Mg.iur. ***Diāna Liepa****, doktorante*
Baltijas Starptautiskā akadēmija
Nīderlande

Pienācīga transakciju monitoringa nepieciešamība trasta sniedzējpakalpojumu uzņēmumos Nīderlandē

Anotācija: Naudas pārskaitījuma uzraudzības procesam (transakciju monitorings) ir būtiska loma naudas atmazgāšanas un terorisma finansēšanas apkarošanā. Holandiešu trasta sniedzējpakalpojuma uzņēmumi ik dienu izpilda nauda pārskaitījumus citu uzņēmumu vārdā, tomēr ir jāvērš uzmanība tam, ka ir nepieciešams īstenot pienācīgas, noteiktas un vienotas polises un procedūras savlaicīgas neparasto un aizdomīgo transakciju atklāšanai, kuras, savukārt, nepieciešams nodot finanšu ziņu vākšanas vienībai (FIU) tālākai izskatīšanai. Efektīvām transakciju monitoringa polisēm jāsatur sistemātiskas uzraudzības, kontroles procedūras, datu apstrāde, analīze un datu atbilstība iespējamiem risku faktoriem, noteikti pasākumi aizdomīgu naudas operāciju atklāšanas un novēršanas izpildē. Trasta sniedzējpakalpojumu uzņēmumiem ir nepieciešams pārņēmt un iekļaut transakciju monitoringu ikdienas uzņēmējdarbībā un pieņemt šādas procedūras un polises kā neatņemamu uzņēmējdarbības daļu.

Atslēgvārdi: naudas pārskaitījuma uzraudzības process (transakciju monitorings), neparasts darījums, trasta sniedzējpakalpojumu uzņēmums, naudas atmazgāšanas novēršana, atbilstība (compliance), finanšu ziņu vākšanas vienība (FIU).

Mg.iur. ***Диана Лиепа****, докторант*
Балтийская Международная Академия
Нидерланды

Необходимость надлежащего мониторинга транзакций в компаниях, предоставляющих трастовые услуги в Нидерландах

Аннотация: Процесс мониторинга денежных переводов (транзакций) играет важную роль в борьбе с отмыванием денег и финансированием терроризма. Голландские компании, предоставляющие трастовые услуги ежедневно выполняют денежные транзакции и в связи с этим, компаниям необходимо внедрить надлежащие, определенные и унифицированные процедуры, для своевременного выявления возможных необычных и / или подозрительных денежных операций, о которых необходимо сообщать в подразделение финансовой разведки. Эффективная политика мониторинга транзакций должна содержать систематический контроль, обработку данных, анализ и сопоставление таких данных с возможными факторами риска, определенные меры обнаружения и предотвращения выполнения таких транзакций. Трастовые компании должны интегрировать политику мониторинга транзакций в свою повседневную деятельность и рассматривать ее как неотъемлемую часть своего бизнеса.

Ключевые слова: мониторинг денежных переводов (транзакции), необычные и подозрительные денежные переводы, трастовая компания, борьба с отмыванием денег, соответствие правилам (комплаенс), подразделение финансовой разведки (FIU).

Mg.iur. ***Diana Liepa****, Doctoral Student*
Baltic International Academy
The Netherlands

The need for proper transaction monitoring in the trust service provider companies in the Netherlands

Abstract: The transaction monitoring process plays a vital role in combating money-laundering and terrorism financing. The Dutch trust service providing companies are dealing with the execution of the transactions on daily basis and are required to implement proper, defined and uniform policies procedures in order to be able to timely detect the possible unusual and/or suspicious transactions and report them to the national Financial Intelligence Unit. The effective transaction monitoring policies should contain systematic controls, processing of data, analyzing and matching such data with possible risk factors, certain measures for detecting and preventing the transaction being executed. The trust companies should integrate such transaction monitoring policies in their daily business and consider such compliance policies as integral part of the business.

