

## **Tackling the threat from Identity crime**

### **Introduction**

ID crime is the creation of a false identity or the misuse of a genuine identity. It is a cross-cutting enabler used to commit further criminality, evade detection from law enforcement and launder criminal profits.

The threat is significant and growing. Threat analysis by the City-of-London Police in 2015 found that the criminal production of false documents and digital credentials is extensive and an established and lucrative criminal enterprise. There has not been another strategic threat analysis since, but Cifas figures show that identity fraud has grown by 32% in the last five years.

Despite the growth of this cross-cutting enabler of illegal migration, terrorism, fraud and other serious crime, the UK response is poor, siloed and uncoordinated. The private and third sector offer a range of checking services and advice, whilst government departments and law enforcement provide thematic services and responses whilst failing to consider identity as a significant enabler of criminal attacks on these services.

Identity crime is complex and extensive, and requires a cross sector, cross government coordinated response. The attached appendix shows some of the organisations and departments across all UK sectors that have an interest in identity.

### **The current situation**

No individual or team in either the public sector or the private sector is taking a holistic approach. Where does responsibility lie for the strategic oversight necessary to ensure a coordinated and effective approach?

The Department for Digital, Culture, Media and Sport leads on a digital identity framework which has checking identity as a key requirement. It references fraud prevention and disseminating intelligence to government but misses opportunities to utilise significant intelligence that would support this because identity crime intelligence is not properly collected and shared. If the government does not address this issue, then there is a risk that the UK digital infrastructure could be undermined from day one.

The Cabinet Office and Government Digital Service Good Practice Guide 45 is guidance on how to check someone's identity. However, the guidance makes reference to levels of assurance that can only be achieved by access to training by government bodies that is not available and government databases that cannot be accessed by the private sector validation industry that is undertaking hundreds of thousands of checks on behalf of private businesses and government departments every month.

The Home Office no longer has a cross-cutting policy team looking at the security of identity. It now focusses on illegal migration, whilst other departments within the Home Office focus on its own business without considering opportunities to tackle the identity crime threat in a collaborative way. The National Crime Agency no longer references identity crime as an enabler in its National Strategic Assessment. The Disclosure and Barring Service (DBS) manages the safeguarding threat. DBS highly values the Metropolitan Police false document database Amberhill as a vital source of intelligence, yet the Metropolitan Police has significantly reduced the capacity and capability of Amberhill, and the database is not networked and is under-utilised.

Better intelligence sharing is critical. The national intelligence picture is incredibly poor and there is no effective national database for collecting, collating and sharing data. Data is collated by the police via both Amberhill and the Know Fraud database in the City-of-London Police, by immigration Enforcement, by Cifas and the Fraud database and by private companies involved in electronic validation. However, legislation, the interpretation of legislation and simply the capacity, capability and willingness to share intelligence across these organisations and others such as the government departments that issue government documents prevents the sharing of intelligence that could significantly enhance the UK response to the Identity Crime threat.

The existing legislation that enables law enforcement and other agencies to effectively deal with identity crime is not well known and not fully utilised. Also, a lack of legislation that compels the passing of identified fake documents and identities to law enforcement adds to the lack of intelligence and capability of law enforcement to pursue criminals. Too often GDPR is an obstacle, despite the fact that information can be shared if it is about the preventing and detecting of crime, and where the credentials and documents are fake and therefore not personal and private information.

Polls and studies confirm that the public are fearful of identity crime, especially impersonation. They suffer harm, and this is exacerbated by the difficulties faced when trying to repair their identity.

The private sector has the electronic validation industry, advisory and not-for profit organisations each dealing with a part of the problem.

The Association of Document Validation Professionals (ADVP) is a trade association representing companies that provide electronic validation of identity documents in the UK. The ADVP has also been engaged in much of the work around the development of a UK digital identity ecosystem. The UK Identity Fraud Advisory is a social enterprise focussing on supporting victims and businesses because there is little ability for victims to repair a compromised identity. Cifas is a not-for-profit organisation that is the leading UK fraud prevention service, and particularly focussed on identity crime.

In the same way that the public sector is fragmented and uncoordinated, the private sector is operating in isolation from each other and the government, with overlapping objectives and duplication of effort.

There are exceptions where bilateral relationships such as those between a single ADVP company and Amberhill have demonstrated the benefits of partnership working and intelligence sharing. This good practice needs to be properly evaluated, acknowledged and built upon without hinderance by lack of capacity, legislation and conflicting priority setting.

### **Why this matters now**

The traditional threat from organised crime and individuals across fraud, immigration, terrorism and other crime remains and is potentially growing.

The development of a digital framework offers the potential for a criminal to exploit government services in a way not previously possible and it is vital that onboarding is as robust as possible to avoid compounding the identity crime by legitimising a digital identity.

