Journal of Forensic Anthropology

Simonovsk and Nikoloska, J Forensic Anthropol 2016, 1:1

Research Article Open Access

Profiling of High Risk Profiles of Clients in Order to Prevent Money Laundering and Terrorism

Ivica Simonovski[1]* and Svetlana Nikoloska[2]

[1]*Corporate Security and Crisis Management Initiative, Skopje, Macedonia*

[2]*Faculty of Security, MIT University, Skopje, Macedonia*

Abstract

One of the goals of the strategy to prevent money laundering and financing of terrorism is to keep the policy through preventive measures and activities by all stakeholders. These include financial institutions, especially banks which are most frequently used institutions by perpetrators for laundering the proceeds of crime or to support terrorist activity.

Leading the preventive policy covers several activities. This paper will analyze the creation of high-risk profiles of clients based on risk factor categories and financial reconstruction or analysis of financial transactions of the past. Based on the data obtained from the analysis should create profile (typology) of the individual who should be an indicator to show:

- Wheter the bank to establish business relationship with the potentional client in order to protect their reputation;
- Profiling of high-risk profiles that have already established business relationship with the bank and in accordance with the objectives of the strategy and aimed at minimizing risk, it is necessary to carry out their detection, determination of risk (rating), paying attention and monitoring.

Banks looking to bank customers in traditionally higher risk customer segments need to first understand that the main purpose is not to detect and report every illegal transaction that is related to the customer. The goal is to have a risk-assessment framework that is “proportionate with the risks” and is in line with the strategy and risk tolerance of the board.

Customers should be categorized into risk-assessed groups titled risk classes. Risk classes may be simple in development, such as low, medium, and high, or they can be more elaborate, such as low, medium, medium-high, high, and very high.

Keywords: Money laundering; Terrorism financing; Indicators; High risk clients; Risk factors

Term of Money Laundering – General Overview

"Money laundering is not only a process that is associated with the functioning of criminal organizations, but it is an indicator of their success. Moreover, money laundering, providing a steady stream of capital that allows criminal organizations to buy protection through the corruption of government officials and members of law enforcement. How it makes money laundering attractive target for law enforcement agencies, even more criminal organizations are becoming more energetic and bring even more innovations in the provision of transformation of their illegal initiatives into usable assets. The result is that money laundering is one of the most important links between the criminal world and the legitimate society. Money laundering is one of the ways in which criminal organizations wish to penetrate into the legal economy and often involve seemingly respectable members of society (bankers, lawyers, etc.). Admission of money laundering to flourish undisturbed will have corrosive impact on the integrity of financial institutions [1]”.

With the amendments to the international regulations, made major changes in incrimination of this crime, so it is removed the requirement for prosecution, greater benefits, need not necessarily prove the existence of a prior offense - predicate offense and provided other criminal behavior that protects the confidentiality of keeping financial controls over suspicious transactions of legal and natural persons. Envisages criminal responsibility for an official, responsible person in a bank, insurance company, company is engaged in games of chance, exchange, stock exchange or other financial institution, a lawyer, except when acting as a lawyer, notary or other person exercising public powers or matters of public interest, which would allow or permit a transaction or business relationship, contrary to the prohibition imposed by the competent authority or a temporary measure determined by the Court, or failing to report money laundering, property or other proceeds that he found in exercise of their functions or duties.

Then for the official, responsible person in a bank or other financial institution, or person performing activities of public interest, which by law is authorized entity for measures and actions to prevent money laundering and other proceeds, which on unauthorized customer or to an unauthorized person shall disclose information relating to the procedure for examining suspicious transactions or the implementation of other measures and actions to prevent money laundering. As qualified forms of the offense is: if the crime was committed out of greed or because data usage abroad. By this provision protects the confidentiality of financial investigation by financial institutions at home and abroad. Any disclosure on this secret is quite a large risk and a danger of offenders to take action to recover money from the accounts and seeking other ways to switch to safe places abroad or hiding the "cash".

