Camouflage passports still unknown to many compliance staff

A question at a recent World-Check lecture revealed that many compliance staff are still not aware of the existence and use of camouflage passports, and are therefore apt to allow them as proof of identity of a new bank customer. Identifying camouflage passports requires a working knowledge of both geography and world history.

A camouflage passport, also sometimes known as a decoy passport, is an authentic-appearing document from a country that does not currently exist, by reason of independence, change of name, federation, governmental designation, or some other reason. It is not a ‘fantasy’ passport from a nation that never was, but a name from the past.

The reasons that a person might purchase such a bogus document, which is not counterfeit, but in the name of a bygone state, are:

- Insurance in the event that a foreign invasion or a regime change occurs, and one must safely exit one’s country under another nationality.
- Involvement as a victim in an airline or maritime hijacking, where having a passport from certain countries may cause one to be held hostage, kidnapped, or worse.
- Being caught up in a terrorist event, where a ‘safe’ third-world identity may save your life.
- Opening a bank account in a faraway country under an alias, to support or advance criminal conduct. Of course, this is itself a crime.

They are not illegal, as they do not actually purport to represent a nationality document of an existing country. As a matter of fact, though such jurisdictions such as the Isle of Man warn their financial services industry to beware of their existence, the possession of one is not a crime in the UK or US.

I was lucky enough to have been a history major as an undergraduate, but if a bank officer does not have the benefit of a traditional liberal arts education, one which includes geography and world history, he or she may not know the details of independence of colonial states, or of changes of names after political upheaval, and other esoteric facts of political geography which would lead to the swift identification of a camouflage passport.

In fact, a US District Court judge in the District of Columbia last year pointed out in a written opinion that camouflage passports are used as false identification in other countries where bank employees are generally not trained to spot them.

Since we cannot turn back the hands of time on educational backgrounds of your staff, they should at a minimum memorise the most common ‘countries’ employed by camouflage passport creators:

- Zanzibar
- British Guiana
- British Honduras
- British West Indies
- Burma
Perhaps a short training course for your staff, with a world map illustrating exactly why these names are no longer legal states would serve to reduce the risk that a junior compliance staffer will, in the future, pass a camouflage passport as a real identification document.

Mr. Rijock, Financial Crime Consultant to World-Check in association with COMSURE
20 October 2006
Do financial criminals operate some hedge funds?

Recent disclosures of what can only be described as economic crime originating inside major hedge funds begs the question; are financial criminals operating hedge funds?

The potential for conducting financial crime from inside hedge funds is disturbing, and compliance officers at financial institutions that bank hedge funds should be aware of these possible scenarios. Should hedge funds be considered high-risk? We cannot say, but the opportunities for a number of different financial crimes exist in the typical hedge fund:

- Money launderers operating for wealthy criminal organisations could ‘invest’ their clients’ dirty offshore profits, disguised as innocent investor funds held in some anonymous corporate form, turn a handsome profit through the use of these monies in the hedge fund, and reap large management fees and profit percentages. The result would be legitimate, onshore profits, upon which taxes would be gladly paid, derived solely from the proceeds of crime.

- Hedge funds purchase the bulk of the debt of distressed companies at extremely low prices. Should any of these companies seek the protection of bankruptcy court, the hedge fund uses its creditor status to sit on creditors’ committees, and obtain favourable payouts that come at the expense of other creditors whose debt was not discounted. There may even be fraud and collusion involved in the purchase of the debt in the first place.

- Personal information, including financial data to qualify them as sufficiently affluent, sophisticated and exempt submitted to hedge funds by wealthy investors could be sold to criminal organisations for the purposes of identity theft on a grand scale.

- Hedge funds who lend money to publicly traded corporations require detailed, non-public financial data to make those loans. There have been allegations that there has been improper ‘Insider Trading’ on that financial information, for the profit of the hedge funds, and at the expense of the investing public, who is not privy to this intelligence. Anyone in possession of inside information must either disclose it, or refrain from trading; Rule 10b-5; SEC vs. Texas Gulf Sulphur Co., 401 F.2d 833 (2nd Cir.1968).

Mr. Rijock, Financial Crime Consultant to World-Check in association with COMSURE
17 October 2006
Are money launderers using hedge funds to gain access to illicit offshore cash?

A Congressional committee report that worried aloud whether money launderers were using hedge funds to move illicit cash into the United States, and making legitimate profits onshore raises some interesting questions. Is this a widespread tactic?

The technique can be summarised as follows:

- A criminal organisation has its illicit profits deposited offshore, in tax haven banks.
- The organisation’s money laundering team creates a hedge fund, which it manages for a set fee that is a percentage of the amount managed, plus a large percentage of profits earned, within industry norms.
- Large amounts of the offshore funds are transferred to anonymous offshore corporate entities or trusts, and the money then invested in the hedge fund, which is controlled by the organisation’s laundrymen.
- The laundering team, who are the designated hedge fund managers, take large fee, as well as a share of the profits they achieve through legitimate investments onshore.
- The criminal organisation has virtual access to its illicit cash, through the investment team, but any investigation would be unable to link beneficial ownership of the offshore investment capital to them.

The issue appeared in the August, 2006 report of the US Senate Permanent Subcommittee on Investigations and Homeland Security entitled 'Tax Haven Abuses: the enablers, the tools and the secrecy.' Although the factual context did not address the proceeds of crime, one wonders how much hedge fund capital coming from offshore sources is actually illicit, untaxed profits sneaking back into the US financial system through this subterfuge.

