WORLD-CHECK™
REDUCING RISK THROUGH INTELLIGENCE

JULY 2009

Industry Voices

Passport Verification: Is the person in front of you who they claim to be?

Newsletter by World-Check, the recognised authority on reducing risk through intelligence.
www.world-check.com/industryvoices

Forged or 'fake' passports are used to commit a range of financial crimes, including identity theft, fraud, illegal immigration and organized crime such as the regional and international smuggling of contraband.

"Books", as some forgers refer to their trade, is big business, with fake identification documents increasingly being sold online. Although the exact scope of passport forgery in Australia remains unknown due to the high incidence of unreported and undetected cases, the problem is undoubtedly proliferating. As early as 2003, national media reported 14 000 Australian passports being "lost or stolen" in only five months.

According to the Australian Institute of Criminology (AIC), the cost of fraud to Australia is in excess of $5 billion per year, and accounted for 40% of Australia's crime in 2005. The estimated cost of identity fraud alone amounted to more $1.1 billion per year by 2006*.

Identity theft and ID forgery are essentially prerequisites for financial crime, making the fight against forgery a top national priority, both from a law enforcement and compliance perspective. Financial institutions and businesses accepting money deposits – banks, law firms, asset management house as well as online and land-based casinos – are targeted by criminals on a daily basis, making ID verification a critical first line of defence.

Within the context of new client sign-up or intake processes, the ability to instantly and effectively verify the authenticity of identity documentation in-house is key.

Caution: Not all illegal identification documents are altered or falsified
Fraudulently issued passports, for example are far harder to detect as they are not altered; just falsely issued. Successful verification techniques thus leverage a combination of security features, technologies and the MRZ's correlation to personal data.

Verifying a passport's authenticity by eye is a tough task, and compounded by the fact that new forgery techniques are continually developed to overcome counter-forgery measures employed during legitimate passport production. The secrets normally lie in characteristics such as watermarks, special security threads inserted during the paper production process, threads coated with ink that react to ultraviolet light, miniature plastic disks embedded in the paper, micro-line printing, background printing, holograms and similar reflective coatings.

Appraising passports using these features means staying abreast of production techniques for both real and fake passports in all jurisdictions concerned, and is therefore simply not practical. This challenge gave rise to the adoption of an international passport verification standard, utilising the so-called Machine Readable Passport Zones (MRZ) format.

Developed by the International Civil Aviation Authority (ICOA) and adopted by all member states, it is the globally recognised data display and authentication format for all machine-readable passports and identity documentation.

What's wrong with this picture?
The second MRZ line of Mokbel's fake passport contains inconsistencies with the passport's input data, revealing it as a forgery. The passport number and control digit are regular, yet the Date of Birth doesn't have a control digit, and the Expiry date is cited as the Date of Issue – again without a control digit.

The lack of control digits in the MRZ is a huge red flag; as is the fact that the Expiry Date is replaced by the Date of Issue.

Identity verification:
Protecting your business against reputational risk

Online traders and auctioning businesses, for example, are increasingly regulated in terms of know your customer (KYC) compliance. The ability to verify a seller's identity documentation independently enables vendors to offer their buyers increased transactional security. Used in conjunction with the Australian 100-point ID check list, MRZ-based ID and passport checking enables online vendors to offer their buyer base peace of mind whilst mitigating their business, legal and potential reputational risks.

Alleged underworld kingpin "Fat" Tony Mokbel aka Stephen Papas, for example, is not the sort of client institutions would want to be associated with. Wanted by the authorities in connection with a host of crimes ranging from narcotics trafficking and murder to forgery and possession of falsified identification documents, Mokbel fled Australia for Europe in 2006. He was travelling on a falsified passport. A reward of AU$1 million was offered for his recapture, and he was subsequently arrested in Greece in June 2007.