***Corresponding author:** Ivica Simonovski, Co-Founder of Cyber Security, Corporate Security and Crisis Management Initiative, Skopje, Macedonia, Tel: 389-0-76-31-93-19; Fax: 389-0-78-26-82-68; E-mail: ivceC3I@yahoo.com

Received December 31, 2015; **Accepted** February 29, 2016; **Published** March 15, 2016

Citation: Simonovski I, Nikoloska S (2016) Profiling of High Risk Profiles of Clients in Order to Prevent Money Laundering and Terrorism. J Forensic Anthropol 1: 102.

Object of protection is defined as: 1) Monetary, financial and 2) the legal terms of the acquisition and disposal of property and money in the economic performance [2].

As an object of protection in this crime is significant:

1) Whether money or property acquired by commission of the predicate criminal act or there are reasonable suspicions that money or property have a illegal origin - source;

2) To determine the properties, status and role on criminal offenders in the criminal operation;

3) The structure and functioning of the criminal group, gang, in order to detect whether the money laundering offense is committed by an organized group or criminal gang;

4) Determining the involvement of officials, responsible persons or persons performing activities of public interest;

5) The type and the amount of laundered money.

The term "money laundering" is used to describe the procedure in which the "cash" money derived from illegal and criminal activities are converted into legal form, in a manner that conceals their origin or ownership. While money laundering schemes can be of various degrees of sophistication, they are designed to accomplish the goal - to blur, or if possible to eliminate attempts to control. Different ways and modus operandi that follow with the laundering of dirty money is only limited by imagination and creative expertise on entrepreneurs who develop these schemes [3].

In modern conditions of economic operation of functioning of economic relations, the distinction between legal and illegal is so complex, it is very difficult to determine the border between both. This situation is a product of the modern development of economic relations and the tendency modern liberal economy to get rid of the control of the state, which seeks to control the continued operation of the companies and economic organizations and relationships in which they are exercised. This contradictory tendency creates the difficult problem on distinguishing the legal from the illegal, and therefore strive to ensure a prosperous economy [4].

The meaning of the subjects to the functioning of an efficient system for prevention of money laundering and terrorism financing is explained by two aspects. On the one hand, it is an indisputable professionalism of the employees who work in the entities, their professionalism and knowledge in that work, coupled with knowledge of the fight against money laundering and terrorist financing, a source of experience regarding the identification of products customers and activities at risk in terms of money laundering and terrorism financing as a source of identifying ways and methods to carry out these criminal activities. On the other hand, it is important to point out, starting from the fact that employees of the entities are best familiar with their customers, their intentions and legitimacy of the activities they perform, ie knowing the profile of its client, very easy to recognize activity that deviates from the usual activities of client activity that is logical in terms of the whole on that business relationship [5].

The entities have separate lists of indicators developed by the Financial Intelligence Units, and these lists are accepted internationally and are constantly supplemented and corrected. From another point of view, they are like manual work or roadmap in terms of detection and identification of suspicious clients and suspicious transactions.

The first component of the set of measures and actions that need to be undertaken by the entities is an analysis of the client.

Entities are required to implement on procedure analysis of the client in these cases:

- When establishing a business relationship.
- When performed one or several related transactions amounting to EUR 15,000 in denar equivalent or more.
- When there is suspicion of money laundering or terrorist financing, regardless of any exemption or amount of funds.
- When there is doubt about the veracity or adequacy of previously obtained data on the client.

The procedure of analysis of the client includes the following:

- Customer identification and verification of his identity.
- Identification of the beneficial owner and principal and verifying his identity, ownership and management structure.
- Providing information on the purpose and intended nature of the business relationship or transaction.
- Constant monitoring of the business relationship, including a detailed review of the transactions undertaken in the framework of that relationship, in order to ensure that transactions are carried out in accordance with the objective, business and risk profile and financial condition of the customer and update the customer.
- Subjects apply any measure, but may determine the extent depending on the risk assessment of the client, business relationship, product or transaction.

The Need for Risk Assessment

"If you don't know where you are going any road will take you there."

