RISK PROFILING OF MONEY LAUNDERING AND TERRORISM FUNDING

Practical Problems of Current Information Strategies

B. H. M. Custers
Tilburg Institute for Law, Technology and Society, Tilburg University
Warandelaan 2, PO Box 90153, 5000 LE Tilburg, Netherlands
Capgemini Consulting Services, Capgemini Netherlands BV
Papendorpseweg 100, PO Box 2575, 3500 GN Utrecht, Netherlands

Keywords: Risk profiling, identification, money laundering, terrorism, terrorism funding, information strategy, KYC, Patriot Act.

Abstract: In order to track money laundering and terrorist funding, banks have to create risk profiles of their clients. Banks that want to do business in the United States have to implement a worldwide Know Your Customer (KYC) program, partially based on the Patriot Act. Implementing a KYC policy, however, raises several problems and seems to be neither effective nor efficient in tracking money laundering and terrorist funding. Given problems regarding the identification of individuals, it is not too difficult for criminals and terrorists to avoid being detected by certain types of screening. In this contribution, the way risk profiling strategies are implemented in practice are discussed, including the problems this may raise.

1 INTRODUCTION

Since the attacks of September 11, 2001, the war on international terrorism is being waged in many fields. Suspects of terrorism are being tracked and prosecuted, there is an active battle against Al Qaeda in Afghanistan, and, security of high-profile objects and persons has increased. Although it may be less well-known, tracking terrorist funds is playing an increasingly important role in the war on terror. Owing to new legislation (particularly in the United States), financial institutions, particularly banks, are legally required to know whom they are doing business with. Of each client, a risk profile has to be made and, in cases of high or unacceptable risks, action can be taken, for instance, by removing clients from the lists of business partners or by informing the supervisory authorities. This process is known as Know Your Customer (KYC). In this contribution, it will be argued that this process is not very effective when it comes to tracking money laundering and terrorism funding and that it is relatively easy for both potential and actual terrorists to avoid being detected during these types of screening. For related work and references, see (Custers, 2006). This contribution is focused on risk profiling customers, rather than monitoring unusual transactions.

2 LEGISLATION

Long before the attacks of September 11, 2001, Anti Money Laundering (AML) was an important subject on the agenda of the US government. AML programs received more attention after the terrorist attacks because they may help to detect and prevent financing terrorism.

A Know Your Customer policy is focused on implementing a client identification program. This is mandatory under the US Bank Secrecy Act (BSA, 1970), (Comptrollers Handbook, 2000) and the Patriot Act (Patriot Act, 2006). The main goal of a KYC policy is to address identity fraud, terrorism funding, and money laundering.

The BSA dates from 1970 and obliges financial institutions to cooperate with government institutions to track cases of money laundering. In practice, this often means detecting large or unusual transactions and suspect activities that may indicate money laundering, tax evasion, or criminal activities.

H. M. Custers B. (2007).
RISK PROFILING OF MONEY LAUNDERING AND TERRORISM FUNDING - Practical Problems of Current Information Strategies.
In *Proceedings of the Ninth International Conference on Enterprise Information Systems - ISAS*, pages 90-94
DOI: 10.5220/0002347700900094

The Patriot Act dates from October 2001, just after the attacks on the World Trade Centre and the Pentagon. Pursuant to this Act, criminal investigation departments have considerably more powers. In addition, the Patriot Act introduced amendments in legislation regarding immigration, passport controls, and anti money laundering. In March 2006, the Patriot Act was reinforced by the US Congress.

Although US legislation is obviously not applicable worldwide, financial institutions in the US are obliged to implement KYC policies worldwide. Since many international banks have major businesses in the United States they cannot afford to lose, KYC obligations are indirectly imposed on other countries as well. Revoking a banking licence may be the ultimate sanction of a supervisory authority, but fines are also possible. This is a real risk, as a large Dutch bank experienced in 2005, when it was fined millions of dollars for illegal transactions with Iran and Libya (Simpson, 2005).

3 IMPLEMENTATION

In practice, for a financial institution, implementing a KYC policy means that a system must be installed that builds risk analyses of all existing and new clients. In order to determine the scope of a KYC project, it is necessary to know how many clients there are. Since multinationals may have many clients (hundreds of thousands or millions of clients), this may cause difficulties. Once a client has been identified, the risk analysis can be started. Usually, a risk analysis consists of mapping a number of characteristics of a client, collecting the evidence for these characteristics, and, finally, attaching a risk index to the characteristics by weighing them (Custers, 2004).

Relevant client characteristics in the case of natural persons are name, address, date of birth, solvency, number and types of accounts, data on fraud or criminal activities in the past, etcetera. Evidence regarding identity usually consists of photocopies of passports. Evidence for other characteristics may be government documentation, such as certificates of good conduct.