The MRZ on his falsified passport didn't correspond to its biometric data. (See above)

Identity falsification plays a pivotal role in most types of fraud. Effective passport and ID verification is therefore vital to avoid any association with known financial criminals and their associates. Using the MRZ checking technique to verify Mokbel's passport would have immediately raised suspicion, should he have attempted opening an account or conducting a deposit transaction. Using a two-in-one online screening solution such as Passport-Check would have highlighted Papas' criminal record and high-risk associations.

How to spot a fake passport using the MRZ

- Forgers often falsify personal data such as the Date of Birth, Date of Expiry, Passport Number or even the bearer's sex on the photo page.
- Experience shows most forgers do not adjust the figures of the Machine Readable Zone (MRZ) to reflect the new data.
- Checking the Machine Readable Zone with an optical reader will not consider the above and only confirms that the calculation of the check digits is correct.
- Alterations in the upper part of the document are not taken into consideration; therefore, checking with an optical reader provides a false sense of security.
- In case of doubt, always ask for a second opinion from a colleague or consult your security manager.

Fighting fraud through identity verification

In 2003, former principal of Cairns-based Parry & More Accountants, Elizabeth Heather Parry, was charged by Queensland Police with 27 counts of misappropriation, forgery and dishonestly obtaining property to the value of over $4.7million. She was sentenced to a 10-year jail term after being found guilty of fraud in August 2005. Reportedly linked to several other business entities, Parry may be eligible for parole after serving four years (i.e. in 2009).

Knowing who you're dealing with is critical; knowing who they're associated with even more so. Combining instant document verification and risk screening processes therefore makes sense from a commercial risk management perspective.

Passport Verification: Some best practice recommendations

- Never accept expired documentation – it's not valid and therefore illegal.
- Never accept a damaged, defaced or altered document.
- Only accept clear passport photos – follow your domestic regulatory guidelines, or refer to the Useful Links below.
- MRZ are generated based on user-submitted data – be sure to type all data in correctly to prevent delays, false alarms, and time and resource expenditure.
- Always try to get a clear colour copy – faxed copies not recommended, even if they are certified by the police or a commissioner of oaths.
- Beware of electronic passport amendments – always scrutinize the MRZ font for deviations from the standard fonts.

New passport verification technologies

and the future One of the MRZ's key strengths lies in the fact that it provides a global standard for how passport data is visually presented. Although technological and biometrical measures are increasingly employed to help fight passport and ID forgery, the MRZ will continue to serve as a standard visual format and first line of defence against identity fraud and associated crimes. The following are examples of new and complementary ID verification technologies:

- The Australian Department of Foreign Affairs and Trade started introducing a new biometrics-based 'ePassport' in late 2005, with the $62 million "SmartGate' passport checking systems being rolled out at Australian airports during 2007 and 2008.
- In European countries such as Germany and the UK, Radio Frequency Identifier (RFID) technologies are also currently being implemented. Biometric data is embedded in a radio chip, adding an additional layer of security, and enabling one-swipe verification.
- Similarly, the United Arab Emirates (UAE) are implementing iris scanning capabilities at airports to match passport data against biometrics.

Visit the below links to find out more about new document formats, best practice and advanced passport verification techniques:

Australian Passport Photograph Guidelines
http://www.passports.gov.au/Web/Requirements/Photos.aspx

Passport-Check
http://www.world-check.com/passport-check/

Instant web-based ID and passport verification service for all types of machine-readable (MRZ) identity documents. Combines document verification and risk screening against World-Check's risk intelligence in one step.

Australian ePassport Information
http://www.passports.gov.au/Web/ePassport.aspx

The Council of the EU Glossary of Security Documents
http://www.consilium.europa.eu/prado/EN/glossaryPopup.html

This article first appeared in AFMA's Anti-Money Laundering Magazine, March 2009 Edition

About Industry Voices

Industry Voices is a collection of articles and papers that address common issues and challenges faced by the compliance community. World-Check has embarked on this project with the aim of facilitating debate among committed professionals from the financial, legal, regulatory and enforcement sectors. To produce such a library of knowledge, World-Check has invited industry experts, scholars, consultants and professionals to contribute to this series.

The articles can be viewed on **www.world-check.com/industryvoices**