(*James Howcroft, George C. Marshall European Center for Security Studies, Director of Program on Terrorism and Security Studies****)***

The strategy is a plan that should answer the following questions:

- What do you do… (Object)
- How to do… (Methods)
- What… (Resources)

The determination of threat is a driver in the creation of a specific strategy that will allow balancing the available tools and resources and allocating them in order to minimizing risk (Figure 1).

Profiling the high-risk customers is essential for the financial situation, in this case the bank in order to determine the potential risk of establishing a business relationship with them. In terms of competitive race in gaining customers, and more profits for the bank the question is whether the bank has an interest to establish business relationship with customers who are potentially risky customers? - The answer depends on internal business policy of the bank. How the bank is ready to carry the burden called "risk client" on his shoulders, while consciously or unconsciously threatening reputational risk and security risk in the country. As an illustration, if the bank established business relationship with a customer who is on sanction list, the consequences will be borne by the bank and the state at international level because it has not taken appropriate measures to prevent it and to guarantee its own security. The main goal in this article is to perform profiling high risk profiles

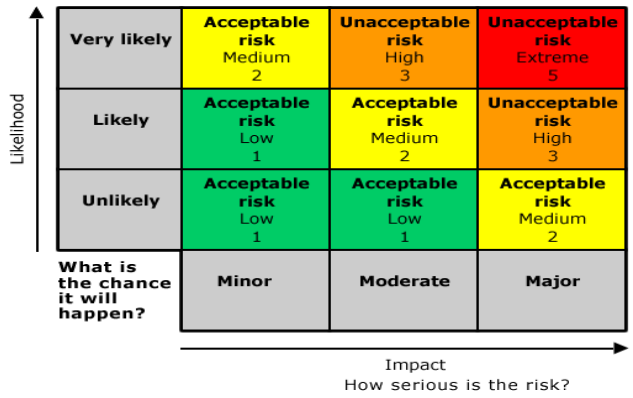

Figure 1: Security risk assessment.

who wish to establish business relationship with the bank or Profiling of high-risk profiles that have already established business relationship with the bank and in accordance with the objectives of the strategy and aimed at minimizing risk, it is necessary to carry out their detection, determination of risk (rating), paying attention and monitoring [6].

Know Your Customer Proceure – KYC Standards

As mentioned before, the main objective of KYC Procedure is to prevent banks or other financial institutions from being used, intentionally or unintentionally, consciously or unconsciously for money laundering or financing of terrorism activities. This procedure will enable banks to know their customers, to know and better understanding their financial dealings. From other side, KYC procedure will help them to manage their risk prudently. An institution's AML program may have a very rigorous and robust KYC program, complete with stringent account opening procedures; however, if this data is not readily available, then banks can face the prospect of limited risk factors for consideration in their risk modeling [7].

The KYC program should define the strict criteria which will be implemented in the process during the establishment of the relationship between the client and the bank. The Customer Acceptance Policy indicated the criteria for acceptance of customers shall be followed by all banks, and the banks shall accept customer strictly in accordance with that policy. The banks would not be allowed to establish a business relationship in the following cases:

- In cases in which the entity wants to open an anonymous account or used fictitious name(s);
- In cases in which the entity is a famous perpetrator of crimes or having connections with the criminal organization (s), want to establish business relationship with the bank;
- In cases in which the entity is a terrorist or having connections with terrorist organizations;
- In cases where the entity coming from country where operating criminal or terrorist organizations;
- In cases where entity based in high risk countries/jurisdictions or locations;
- Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk;
- In cases where entity is listed in sanctioned list issued by United Nation Sanction Committee, European Union, Interpol and other similar international organizations;
- In case of Non face-to-face customers;
- In all cases when the client due diligence measures cannot be implemented by the bank, the bank shall be obliged to reject to establish business relationship [8].