Characteristics of legal persons may consist of name, address, date of incorporation, business activities, names of directors, names of shareholders, names of owners. Furthermore, it may be investigated whether a particular legal person is registered at or supervised by a stock exchange, a local chamber of commerce, a financial authority, a local government, or any other supervisory authority.

Proving the identity of a legal person may be done, depending on the country, with a certificate of incorporation or a registration certificate of the chamber of commerce. Other characteristics may be proven with the use of documentation of chambers of commerce and supervisory authorities, annual reports with audit reports, certificates of incorporation, photocopies of passports of directors, shareholders and owners, etcetera.

Determining the risk is a final weighing of all the characteristics of a particular client. Several characteristics may indicate increased risks:

- *The location of the client:* countries such as Iraq, Somalia, or Libya are considered high risk because there is little or no supervision on natural or legal persons. The same, but to a lesser extent, applies to countries like Russia and India. Furthermore, the US government prohibits trade with particular countries. Examples are Cuba and Iran (US Sanctions list, 2006).
- *Business activities:* particular business activities are sensitive to money laundering and terrorism funding. Examples are casinos, exchange offices, and diamond trading offices.
- *Legal company structure:* so-called shell companies are administrative constructions where no real business activities are performed. Due to favourable tax climates, these constructions are often not very transparent when determining who the directors or the owners are. Many shell companies are found in tax havens such as the Cayman Islands, the British Virgin Islands, or Bermuda. Other legal constructions may also lack transparency. Examples, depending on the legal regime of a particular country, may be foundations and structures with silent partners.
- *Occurrence on black lists:* when directors, shareholders or owners appear on black lists, this may indicate increased risks. In the case of legal persons, there are also black lists with company names. It is important to distinguish lists with increased risk and lists that prohibit transactions with particular clients. Sometimes lists with increased risk are indicated as ‘grey lists’ to distinguish them from the ‘real’ black lists, that contain prohibitions.

The latter issue, black lists, may need further elaboration. Both in the United States and in the European Union, various black lists exist. An example is the OFAC list (OFAC List, 2006) of the

Office of Foreign Assets Control (OFAC) of the US Department of the Treasury. There are more than 5000 persons on the OFAC list who the US government has marked as terrorists and/or heavy criminals. Doing any business with persons on this list is prohibited. Examples of other lists that are being used to check persons are the FBI ('most wanted') list, the EU list of terrorist organizations, the Australian DFAT list, the Bank of England list, and Europol lists. Apart from lists of suspects of terrorism and criminality, it is also possible to check against, for example, other lists, such as solvency lists.

Apart from characteristics that increase a risk, there are also characteristics that decrease it. This is often the case when independent authorities are supervising a client. For legal persons, a listing on a stock exchange may only be possible when higher demands regarding the transparency and a solid financial situation are met. In several countries registration at the chamber of commerce is mandatory and subject to critical investigation. Clients operating in financial markets, such as banks and insurance companies, are usually subjected to critical supervision. Clients that are part of or related to (semi-)government organizations are also supervised in many cases. Obviously, these characteristics only decrease the risk in countries where the government and supervisory authorities are considered reliable.

Based on a weighing of all characteristics that are discovered in the process, a risk assessment is made. In cases of increased risks, this may involve periodical scrutiny. In cases of unacceptable risks, it may be decided to end relationships with such a client. A risk profile clearly has a limited durability and will have to be updated periodically (Custers, 2003). Both the data in the profile and the weighing and risk assessment may then need to be updated.

4 PRACTICAL PROBLEMS

In practice, implementing the legal KYC requirements into a process as described above may lead to several problems.

4.1 Unclear Scope

Large multinationals do not always know how many customers they have. This is often due to their growth by mergers and acquisition. Sometimes it is difficult or impossible to link or integrate client databases of merged or acquired companies. There may be dozens of databases that contain hundreds of thousands or millions of clients. As a result, there may be a fragmented registration of clients and a great deal of overlap in the data. For instance, a person or company may be a client at several banks that were merged. As a result of this overlap, it may be hard to determine how many unique clients are hidden in the various information systems. When it is unknown how many and what customers are to be analyzed, the scope of the project is unclear.

4.2 Identification Issues

Identifying persons or companies may be difficult. How do you know whom you are dealing with? When a particular database contains Mr. William White and another database contains Mr. Bill White, they may be the same person. When the address is the same in both records, it is likely that it is the same person using a shortened version of his name. The probability that it is in fact one and the same person increases when more characteristics are identical, such as date of birth, phone number, and social security number. Currently, there are technological solutions that may establish, based on overlap, whether the same person is concerned. An example is IBM's Entity Analytics Solutions (Baker et al., 2003).