More directly, are there hedge funds controlled by money launderers working for organised criminal groups for the sole purpose of deriving large legitimate onshore profits through the investment of dirty money?

After all, hedge funds currently fit into a gap in our regulatory scheme, a fact which surely has not escaped the attention of the money laundering profession. Now, if one was able to actually work with one’s dirty money, and realise a legal profit, paying taxes upon it to legitimise the ‘management fees,’ it seems like every organised crime group would flock to the scheme. Are they?

Mr. Rijock, Financial Crime Consultant to World-Check
in association with COMSURE
9 October 2006
16 BVI companies indicted for conducting illegal money remittance business operations in NYC

The District Attorney for New York has filed an indictment against sixteen British Virgin Islands-registered companies for conducting illegal money remittance activities into New York City. In a civil action, $17.4m that was allegedly illegally transmitted from Brazil to New York was frozen. Prosecutors in New York continue their campaign against the firms who have moved an estimated $19bn from Brazil into Manhattan recent years. The BVI companies, all of whom are listed as being incorporated in Road Town, Tortola, are:

- Avion Resources Ltd. (UID 502675).
- Bahia Blanca Ltd. (UID 502676).
- Best Consulting, Ltd. (UID 502677).
- Beverly Hills Group, Inc. (UID 502678).
- Braza Corporation (UID 502679).
- Chettiar Business, Inc. (UID 502680).
- Farswiss Asset Management Ltd. (UID 502681).
- Gatex Corporation (UID 70556).
- Harber Corporation (UID 70557).
- Harborside Corporation (UID 502684).
- Mabon Corporation (UID 502685).
- Midland Financial Inc. (UID 502686).
- Phoenix Export Import SA (UID 502687).
- Safe Port Investments Corporation (UID 502688).
- Silver Commodities Ltd. (UID 502689).
- Tigrus Corporation (UID 502690).

Complete profiles of these companies are, of course, available on World-Check, including companies and individuals linked to those listed. Compliance officers should check these company names against customer lists as soon as possible; any positive results require a further enquiry for any linked companies or individuals shown one on the World-Check Profiles.

Mr. Rijock, Financial Crime Consultant to World-Check in association with COMSURE
2 October 2006
PEP guidelines are flawed

Recent guidelines on when one should employ specialised PEP databases employ faulty logic that could result in the failure to identify PEPs, or even terrorist financiers. Today we examine the difference between subjective and objective PEP due diligence, and why it is inappropriate to link risk to perception.

Let us begin by summarising paragraph 4.32 of the Treasury consultation document:

- Companies that have a high risk of exposure to Politically Exposed Persons, PEPs, such as multinationals and private banks, must employ systems ‘appropriate’ to the ‘perceived risk.’ This would generally translate to a permanent subscription to a specialised, commercially-available PEP database.
- All others, understood by the author to be ‘a majority’ of firms and businesses, must utilise ‘common sense and judgment,’ and if high risk is perceived, further research is called for, such as internet searches, or a review of papers, reports or simple databases.

Why is the aforesaid logic fatally flawed? If we must make a value judgment as to the extent of perceived risk, compliance decisions become subjective, rather than objective, as they must indeed be in the deadly serious world of PEP and terrorist financier identification. If one must only employ adequate PEP identification systems when one perceives risk, then what if the MLRO or compliance officer making that call has inadequate information, or even disinformation, and erroneously believes a client to be a low risk non-PEP and non-terrorist?

The guidelines do not impose a duty to do anything if you do not perceive risk. This is a recipe for disaster.

Here are the dangers of relying upon these guidelines:

- If your business does not clearly fall within the specified class of high risk entities, the only due diligence the guidelines offer is the internet, research papers, reports and government lists. This is grossly inadequate. Many PEPs and terrorist financiers do not show up as such on the internet. The government lists often do not post emerging threats until they have been involved in criminal activity for an extended period of time, and come to the attention of law enforcement.
- Also, the internet contains many instances of information laundering. These are articles favourable to the subject, and paid for covertly by interested parties. They often contain misinformation, and could easily be taken for independent, authoritative material. The reader is thus misled as to critical facts. He may believe a customer is a private businessman when that is far from the truth
- Money service businesses involved in funds transfers and foreign exchange firms, having no perceived risk in ‘routine transactions have been involved with illicit PEP funds and terrorist funding. The guidelines do not allow for these types of situations.
- The guidelines do not allow for the wide variations in training and experience amongst compliance officers. What is senior staff is away on that particular moment, leaving only a low-level trainee to judge whether a transaction, in his perception, is a risk?
There must be an objective standard regarding PEPs and terrorist financing, and that is to check all new, potential and proposed customers, using the best specialised database available to MLROs and compliance officers at financial institutions and non-bank financial institutions (NBFIs).

In my humble opinion, that is World-Check, because it is viewed by 45 of the world’s 50 largest banks as ‘best practice.’ To do anything less constitutes what can only be described as compliance malpractice. Compliance officers simply cannot open their doors of perception and effectively and consistently identify PEPs and terrorist financiers without the use of a specialised database.

Mr. Rijock, Financial Crime Consultant to World-Check in association with COMSURE
11 September 2006