In order to generate a risk, banks may include additional factors through which they would do an assessment. That factor included:

- The transparency of company structures and beneficial owners;
- Political connections of the customer or associated individuals;
- The customer's reputation and/or known adverse information about the customer;
- The source, structure and adequacy of information about the customer's wealth;
- The source of the customer's funds;
- Expected activity on the account (types of transaction, volumes, amounts, the use of cash);
- The customer's profession/industry sector;
- Involvement of natural or legal entity in public contracts.

The branches shall make necessary checks before opening a new account so as to ensure that the identity of the entity (Potentional client) does not match with any of abovementioned criteria. In cases when the entity is match with any of abovementioned strong criteria, the banks would not be allowed to establish a business relationship with the natural and legal person. Thus the banks primarily protect its own reputation and are not included in any risk and protection form possible abuse for the purpose of money laundering and financing of terrorism.

Profiling of High Risk Profiles of Clients in Order to Prevent Money Laundering and Terrorism

The procedure of profiling high risk profiles of clients is different than procedure of "The Customer Acceptance Policy". The reason is very simple. This procedure covers profiling of customers who have already established business relationship with the bank and who previously have passed through the filter of the strict criteria used in the process of establishing business relationship. This procedure will allow the bank to use the available tools and resources in order to determine the risk of risky customers, categorizing them into certain levels, such as low, medium and high, or they can be more elaborate, such as low, medium, medium - high, high and very high, with the ultimate aim to minimize and menage the risk [9].

As I mentioned before, there is no financial sector business which is immune from the activities of criminal elements. The level of Money Laundering and Financing of Terrorism Risk to the customer shall be assigned on the following basis [10]:

Low risk level

Low level risk, banks can determine in cases in which the identity and sources of wealth of the individuals and entities can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as low risk. Additional criteria for low risk customers could be employees whose salary structures are well

defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover. Also customers who receive salary from Government Departments and Government owned companies, regulators and statutory bodies etc., can be designated as low risk. Depend case by case, only the basic requirements of verifying the identity and location of the customer shall be met. [11].

Medium risk level

Bank can categorize customers as medium or high risk according to their origin, nature and location of activity, country of origin, sources of funds and his client profile etc; such as:

➢ Customers in business or trading activity (including export/import, reexport) which live or place of business has a scope or history of unlawful trading and business activity.

➢ In cases in which the bank estimated that the profile of the customer when opening the account is uncertain and doubtful.

High risk level

High risk client's bank may categorize on the basis of strict criteria (some of them mentioned in the above text) and based on the products and services used by customers. As most used criteria for risk assessment for money laundering and financing terrorism are:

➢ Risk from the country of origin,

➢ Risk from a profile of a client,

➢ Risk of a product or service [12].

Risk from country of origin: As a separate category for risk assessment is determined the geographical risk, i.e. risk from country of origin**.** The evaluation of the risk from country of origin is performed according to the following:

➢ **For natural persons:** The residence country

➢ **For legal entities:** The country in which is the legal entity's seat.

Countries with high risk, from money laundering and financing terrorism point of view, are those countries with high corruption index, unsecure economical and political systems, inefficient legal system or small number of requirements for the documentation needed for opening businesses, countries known for production, processing and trafficking drugs and weapons.

As additional factors that would influence the decision whether some country represents a risk, could be:

➢ States under sanctions, embargos or similar measures, issued, for example, from the United Nations,

➢ States identified, by credibility sources, as states having incompatible regulation for prevention of money laundering and financing terrorism with the international regulation from this area,

➢ States identified, by credibility sources, as states financing and supporting terrorism [13].

Risk from profile of a client: *Clients with high risk,* from money laundering and financing terrorism point of view, are clients whose activities can cause higher risk i.e. within which can be encountered one or more of the following criteria:

➢ Significant and unexplainable geographic distance between the entity who should perform the activity and the place of residence or the seat of the client;

➢ Frequent and unexplainable movements of assets between accounts in various financial institutions;

➢ Frequent and unexplainable cash flows between financial institutions in different geographic areas;

➢ Clients for which is difficult to identify the real owner (off-shore companies).