When dealing with companies, this may be even more difficult, since legal structures of large companies often contain many different legal persons. For instance, Jones PLC, Jones International, and Jones International Holding PLC may all be different companies and different legal persons. However, it is also possible that these names refer to same company, with the same directors. A company may use different names for branding and marketing purposes. It may be that the official name registered at the chamber of commerce is much longer than the name used for advertising. Names of divisions may also differ from the conglomerate name.

4.3 Persons behind Organisations

Obviously identifying companies is not a goal in itself. The ultimate aim is to identify the persons behind organizations, such as directors and shareholders. Sometimes the shareholders of companies are other companies. Searching for a parent company may lead to natural persons who are directors and shareholders. Any relation to terrorism or money laundering of all persons involved in a company should be investigated.

However, it may be difficult to find the persons behind organizations. Many international companies have parent companies in countries other than the country where a subsidiary is located. As a result, the search may depend on other sources (such as local supervisory authorities and chambers of commerce). These other sources may be in different

languages and subject to other rules. Many companies are located in countries with strict banking secrecy for tax purposes (e.g., Luxemburg, Switzerland) or in countries with a tax regime that is not very transparent (e.g., Cayman Islands, British Virgin Islands, Channel Islands). Other company structures, such as foundations or partnerships with silent partners may also lack transparency; this may vary from country to country.

All names that are found must be checked against the black lists that are used by secret services and surveillance authorities such as the CIA, FBI, Interpol, and Europol. More general checks, such as bad press, may provide more background information. Note that all these checks against black lists may only result in 'hits' on persons who were related to terrorist incidents in the past. First time terrorists intending to prepare, finance, or commit an attack are usually not on black lists.

4.4 Standardisation

KYC legislation states that all clients must be profiled. For large international financial institutions, this may involve hundreds of thousands of clients. Because of the amounts of time and money involved, there is a tendency towards standardisation. Procedures are required to streamline the processing of large amounts of data. However, standardization and procedures usually focus on the average funds, whereas a search for terrorist financing should focus on the exceptions. Using a standardized and predictable approach may have as a result that the suspects are overlooked. Furthermore, there is the risk that the persons who do not want to be traced have plenty of time to change their strategies in order to avoid being burdened with increased risk profiles.

4.5 Documents Rather than Persons

Although a KYC policy aims at identifying suspect clients, the current profiling strategies are performed on the basis of documents. The main reason for this is usually not to bother clients with requests for information. This is, however, an indirect type of checking, because the integrity of the document is checked, rather than the integrity of the person. This means that two things can go wrong: the document or the link between the document and the person may have been tampered with.

The first problem, tampering with documents, occurs regularly in international criminality and terrorism. People may use different passports and aliases. For this reason, documents are nowadays equipped with features that are hard to counterfeit, such as graphics, watermarks, holograms, and seals. Distinguishing real from forged documents requires frequent training of inspectors.

The second problem, tampering with the link between person and document, occurs more and more frequently. For this reason, passports of many countries are nowadays equipped with biometric data (Anderson, 2001, Schneier, 2000). Obviously this is not possible for documents identifying legal persons. By integrating body characteristics of a person in the identity document, the link between person and document can be strengthened. This makes it more difficult for people to hide behind documents. Note that these do not have to be fake documents. A person may simply use a real document belonging to another person, a setup known as look-alike fraud. The link between person and passport may be hard to verify. Inspectors often focus on the picture in the document, but the passport photo may be old. A beard may have been shaven or glasses may have been replaced with lenses.

5 CONCLUDING REMARKS

Collecting many data on clients and funds does not automatically mean that terrorism funding is revealed. Usually, fewer than one out of every thousand customers is suspected of terrorism funding, fraud, or money laundering. The general approach that KYC legislation prescribes, in which all clients and funds are screened, results in a great deal of work, but relatively few hits. Instead of investing much time, effort, and money in profiling everyone, it is recommended to target the search by using suspect patterns and characteristics. Only by clever searching will detecting terrorism funding become more efficient.

A targeted search will also be more effective. The current generic approach makes it easy for criminals and terrorists to avoid discovery. A few people will be tracked, but others will try to hide characteristics that may cause increased risk. Tracking money laundering or terrorism funding is a cat-and-mouse game in which the players are trying to outwit each other. In order to win this game, an ad hoc approach is most suitable, as it provides a creative and flexible approach rather than a generic and predictable approach.

What should be done? The best option seems to be to start with creating search profiles based on characteristics that cause suspicion or increased risk. For instance, risk increasing characteristics may be found when looking at previous cases in which terrorist funds were discovered. Using these search profiles, it may be investigated which clients are

indeed suspects. These suspects can than be subjected to more detailed investigation. Rather than profiling all customers, this approach focuses on a small percentage of customers that is relevant. Early 2007, the Dutch government started a pilot using this approach regarding their surveillance on legal persons (Dutch Ministry of Justice, 2006).

