2003; Martinez and Sher 2010; Miro and Curtis 2003; National Commission on Terrorist Attacks upon the United States 2004; Ombelli and Knopjes 2008; Pontell 2002; Rudner 2008; Schloenhardt 1999; Smith 2003; SOCA 2009; UNODC 2010a, b; Webb and Burrows 2009; Willox and Regan 2002.*

[6] *Baechler 2020, 1;*

[7] *Europol Press Release 13 Sept 2017.*

[8] *Europol Statement 2020.*

[9] *Ibid.*

[10] *US Govt Staff Statement No. 1*

[11] *Zill (NDA)*

[12] *Europol Statement on Trafficking in Human Beings*

[13] *An ADVP Member 2019, H1 Report*

[14] *Dept for Work and Pensions 2019.*

[15] *German Federal Ministry of Finance, Statement 2019.*

[16] *O'Connor 2020.*

[17] *Crates 2020.*

[18] *Brongers 2003; Romagna 2014, 2015; Smith 2003.*

[19] *Yar 2005.*

[20] *UK Gov News Story 1 Sept 2020.*

[21] *Baechler 2020.*

[22] *Baechler and Margot 2016; Baechler 2020.*

[23] *Keesing ID Academy 2018.*

[24] *UK Home Office Statement on Penalties for Employing Illegal Workers*

[25] *See Section 38 and Schedule 6 of the Immigration Act 2016.*

[26] *See Page 1 UK Home Office Statement on Penalties for Employing Illegal Workers*

[27] *Employer's Guide 15.*

[28] *UK Home Office 2018.*

[29] *Cabinet Office, ID Fraud: A Study (2002), 24.*

[30] *Ibid., 25.*

[31] *Ibid., 29.*

[32] *Notes just: NAO 2020*

[33] *Data has been extracted from two sources: Server data from an ADVP Member's Cloud services, covering scans performed by all of an ADVP member's Cloud services customers and potential customers running trials; Amberhill data: Covers scans performed by the majority of an ADVP member's Desktop, Desktop Plus and Mobile customers. NB: This ADVP member's, Desktop Plus and Mobile customers who do not use Amberhill have not been included in this study. These customers represent approximately 10% of all Desktop and Mobile customers. The negative impact of this is reduced as the above mentioned ADVP solutions are installed across the full range of industry sectors and therefore affects them all to an equal degree. Cloud data does not include data from law enforcement tests or from customer trials where "test fake" images were being used.*

[34] *An ADVP Member, Document Intelligence Report H1 2019.*

[35] *Baechler 2020.*

[36] *An ADVP Member, Document Intelligence Report H1 2019.*

[37] *Breeder documents are documents used to support applications for identity, residence and travel documents, such as birth, marriage and death certificates.*

[38] *ICAO Trip Guide on Border Control Management 2018.*

[39] *Ciarniello 2020; Holm 2017; Keesing Platform 2015.*

[40] *Dowdy et al. 2017.*

[41] *Ibid.*

[42] *Forbes 2012.*

[43] *Ellium 2019.*

[44] *Ibid.*

[45] *Munton and Fredj 2013.*

[46] *Ibid., 677-678.*

[47] *https://www.interpol.int/en/Crimes/Counterfeit-currency-and-security-documents/Identity-and-travel-document-fraud*

[48] *Council Doc. 12004/1/17 of 27 November 2017.*

[49] *Heaton 2000; Ratcliff 2008; Baechler 2020.*

[50] *Sourced from ADVP interview, November 2020.*

[51] *Dowdy et al. 2017.*

[52] *Mergel 2018.*

[53] *Cankar and Petkovšek 2013.*

[54] *UK Home Office (2018).*

[55] *Ibid.*

[56] *GDPR, Art. 14.*

[57] *Home Office 2018.*

[58] *Ferrara et al. 2014.*

[59] *Robertson et al. 2017.*

[60] *Seibold et al. 2018.*

[61] *Neubert 2017.*

[62] *Raghavendra et al. 2016.*

[63] *Seibold et al. 2016.*

[64] *Raghavendra et al. 2017.*

[65] *NIST 2020.*

[66] *http://geometricdeeplearning.com*

References

Baechler, S., & Margot, P. (2016). Understanding crime and fostering security using forensic science: the example of turning false identity documents into forensic intelligence. Security Journal, 29(4), 618–639.

Baechler, S. (2020). Document Fraud: Will Your Identity Be Secure in the Twenty-first Century? European Journal on Criminal Policy and Research, Special Issue: Fraud in the 21st Century.

Brongers, D. (2003). Genuine(ly) unreliable passport – how to obtain a second identity. Keesing Journal of Documents & Identity, 2, 16–17.

Cabinet Office (2002). Identity Fraud: A Study.

Cankar, S., and Petkovšek, V. (2013). Private and Public Sector Innovation and the Importance of Cross-Sector Collaboration. The Journal of Applied Business Research, 29(6), 1597-1606.