➢ Cash activities that include or originate from:

➢ Activities that offer money services (remittances, exchange of foreign-exchangeable operations, services for fast money transfer, as well as other activities offering money transfer)

➢ Casinos, betting shops and other activities related to the games of chance;

➢ Activities which in regular business operations are not in cash, and which generate large amounts of cash for certain transactions;

➢ Charity organizations and other "non-profit" organizations which are not subject of a control (especially the ones acting across borders);

➢ Bank accounts of accountants, lawyers or other professionals who act in the name of their clients, who by the financial institutions are treated as VIP clients;

➢ Clients using non-resident accounts, especially as an opportunity for assets transfer across borders.

➢ Using mediators within the business relationship which are not subject to the regulation for prevention of money laundering and financing terrorism and is not supervised;

➢ Using corporate mediators or other structures in order to unnecessarily increase the complexity and decrease the transparency.

➢ Clients who are politically exposed and others.

Risk from products/services: The overall risk assessment should also contain assessment performed according to the third category of risk, i.e. according to the risks of money laundering and financing terrorism, which can appear in using certain products or services offered by the entities. From this point of view, the entities should take into account, both, the new products and the services, not directly offered by them, because they play the role as mediators, i.e. their services are used to deliver the product [14].

While determining the risks of money laundering and financing terrorism by products and services categorized according to riskiness, we should take into account the following factors:

a) *Products with low risk,* from money laundering and financing terrorism point of view, are: products that the bank makes them easy available, i.e. in the cases of financing, loans or mortgages with long lasting business relationship between the bank and the client.

b) *Products with high risk,* from money laundering and financing terrorism point of view, are the ones that include high level of anonymity or are referring to cash transactions. Services and products which can be categorized as potentially risky, associated with money laundering or financing terrorism, are:

➢ International correspondent banking services which include transactions, i.e. commercial payments for persons who are not clients of the bank-mediator;

➢ Services including transactions' realizations through use of non-resident accounts;

➢ Private banking services;

➢ Services including or enabling cash usage;

➢ Services related to trading with precious and noble metals;

➢ Services related to the new technologies or developing technologies preferring client's anonymity, for example, electronic banking etc.

The entities who after the performed risk assessment have determined high risk, should implement appropriate measures and control in order to reduce the potential risk. Parts of the measures that can be undertaken by the entities are following:

➢ Increasing the awareness for their own high risk clients and transaction;

➢ Reinforcement of the measures for knowing the client and reinforced analysis of the client (CDD) ;

➢ Increasing the requirements for account approval and establishing business relationship with the client, ;

➢ Increased monitoring and analysing of the transactions;

➢ Increased level of continuous control of the business relationship with the client;

➢ And many other

Some Different Approach

For the purpose of his research we will present one different procedure for profiling the high risk customers. To perform profiling of high-risk profiles first need to determine the following basic criteria:

➢ Sex;

➢ Age;

➢ Social status (data based from aplication);

➢ Economic status (data based form transaction analyses);

➢ Microenvironment (in which areas perform payments and payments of cash);

➢ Criminal past (based on online data and public information);

➢ Psychological Profile (monitoring the activities of the client by the bank officer);

➢ Politically exposed persons (PEPs);

➢ Nature and intended purpose of the business relationship;

➢ Resident or nonresident;

➢ Sanction lists or black list;

➢ High risk countries.

Based on the above criteria, the bank officials should be observed and prepare an initial profile of their clients in order to identify whether it is a risky customer or not. Each of these criteria is linked to each other and each criterion answers the specific question that banking officer sets when profiling.

The determination of sex and age answers the question whether the client belongs to a certain vulnerable group which according to these two criteria are suspicions and that may be involved in suspicious activities related with money laundering and especially financing of terrorism.

Then, based on the information stated in the application for establishing a business relationship determines whether the status of the person, whether it is employee, whether he is on welfare, pension, etc.. These data are compared with data obtained from the analysis of the economic power of the client, ie the dynamics and value of funds that have entered or are paid from the client's account.