Obviously it is very important to use very sophisticated profiles to prevent particular terrorist funds from being out of scope. Furthermore, the risk profiles should be handled with care, because they may be very stigmatising for particular groups in society (Harvey, 1990).

Note that this targeted approach requires changes in the current KYC legislation. Most KYC requirements stem from US legislation, but it is important to note that several European countries have already implemented similar legislation that makes it mandatory for financial institutions to identify and profile their clients. Since most of this legislation is less than a year old, it is neither likely nor desirable to implement changes immediately. However, careful evaluation of the current legal framework and best practices may be useful to reveal further lessons to be learned.

Obviously, the current approach raises many issues related to privacy and data protection. Collecting and processing data of all clients involves the use of personal data of innocent people, often without informing data subjects and without their consent. Using a targeted approach, much less personal data is required, i.e., only personal data of the people involved initially showing increased risk. This may result in fewer violations of (European) data protection laws (Bygrave, 2002).

Whatever method is used, tracking money laundering and terrorism funding is ultimately based on human intuition for a significant part. There are all kinds of technological possibilities to gain insight into large amounts of data stored in databases, for instance, searching for patterns and relations in databases, often referred to as KDD, 'Knowledge Discovery in Databases' (Piatetsky-Shapiro and Frawley, 1993). Creating risk profiles may also be automated to some extent. However, it remains difficult to get a good understanding of who an individual is and what his intentions are if only data in databases is used. Since data can be manipulated too easily, tracing money laundering and terrorism funding has to rely on clever searching combined with some intuition and experience.

REFERENCES

Anderson, R.J., 2001, *Security Engineering; a guide to building dependable distributed systems*. New York: John Wiley & Sons, Inc.

Baker, S., Kuilwijk, K., Chang, W., and Mah, D., 2003, *Anonymization, Data-Matching and Privacy: A Case Study*. Washington DC: Steptoe & Johnson LLP, Attorneys at Law.

BSA, 1970, US Banking Secrecy Act, 1970, <http://www.federalreserve.gov/boarddocs/supmanual/bsa/7-00bsaman.pdf>

Bygrave, L.A., 2002, *Data protection law; approaching its rationale, logic and limits*, Information Law Series 10, The Hague, London, New York: Kluwer Law International.

Comptrollers Handbook, 2000*, Bank Secrecy Act/Anti-Money Laundering*, Comptroller of the Currency, Administrator of National Banks, US Department of the Treasury.
<http://www.occ.treas.gov/handbook/bsa.pdf>

Custers, B.H.M., 2003, *Effects of Unreliable Group Profiling by Means of Data Mining*. In: G. Grieser, Y. Tanaka and A. Yamamoto (eds.) *Lecture Notes in Artificial Intelligence, Proceedings of the 6th International Conference on Discovery Science (DS 2003)* Sapporo, Japan. Berlin, Heidelberg, New York: Springer-Verlag, Vol. 2843, p. 290-295.

Custers, B.H.M., 2004, *The Power of Knowledge; Ethical, Legal and Technological Aspects of Data Mining and Group Profiling in Epidemiology*, Tilburg: Wolf Legal Publishers.

Custers, B.H.M., Risicoprofilering en identificatie van terreurfondsen, *Banking Review*, October 2006, p. 28-33.

Dutch Ministry of Justice, 2006, *Snel en Secuur Toetsen; het alternatief voor de verklaring van geen bezwaar*. Bijlage bij het eindrapport interdepartementale werkgroep Toezicht Rechtspersonen, Niet-dossierstuk just050263.

Harvey, J., 1990, Stereotypes and Group-claims; epistemological and moral issues, and their implications for multi-culturalism in education, *Journal of Philosophy of Education*, Vol. 24, No. 1, p. 39-50.

OFAC List, 2006 <http://www.ustreas.gov/offices/enforcement/ofac/sdn/t11sdn.pdf>

Patriot Act, 2006 <http://www.epic.org/privacy/terrorism/hr3162.html>

Piatetsky-Shapiro, G., and Frawley. W.J., 1993, *Knowledge Discovery in Databases*, Menlo Park, California: AAAI Press/The MIT Press.

Simpson, G.R., How Top Dutch Bank Plunged into World of Shadowy Money, *Wall Street Journal*, 30th December 2005, p. A1.

Schneier, B., 2000, *Secrets and Lies; digital security in a networked world*, New York: Wiley Computer Publishing.

US Sanctions list, 2006 <http://www.ustreas.gov/offices/enforcement/ofac/programs/>