The intelligence collated by the private sector provides a new insight into the level and methodology of the criminal exploitation of false and fake identity that was never previously available and offers an opportunity for collaboration and intelligence sharing that has not existed.

### **What can be done**

The single overarching priority must be to reduce the prevalence of the misuse of identity. Better verification and authentication processes and techniques highlight more fraudulent documents and credentials. A holistic strategy and common approach across government and the private sector that recognises best practice and enables the sharing of intelligence would increase the understanding of the threat and inform ways to reduce it.

This paper seeks to find a minister and/or senior civil servant to support the principle of the need for a better coordination of a response to the prevention and detection of those that seek to exploit the misuse of identity for whatever purpose. figures across government

A round table discussion of interested parties would be a logical next step, with a view to the appointment of a single point of contact who has a responsibility for overseeing the better coordination of all aspects of identity whether digital or analogue.

**Appendix – Organisations, departments and bodies with an interest in identity**

<b>UK Government</b>		
Main Department	Sub-Department	Interest
Cabinet Office/Government Digital Service		Protecting government platforms, products and services from fraud. Good Practice Guide 45 and how to check someone's identity.
Department for Digital Culture Media and Sport		The UK digital and identity and attributes trust framework and the prevention of onboarding a person with fake credentials.
Home Office	Immigration Enforcement	Persons attempting to enter and remain in the UK as imposters.
	Border Force	
	Disclosure and Barring Service	Detection of applicants using fake identity and credentials.
	National Crime Agency	The National Strategic Assessment has previously recognised identity as an enabler for organised crime, and the criminal production of documents and credentials is itself organised crime.
Her Majesty's Passport Office		Prevention of fraud by reducing the number of successful fraudulent applications for a passport.
Driver and Vehicle Licensing Agency		Prevention of fraud by reducing the number of successful fraudulent applications for a driving licence.
Department for Work and Pensions		Prevention of fraud by reducing the number of successful fraudulent applications for a National Insurance Number.
Her Majesty's Revenue and Customs		Identity fraud is an enabler for repayment fraud committed against and investigated by HMRC.

National Health Service		Identity crime in areas such as payroll, use of the European Health Insurance Card for access to services, and registration for accessing drugs and services.
Companies House		The registering of companies using a fake identity for the purposes of committing fraud.
Security Services		The use of a fake identity is a recognised tactic for terrorists and features in many recent acts of terrorism to enable the movement of terrorists.
Law Enforcement (Also Home Office)	National Policing generally	To ensure offenders are identified as part of processing and charging.
	City-of-London Police	Lead force for the National Policing Identity Crime Portfolio. Also, identity is a significant enabler of fraud and is of interest in relation to Action Fraud and the Know Fraud database.
	Metropolitan Police	Amberhill is a team managing a database of known fake and fraudulently altered UK and foreign government issued documents. It is not networked or properly utilised.
	Other national policing portfolios	Identity is a significant enabler of many other crimes including sex offending, people trafficking and modern slavery.
Cross Government generally		Robust recruitment procedures and identity verification for working in the Civil Service.
<b>Voluntary Bodies and Third Sector</b>		
Open Identity Exchange		A community connecting those involved in the identity sector to help create trusted and universally accepted identities.
UK Identity Fraud Advisory		A social enterprise helping protect individuals from identity fraud and help businesses identify fake documents.

Cifas		Not-for-profit organisation working to reduce and prevent fraud and financial crime in the UK.
Get Safe On-line		A public/private sector partnership offering advice on protecting yourself from fraud and identity theft.
<b>Financial Services Sector</b>		
Emerging Payments Association		An association of payment professionals collaborating to reduce fraud.
Joint Money Laundering Steering Group		A group made up of UK trade associations in the financial sector which supports and advises re economic crime.
UK Finance		Represents 300 firms across banking and finance with expertise in economic crime.
Financial Conduct Authority		The conduct regulator for financial services firms.
The Investing and Saving Alliance		An alliance working to improve the financial wellbeing of UK consumers.
<b>Private Sector/Industry</b>		
The Association of Document Validation Professionals (ADVP) is a trade body representing the majority of firms involved in the electronic validation of UK and foreign government issued documents used for asserting an identity.	ADVP members support the checking of documents across many public sector areas such as the NHS and private sector areas, including _ <ul style="list-style-type: none"> <li>• Financial Sector (banking, pensions, insurance)</li> <li>• Employers in the UK</li> <li>• Aviation</li> <li>• Car Hire</li> <li>• Landlords</li> </ul>	Hundreds of thousands of checks per month in relation to – <ul style="list-style-type: none"> <li>• Fraud prevention</li> <li>• Legislative requirements such as AML, Right to Work, Right to Rent and Right to Study.</li> </ul>