Then compare the regions or branches in which the client performs banking services, ie entry and payment of funds.This information is important in order to determine whether the customer often changes various branches of the bank in order not to leave suspiciousness in some bank officer or a customer intends to perform banking services with just one bank officer then determines whether the bank branches where performed services are located in areas that are suspected to have the presence of supporters of terrorist organizations or radicalism and extremism. Using publicly available information through the media and Internet have to determine whether the client behind a criminal record and history in order to see what is his profile. Based on a psychological profile, banking officer should determine whether the client during his visit to the bank performs dubious activities, his physical appearance, nervous, scared, whether it comes in the presence of other people and etc. And finally determines whether the customer is a politically exposed person (MP, Director, Minister, President etc..), whether a resident or coming from another country which is high risk country, ie a state that does not implement standards on the legal framework for prevention of money laundering and financing terrorism or state in which there are terrorist organizations, terrorist organizations and sponsors etc..

In order to have a complete picture of your customer, the bank should provide information on the nature and intend purpose of the business relationship and means measures to establish the customer's occupation and source of funds. This kind of information is crucial to provides banks with a solid basis for monitoring the business relationship and opportunity to assess whether the proposed business relationship is in line with the bank would expect.

Before, we mentioned that the banks would not be allowed to establish a business relationship in cases where entity is listed in sanctioned list issued by United Nation Sanction Committee, European Union, Interpol and other similar international organizations, or other internal "black" list issued by the bank or other institutions. In certain cases may occur, the client who wants to establish a business relationship with the bank is not on a sanction list, but during the realization of business relationship to be put on a sanction list. In this case the bank shall immediately freeze the accounts of the customer to terminate the business relationship or to set up monitoring, qualifying it as a high-risk client.

Above we mentioned that as a separate category for risk assessment is determined the geographical risk, i.e. risk from country of origin. This kind of information is important to provide banks with a solid basis with the residence country for natural person and the country in which is the legal entity's seat. Also very important for the bank when analyzing the client to determine whether the customer realizes business activities with legal or natural persons from countries that are characterized as high-risk.

Each of these data are scoring (Scoring), and client rank and determine whether to proceed with further analysis.

If bank officials determine that it is a high-risk client access to further deeper analysis of its banking transactions, to determine whether there are suspicious transactions and to execute them scoring.

Then are making scoring of cash transactions, loans, exchange transactions, foreign exchange operations, quick transfers through money transfer etc.. There bank officials determined that transactions are unreasonable, unusual for the client and its business, or transactions that deviate from daily operations. When scoring finished, bank officials rate the client, or make its profiling and identification of suspiciousness.

The second method of determining high-risk profiles is based on templates for comparison. For this it is necessary to carry out financial reconstruction of the customer accounts (natural or legal person) who had committed a crime. So, first choose a target group or individuals for which there are data that they are perpetrators of money laundering or terrorist financing. Then conducts analysis of bank transactions until the moment of committing a crime in order to determine whether there are indications that the suspected bank transactions indicating that the person will commit a crime.

Thus creating templates especially used in detecting criminal acts of terrorism (suicide, participation in foreign military etc..). Also these templates can be used for detection of crimes of cybercrime, trafficking in drugs and human trafficking.

The method of creating the templates will be shown in Figure 2:

According to the abovedescribe case, the object of analysis is the individual who has already committed a terrorist or bomb attack. Analysys is made on banking transactions per month and several months before the event. The goal is to determine whether there were transactions that indicated some suspiciousness, illogical, extraordinariness regarding regular operations of the client.

As can be seen from the analysis, in January, the individual had an influx of cash based of salary. During the month, the individual performed transfers based of payment of insurance and payment of living expenses. These transactions dynamic didn't paid attention in the bank employees. Over the next month, during the account analysis has identified the same dynamic of movement of transactions. In March, again has the same movement dynamics of transactions. This frequency and dynamics of transactions does not cause suspiciousness and client may be subject to deeper analysis. Further analysis determined that in April the customer received funds based on salary, but now as can be noticed missing transactions based of payment of insurance and payment of living expenses, transactions which in the past few months are realized. These actions or inaction by the client should cause attention in order to further monitor the client. In May, there is the same situation as the previous month. This situation should cause suspiciousness among bank officials and they should submit a report to the financial intelligence units of their further processing.