Ciarniello, A. (2020.) Financial Fraud: 7 Critical Dark Web Threats and How to Find Them Fast. Ecosec.net
https://www.echosec.net/blog/financial-fraud-7-critical-dark-web-threats-and-how-to-find-them-fast

Crates, E. (2020). OPERATION FORT: What businesses should learn from the UK's largest anti-slavery prosecution. IASC.
https://www.antislaverycommissioner.co.uk/resources/

Department for Work and Pensions (2019). Fraud and Error in the Benefit System.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/801594/fraud-and-error-stats-release-2018-2019-estimates.pdf.

Delval, P. (1998). Faux et fraudes : la criminalité internationale des faux documents. Presses Universitaires de France.

Dowdy, J., Maxwell, J.R., Rieckhoff, K. (2017). Organizational agility in the public sector: How to be agile beyond times of crisis. McKinsey & Company Report.

Egmont. (1999). In G. Coles, J. Brown, L. Nieuwenkamp, & G. van Dijk (Eds.), 100 cases from the Egmont Group. Toronto: Egmont Group.

Elium Blog (2019). 15 benefits of Knowledge Sharing.
https://elium.com/blog/benefits-of-knowledge-sharing/

Europol (2017). Experts Meet to Tackle Document Fraud as Key Factor in Serious and Organised Crime and Terrorism-Press Release. 15 September 2017.
https://www.europol.europa.eu/newsroom/news/experts-meet-to-tackle-document-fraud-key-factor-in-serious-and-organised-crime-and-terrorism

Europol (NDA(a)). Crimes and Trends-Forgery of Administrative Documents and Trafficking Therein. https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/forgery-of-administrative-documents-and-trafficking-therein

Europol (NDA(b)). Crimes and Trends-Trafficking in Humans. https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/trafficking-in-human-beings

Ferrara, M., Franco, A., and Maltoni, D. (2014). The Magic Passport, IJCB.

Friedrich, E. (2001). Fälschungskriminalität und Prävention – Sicherungstechnische Anforderungen an Ausweisdokumente. Kriminalistik, 55(4), 271–277.

General Data Protection Regulation (2018). https://www.privacy-regulation.eu/en/article-14-information-to-be-provided-where-personal-data-have-not-been-obtained-from-the-data-subject-GDPR.htm

German Federal Ministry of Finance, Statement on Act to Com¬bat Un¬law¬ful Em¬ploy¬ment and Ben¬e¬fit Fraud 3 July 2019 https://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Priority-Issues/Articles/2019-07-03-Act-Combat-Unlawful-Employment-Benefit-Fraud.html

Gordon, G. R., &Willox, N. A. (2003). Identity fraud: a critical national and global threat (A Joint Project of the Economic Crime Institute of Utica College and LexisNexis, a Division of Reed Elsevier Inc.). https://www.lexisnexis.com/presscenter/hottopics/ECIReportFINAL.pdf.

Heaton, R. (2000). The prospects for intelligence-led policing: some historical and quantitative considerations. Policing and Society, 9(4), 337–355.

Hein, E. (2017). The Darknet: A New Passageway to Identity Theft. 6 International Journal of Information Security and Cybercrime 41.

ICAO TRIP Guide on Border Control Management (2018). https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20TRIP%20Guide%20BCM%20Part%201-Guidance.pdf

Keesington Technologies (2015). Cybermarket for forged identity documents. https://platform.keesingtechnologies.com/cybermarket-for-forged-identity-documents/

Martinez, J. A., & Sher, K. J. (2010). Methods of fake id obtainment and use in underage college students. Addictive Behaviors, 35, 738–740.

Mergel, I. (2018). Agile Innovation Management in Government: A Research Agenda. Government Information Quarterly 35(2), 291-298.

Miro, R. J., & Curtis, G. E. (2004). Organized crime and terrorist activity in Mexico, 1999–2002 - Report (L. of C. Federal Research Division under an interagency agreement with the United States government (ed.)). Washington D.C.: Federal Research Division, Library of Congress. National Commission on Terrorist Attacks upon the United States.

Mothershaw, N. (2017). Fraud still costing the UK more than £190bn – new analysis released in the Annual Fraud Indicator. Experian Identity & Fraud.

https://www.experian.co.uk/blogs/latest-thinking/identity-and-fraud/fraud-costing-uk-more-than-190bn-released-annual-fraud-indicator/

Mothershaw, N. (2017). Fraud still costing the UK more than £190bn – new analysis released in the Annual Fraud Indicator. Experian Identity & Fraud.
https://www.experian.co.uk/blogs/latest-thinking/identity-and-fraud/fraud-costing-uk-more-than-190bn-released-annual-fraud-indicator/

Munton, D. And Fredj, K. (2013). Sharing Secrets: A Game Theoretic Analysis of International Intelligence Cooperation. International Journal of Intelligence and CounterIntelligence, 26: 666–692.

National Audit Office, Immigration Enforcement. HC 110 Session 2019–2021 17 June 2020.