Key words: transaction monitoring, unusual transaction, trust service company, anti-money laundering, compliance, FIU.

Introduction

The recent Panama Paper leaks 11.5m files from the database of the world's fourth biggest offshore law firm, Mossack Fonseca [1] containing personal financial information about some of the Mossack Fonseca shell corporations, which were used for illegal purposes, including fraud, tax evasion, and evading international sanctions, the Russian Laundromat case for laundering of $20 billion in Russian money stolen from the government by corrupt politicians or earned through organized crime [2] and the terror attacks of the last few years have placed further emphasis on anti-money laundering measures and the prevention of corruption, bribery, money laundering and terrorist financing. One of the vital elements of preventing and tackling with such crimes is implementation of adequate, proper and effective transaction monitoring systems that would be able to detect the possible suspicious, high-risk, out-of-the ordinary unusual transactions and prevent the transaction being executed. The effective and proper transaction monitoring procedures should be implemented within the Dutch trust service provider companies that are dealing with the financial transactions on daily basis.

According to the Forbes list "The Best Countries of Business 2017" the Netherlands is ranked No. 7 [3] due to the fact that the Netherlands is a well known country for the international entrepreneurs and businessmen with its strategic location, pro-business climate offering a solid combination of a stable economy, a reliable and favourable tax regime, the excellent legal and financial infrastructure as well highly educated and multilingual workforce.

The Netherlands is also familiar with its intermediary holding companies. A holding company is usually private or public company with limited liability that holds shares on behalf of its subsidiaries. The main purpose of an intermediate holding company is to collect dividends, royalties and interest payments from its subsidiaries, and channel the money to be paid out as dividends to a company in a low tax-regime jurisdiction or simply to pay the final beneficiaries. Often from the tax planning perspective the holding companies are used in order to gain favorable tax treatment, as there is no withholding tax on dividends in most cases, no capital gains on the sale of shares, and no foreign currency exchange restrictions. The corporate income tax in the Netherlands for its worldwide profits is at a rate of 20% for taxable profits up to EUR 200,000 and at a rate of 25% for taxable profits exceeding this amount, additionally the participation exemption regime may be applicable.

The intermediary holding companies are usually run by so called "trust offices" consisting of lawyers, accountants, notaries, tax consult-

ants and secretaries. The trust office offers a bunch of services compromising from the management and administration of the company by one of the employees of the trust company or its directors, providing domiciliation and suitable solutions for the daily business, advising on corporate laws and tax benefits, keeping the books, arranging necessary corporate documentation and legalization of such documents and finally executing the financial transactions. The trust offices are governed by the Dutch Act on the Supervision of Trust Offices (hereinafter Wtt) [4] and are supervised by the Dutch Central Bank (De Nederlandsche Bank, hereinafter DCB). According to the Wtt the trust offices must set up their operational management to the effect that they control identified integrity risks, such as risks of money laundering, evasion of sanctions regulations and corruption, as well the trust offices are required to verify the identity their customers and the origin and designated use of the assets belonging to these customers. Based on Article 16 of Money Laundering and Terrorist Financing (Prevention) Act [5] the trust office must be able to detect the unusual and suspicious transactions and report them directly to the Financial Intelligence Unit (hereinafter FIU) in the Netherlands. In order to detect the unusual transaction, the proper transaction monitoring policies and procedures should be laid down.

Transaction Monitoring

The main goal of the transaction monitoring policies and procedures is to detect possible suspicious, high-risk, out-of-the ordinary unusual transaction. The policies and procedures may vary per country, sector, the company and its capabilities, as well as choice of the systems to be used for the transaction monitoring purposes, for instance, atomized computer system or manual in real-time monitoring.

Based on the reports, research papers, guidelines and good practices published by the DCB, the bank calls for implementing the proper transaction monitoring within the trust sector which would serve as an effective way for financial institutions to counter the risks of money-laundering and terrorist financing.