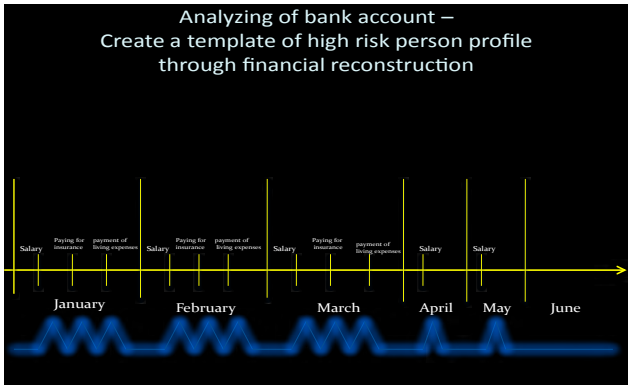

Figure 2: Template of high risk person profile.

As a brief conclusion of the case described above, the person who committed suicide bombing, before doing a terrorist act, stopped paying the living expenses and the cost of insurance as a hint that they are preparing for departure to another world. It is the philosophy of the terrorists before they do the deed, they waive all.

Conclusion

The conclusion begins with this sentence "*There is no single profile*" exactly because each case is separate and apart from the previous or next one. We must distinguish the typology that perpetrators of criminal acts of terrorism differs from the typology of crimes of cybercrime, trafficking in drugs and so on. There is an opportunity to make typologies for each crime separately, based on the practice of bank employees and using templates for high risk customers who already committed a crime. They should be used for comparison in identifying the same or similar high riskprofile clients.

But in terms of keeping preventive policies, determining the riskiness of the client and its profiling will provide an opportunity to discover the perpetrators of crimes during the commission of the crime of cybercrime, trafficking in drugs or events that precede the execution of a crime related to terrorism (suicide bomber, participation in foreign military etc.).

An additional requirement in the conduct preventive policy is timely delivery of information. In this case, bank employees will discover a high risk profile, and they are obliged to promptly inform the Financial Intelligence Unit to act within their jurisdiction. In such cases, retroactive policy may not be useful because the act is implemented, and the damage done.

And finally, in terms of the cash economy or cash payment, the question is whether you can create a profile of high risk customer.

References

1. Houston Real Estate Lawyer's Council (2009) Anti-Money Laundering and its cousin Counter-Terrorism(ist) Financing. Bakerbotts.
2. Petrovic B (2009) Money laundering is the contemporary security challenge.
3. Mihajlova V (1997) Money laundering and other proceeds of crime – the impact on the financial system, preventing the experiences of other countries. Macedonian Reviw of Criminal Law and Criminology.
4. Arnaudovski LJ (2008) Methodological problems of statistical recording and monitoring of economic crime.
5. (2011) Anti-money laundering and terrorist financing measures and Financial Inclusion. FATF Guidance.
6. (2011) Banks' management of high money – laundering risk situations. Financial Services Authority.
7. Basel Committee on Banking Supervision (2001) Customer Due Diligence for Banks. Bank for International Settlements.
8. FATF (2008) Financing of Terrorism. FATF+GAFI, Paris, France.
9. Price C (2008) Metavante White Paper: Customer Risk Assessment. Metavante – Risk and compliance Solutions.

10. (2014) Guidance for a Risk-Based Approach: The Banking Sector. Financial Action Task Force (FATF).

11. High-risk and non-cooperative jurisdictions. FATF's Public Statement.

12. (2015) Financial Regulators Release Revised Management Booklet. Federal Financial Institutions Examination Council, Virginia, USA.

13. What is Customer Due Diligence (CDD)? International Compliance Association, London, UK.

14. Syndicate Bank Services.