Neubert T. (2017). Face morphing detection: An approach based on image degradation analysis, IWDW2017.

NIST: https://pages.nist.gov/frvt/html/frvt_morph.html

O'Connor, N. (2020). UK: First arrests made in connection with alleged Coronavirus Bounce Back Loan Scheme fraud. Bird & Bird News Centre.
https://www.twobirds.com/en/news/articles/2020/uk/first-arrests-made-in-connection-with-alleged-coronavirus-bounce-back-loan-scheme-fraud

Ombelli, D., & Knopjes, F. (2008). Documents: the developer's toolkit. Lisboa: Via Occidentalis International Organisation for Migration. Pontell 2002; Rudner.

Prytherch, J., Brown, A. (2020). UK: HMRC announce their first "furlough fraud" arrest - only a concern for a small few? Bird & Bird News Centre. https://www.twobirds.com/en/news/articles/2020/uk/hmrc-announce-first-furlough-fraud-arrest

Quast, L. (2012). Why Knowledge Management Is Important To The Success Of Your Company. Forbes Online.
https://www.forbes.com/sites/lisaquast/2012/08/20/why-knowledge-management-is-important-to-the-success-of-your-company/#687078d63681

Raghavendra R., Raja K. B., Busch C. (2016). Detecting morphed face images. BTAS2016.

Raghavendra R., Raja K. B., Venkatesh S., Busch C. (2017). Transferable deep-CNN features for detecting digital and print-scanned morphed face images, CVPRW2017.

Ratcliffe, J. (2008). Intelligence-led policing. Portland: Willan Publishing.

Robertson D. J., Kramer R. S. S., Burton A. M. (2017) Fraudulent ID using face morphs: Experiments on human and automatic recognition. PLoS ONE 12(3): e0173319.

Robertson, D.J., Mungall, A., Watson, D.G. et al. (2018). Detecting morphed passport photos: a training and individual differences approach. Cogn. Research 3(27).

Romagna, M. (2014). The cyber-market of identities: criminological analysis on the illegal market of identity documents within the surface Web and Onionland. Utrecht University. Master thesis, Utrecht.
Romagna, M. (2015). Cybermarket for forged identity documents: the illegal trade of identity

documents on the surface web and in Onionland. Keesing Journal of Documents & Identity, 47, 12–15.

Schloenhardt, A. (1999). Organized crime and the business of migrant trafficking. Crime, Law and Social Change, 32, 202–233.

Seibold C., Samek W., Hilsmann A., Eisert P. (2017). Detection of face morphing attacks by deep learning, IWDW2017.

Seibold C., Hilsmann A., Eisert P. (2018). Reflection analysis for face morphing attack detection, Proceedings of the 26th European Signal Processing Conference, July 2018.

Smith, R. G. (2003). Travelling in cyberspace on a false passport: controlling transnational identity-related crime. The British Criminology Conference: Selected Proceedings, 5. http://www.britsoccrim.org/volume5/004. pdf.

SOCA. (2009). The United Kingdom threat assessment of serious organised crime 2008/9. Section "Identity fraud and false documents, intellectual property crime and currency counterfeiting", § 280-287.

An ADVP Member, 2019 H1 Intelligence Report. (Confidential).

UK GOV News Story (2020). Next steps outlined for UK's use of digital identity. 1 Sept 2020
https://www.gov.uk/government/news/next-steps-outlined-for-uks-use-of-digital-identity

UK Home Office Statement on Penalties for Employing Illegal Workers
https://www.gov.uk/penalties-for-employing-illegal-workers

UK Home Office (2015). Guidance on Examining Identity Documents.

UK Home Office, Guide to Identity Document Validation Technology, 28 March 2018.
https://www.gov.uk/government/publications/identity-document-validation-technology/identification-document-validation-technology#fnref:6

UK Home Office (2019) Right to Work Checks: An Employer's Guide
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773780/An_employer_s_guide_to_right_to_work_checks_-_January_2019.pdf

UNODC. (2010a). Guide for the development of forensic document examination capacity. United Nations Office on Drugs and Crime.

UNODC. (2010b). Smuggling of migrants: a global review and annotated bibliography of recent publications. Vienna: United Nations Office on Drugs and Crime.

US GOVT Staff Statement No. 1, Entry of the 9/11 Hijackers into the United States.
(https://govinfo.library.unt.edu/911/staff_statements/staff_statement_1.pdf

Webb, S., & Burrows, J. (2009). Organised immigration crime: a post-conviction study. Home Office Research Report, 15.

Willox, N. A., & Regan, T. M. (2002). Identity fraud: providing a solution. New York: Economic Crime

Institute, LexisNexis.

Zill, O. (NDA). Crossing Borders: How Terrorists Use Fake Passports, Visas, and Other Identity Documents. Frontline-Trail of a Terrorist.
https://www.pbs.org/wgbh/pages/frontline/shows/trail/etc/fake.html