Systematic transaction monitoring process

According to the DCB Good Practices [6] it is advised that the systematic transaction monitoring process shall include the following steps:

1. Analyzing the integrity risks on the client's level;

The analysis includes the initial client verification and identification process. It is necessary to establish who the client is, what kind of business activities are and would take place, where is the "money" coming from, what type of transactions and amounts are expected within this client's portfolio, the residence of the client as well as its position and initial source of wealth of the client and accordingly assign the integrity risk (low, medium, high).

2. Setting up the transaction profile of the client, potential transactions that can take place;

Each trust company shall set up the transaction profile of the client. The decision on how it should be done depends on each and particular company and its resources. The main types of transaction monitoring are computerized software systems which perform the transaction monitoring on automatic basis or hand-draw profiles, where particular responsible person/s should match the available data on manual basis. The profiles should be drawn in such way that it represents a summary of overview of the client. The profile should include, but is not limited to, the following elements:

a. the customers product and activity;
b. the nature, scale and complexity of a financial institution's business,
c. the diversity of the operations, including geographical diversity;
d. whether any intermediaries and/or third parties are applicable;
e. the maximum and minimum amounts being transferred;
f. the flow of funds and corresponding parties sending and receiving the funds;
g. the frequency of the amounts transferred;
h. whether countries with low Basel anti-money laundering index, low corruption perception index and/or law bribery perception index are applicable;

i. whether the financial institution, in particular case, the trust office, has viewing rights of the bank accounts.

3. Monitoring of all the transactions that are taking place;

The most difficult task it to monitor the transaction and evaluate the risks before the decision for the execution of the transaction takes place. All the available data, supplementing documents of the transaction should be accessible to the person reviewing the transaction. Based on the available data the evaluator should establish whether there are any possible risks of money-laundering and/or terrorism financing. In case of any applicable risks, these should be processed, analyzed, reviewed, matched, evaluated and finally recorded whether the transaction can take place or not. It should be concluded in the report whether there are any risks that can be mitigated or not and why the transaction can or cannot be executed.

4. Interposing the adequate measures for keeping the records of transactions and their monitoring in the client dossier;

The transaction monitoring results whether these are positive, false positive or negative should be stored and kept in the client files according to the particular countries regulations. According to Article 25 of Regulation on Integrity of Business Operations under the Wtt (Regeling integere bedrijfsvoering Wtt 2014 / Rib Wtt 2014) [7] the client files should be kept at least for five years after the termination of providing services to the client, either electronically or physically.

5. Immediate and complete reporting of the unusual and suspicious transaction to the FIU.

In case there are any doubts that particular transaction can be related to the money-laundering of terrorism financing activities or considered as unusual to the client's portfolio, the transaction should immediately be reported to the Dutch FIU mentioning whether the reported transaction contains subjective or objective grounds.

Unusual and suspicious transaction and its indicators in the Netherlands

In order to be able to detect unusual and suspicious transactions it is important to pay attention to the risks, indicators that are applicable to the current client portfolio, including geographical location, sector product and transaction risk, the products and services known to have higher risks, frequency of the amounts being transferred as well as the amounts and the method of payment, for instance, whether the payment is in cash of trough wire transfer.

The Dutch law sets two types of indicators for such transactions, namely, the objective indicators and subjective indicators.

1. Subjective indicator

a. A transaction for which the entity has reason to believe that it might be related to money laundering or terrorism financing.

2. Objective indicators

a. A transaction by or on behalf of a person or legal person resident, or with principal place of business, or with registered office in a designated State (as specified in Section 9 of the Wwft Act);
b. A transaction to the sum of €15,000 or more, paid to or through the entity in cash, cheques payable to bearer, a prepaid instrument of payment (prepaid card) or similar means of payment;
c. It is reasonable to assume that transactions reported to the police or the Public Prosecution Service in connection with money laundering or terrorism financing are also reported to FIU-the Netherlands [8].

