ADVP feedback to the Home Office discovery project on Amberhill

Introduction

The Association of Document Validation Professionals (ADVP) is a trade body representing many of the providers of electronic identity document validation technology (IDVT) in the UK. An important objective for the ADVP is the sharing of appropriate fake identity intelligence with and between our industry, government and law enforcement for the prevention of crime and to improve the response to safeguarding.

The ADVP has previously attempted to deliver an industry wide data sharing arrangement with Amberhill, the Metropolitan Police team tasked with delivering data sharing on known and suspected false documents. A data sharing agreement was drawn up but could not in the end be delivered due to technological and process issues.

The ADVP has also conducted a trial intelligence sharing with National Document Fraud Unit (NDFU) and Immigration Enforcement. However this was stopped by the ADVP member involved when it became apparent that NDFU and IE were very happy to take the private sector intelligence but not willing to share anything from their side of the agreement.

The ADVP believes that an intelligence sharing solution in relation to document and identity fraud would significantly enhance the UK capability to detect, prevent and reduce fraud and other serious and organised crime, and would help the current government aim to deliver a fraud signal sharing capability within the emerging Digital Identity Trust Framework. The ADVP therefore strongly supports the work of the Home Office team tasked with undertaking a discovery project into Amberhill and its potential.

Some ADVP members have considerable experience of the issues related to a sharing arrangement with Amberhill. One member in particular has provided thousands of discovered fake documents for the Amberhill dataset and in return received the data to help with its work identifying fake documents presented for the purposes of asserting an identity. The ADVP Liaison Officer has previously worked within the Home Office and law enforcement and has considerable experience in policy and stategy related to the delivery of cross cutting solutions to tackle identity crime. There is considerable learning that the ADVP would like to share with the Home Office team, and we would welcome the opportunity to help and advise on any solution going forward.

Strategic Considerations

Below is a list of strategic issues that the ADVP believes are necessary to be addressed for the successful delivery of an outcome –

1. Ownership and Funding:

    Amberhill is currently funded by the Metropolitan Police (MPS) primarily to support MPS policing priorities. Previously Cabinet office provided significant funding to enhance the capability of the database to be shared. However, the MPS focus is on delivering a service for

the businesses and residents of London, and a lack of investment and central ownership has failed to deliver a standardised, on-line hosted national service. To be successful, a solution must deliver a national cross cutting approach with central funding.

2. Lack of awareness of Amberhill and its benefits: The current MPS data sharing arrangement is limited in that data is not widely accessible and knowledge of Amberhill among both the public and private sectors is very low. Amberhill has provided evidence of the opportunity to deliver significant benefit for preventing and detecting crime and improving public protection but has only delivered a fraction of the capability a national solution could offer.

3. Silo mentality: The current functionality of Amberhill means it is not currently available to as many partners as it could/should be. Likewise, other government departments such as NDFU do not and cannot share intelligence with Amberhill. Historically, government departments have only considered identity where it enters its core business e.g. crime, immigration, public protection, rather than the cross-cutting benefits of inter departmental and cross sector sharing. A central solution needs to have a government remit to overcome silo thinking and boundaries.

4. Imperative for sharing: Historically the willingness to share fake document data has been impeded by hiding behind data protection issues. A national solution needs to define what, how and why data should be shared, and if necessary, consider legislation to compel the sharing of confirmed fake identity data.

5. Industry willingness to share: A solution does not rest entirely with government and the public sector. The failure of Amberhill and ADVP to deliver a data sharing solution was in part due to companies within the private sector involved in identity validation setting up contracts with clients whereby the data remained in the ownership of the client and with no will or mechanism to enable fakes to be identified or shared with the public sector. Any solution should work with the private sector to overcome this obstacle. The ADVP would welcome the opportunity to work with the Home Office to define what reciprocatively sharing means and how it is achieved and policed.

Tactical and practical problems

The current process has many flaws that will need to be considered in any new solution design/ process if there is a decision to progress a national solution. These include:

1. The current dataset is not a live feed, and recipients of the data can only obtain up-to-date datasets by e-mail request, every few months, which means checks are not always against the most up to date counterfeit data.
2. Information on FOG (Fraudulently Obtained Genuine) documents is included within the Data Sharing Agreement (DSA); however, FOG document intelligence does not seem to appear in the shared data.
3. The database does not contain any information on imposters.
4. A large number of entries on the Amberhill database do not contain an image, therefore preventing a "visually similar" match.

5. The Amberhill Team no longer has document examiners to assist with requests; they perform a visual comparison of the document or the individual's face against their record but will not advise on whether a document is potentially counterfeit. Such a gap in capability may reduce confidence in the database going forwards.
6. The process of uploading datasets is through manual insertion. There is no automatic upload.
7. Only 'Primary Document Number' fields are cross-referenced; other data is not cross-referenced for more accurate potential matches / reduced false positives (such as Document Expiry Date).
8. Document Numbers that are input/auto-read to industry systems with non-alphanumeric values (such as hyphens or slash punctuation) will not match on the Amberhill database, (since non-alphanumerical values in document numbers are removed from the database).

Conclusion

The detrimental effect of document and identity fraud to UK society is pronounced. It is realistic to accept that the UK will need to continue to conduct a mix of digital and physical document checks for the foreseeable future. In fact, the importance of intelligence sharing is increasingly important as the UK economy transitions to a more digital ecosystem – a fact recognised by the specific inclusion of fraud signal sharing in the DIATF as a compulsory action for certified IDSPs. Therefore, given the significant and growing detrimental effects of document fraud to UK society, it is vital to enhance the capacity to detect and prevent document and identity fraud, of which intelligence sharing is a key component. The practitioners of document checking would benefit from sharing intelligence and the public sector would benefit from collaborating with the private sector in document checking and intelligence sharing.

The ADVP welcomes the current Home Office initiative and would welcome the opportunity to support and collaborate with the discovery project.