Big brother banking to watch us

By: Ana Monteiro

Posted: 2004/09/20 Mon 18:08

This is an extremely long shot, but imagine if Osama bin Laden manages to open a savings account at, say, the Klerksdorp Absa – highly implausible, we know. However, it could happen that one of his associates succeeds, placing the bank in a precarious legal position.

The provision of financial services to politically exposed persons, known as PEPs, was the topic of a seminar hosted on Moday by the RAU Centre for the Study of Economic Crime (CenSEC), the Compliance Institute of South Africa and the Money Laundering Forum.

PEPs are not only politicians, senior civil servants or high-ranking individuals in organisations: the category also includes the friends, families and business associates of those people who work for political parties, state-owned enterprises, government or high up in the business landscape – anyone who is privy to these people's lives and business interests.

A more realistic scenario in the South African context than the opening example: a senior official in a state-owned enterprise might receive a sum of money from someone who is tendering for a big project, in an attempt to swing the decision that person's way. What would the bank do then?

Providing financial services to PEPs is naturally risky business for all banks: which institution would like to be known for having kept accounts for shady business people or corrupt politicians?

Speaking at the seminar was David Leppan, the CEO of World Check – a company that provides structured intelligence to the financial industry, and has built up the largest structured database of publicly available intelligence on heightened risk financial customers, including money launderers, fraudsters, terrorists and PEPs. Leppan, who hails from South Africa, said that since the crackdown on terrorist financing subsequent to the 9/11 attacks in the United States, the issue has become even more pertinent: "South African banks are under pressure to identify PEPs, even though there isn't any legislation in place obliging them to do so. It has become imperative, though – from a reputational risk point of view – that banks know exactly who their customers are and the types of transactions that are going through their accounts."

Although there is no legislation covering this in South Africa, the Money Laundering Advisory Council (MLAC), formed in October 2002 to recommend amendments to the Financial Services

Intelligence Act (FICA), is giving guidance on terrorist financing and PEPs. The review is due for release soon.

Despite this, however, Professor Louis de Koker of CenSEC and the MLAC said that South African banks could still be held liable in a court of law: “South Africa joined the Paris-based Financial Action Task Force (FATF) - the world body leading the fight against money laundering - in June 2003. At the same time, we implemented the 40 recommendations made by the FATF, when the FICA came into force.”

These are important words, because recommendation 6 made by the FATF says that: “Financial institutions should, in relation to politically exposed persons, and in addition to performing normal due diligence measures:

- Have appropriate risk management systems to determine whether the customer is a PEP
- Obtain senior management approval before establishing business relationship with such customers
- Take reasonable measures to establish the source of wealth and source of funds
- Conduct ongoing monitoring of the business relationship.”

Clearly, checking for and monitoring PEPs is an expensive and difficult process to implement and maintain. It involves going back in time and checking all customers and their accounts, compiling databases of PEPs and then monitoring these accounts on an ongoing basis. Also, both foreign and local PEPs need to be identified, as South Africa may be perceived as a safe haven, away from the eyes of American and European law enforcers.

Options available to banks include:

- Filtering – checking payments made into accounts, especially the origin of the payments.
- Obtaining software and access to a database of PEPs and their associates, and then checking people while they try and open an account – this is expensive and will require huge investments in infrastructure (banks would, for example, need to pay for extra bandwidth).
- Making sure that the correspondent banks with which they are doing business do not pose any risk i.e. also have checks in place to ensure that no illicit transactions are being facilitated by their banks.