In case the report falls under one of the objective indicators, no further assessment is necessary, the transaction should be reported. If the report does not fall under any of the objective indicators, the subjective indicator may apply.

Detection of unusual transaction

The detection of unusual and suspicious transaction is not an easy task. Based on the possibilities and capacity of the particular trust office, usually the transaction monitoring can be done whether through the computerized technological software or in hand-drawn profiles. The choice of the method to be used depends on the capabilities, the manpower, and the available financial means for supporting and maintaining the data as well as on the number of transactions executed by the particular trust office. The banks, for instance, use computer software that allows banks to monitor customer

transaction on a daily basis or in real-time. Such systems require entering and combining data in the "Know Your Customer" database which automatically analysis the customer's historical information and account profile, matches against public and private information to search for risk factors, including, but not limited to, politically exposed persons' status. Such software is also able to monitor the account activity for unusual transaction patterns or events that exceed statistical thresholds within pre-defined scenarios. However, the banks also use manual transaction monitoring, especially for very high risk areas [9]. In this way the software can provide financial institutions with a "whole picture" analysis of a customer's profile, risk levels, and predicted future activity, and can also generate reports and create alerts to suspicious activity [10]. Additionally, the software typically utilizes temporal analysis to evaluate transaction over multiple dimensions of time. However, the management of the computer software requires special knowledge of computerized codes and analytical skills of the officer entering and reviewing data. Determining which codes should be included or excluded, documenting the anti-money laundering data flow or modification logic, and establishing a consistent, enterprise-wide data integrity standard are a few of the obstacles institutions must successfully hurdle to manage transaction data effectively [11].

On the other hand, the manually drawn up profiles require much more time, attention to detail and regular review of the data, as in comparison with the computer software, in this case the compliance officer is responsible for collecting and reviewing the data, matching it to the possible risks and evaluating and concluding whether such risks may lead to the detection of the unusual and suspicious transaction.

In both cases the following tasks should be performed in order to make sure that all transactions are monitored:

a. drawing-up a risk profile for every client;
b. check if each transaction is in line with the company's objective and transaction profile;
c. verify whether sufficient information has been provided to make a sound judgment;
d. assess whether there are any characteristics of unusual and/or suspicious transactions;
e. check if the transaction is within the compliance framework;
f. if there is any involvement of a politically exposed person or a sanctioned person/entity/product;
g. whether this is a sound business transaction (understanding the reason for the transaction);
h. conclude that money laundering and terrorist financing elements have or have not been observed.

It is an open question for each trust office whether the computerized software is much more beneficial, favorable, proper and less costly method being used for detection of the unusual transaction than hand-drawn portfolios. However, it should be noted that even computerized technological software depends on the accurate information timely provided by the client, its processing and analysis, matching against the risk profiles.

Main problems

Effective transaction monitoring and validation have become extremely difficult due to increasing transaction volumes, expanding business lines and geographies, and perpetual changes to the business landscape [11]. Often the process used for monitoring the transactions is inadequate for detecting the risks for money laundering and financing terrorism. The data is out-dated or not complete. The quality, accuracy and completeness of data clearly affect the quality of the alerts generated by a transaction monitoring system or hand-drawn profiles [11]. In order to be able to keep information updated, the regular check-ups should be performed, educated manpower should be employed, proper processing and reporting systems should be available as well as the willingness of the client to cooperate and reply should be achieved. The employees must be trained accordingly in order to be able to verify, identify and record required information, thus making it possible to detect in time the possible unusual or suspicious transaction. Inevitably, the trust office should subscribe to a number of databases that contain information on sanctioned and reported persons and legal entities. The following databases may be useful for the verification and identification

purposes: Relian, World Check, Dow Jones, Accuity or any other client verification compliance database, which often are costly for smaller size trust offices and are hardly accessible for them. In such case, the alternative way of verification of the client should be established. Overall, the proper, defined and uniform transaction monitoring policies and procedures should be implemented.

Conclusions

Inevitably, the need for proper, defined and uniform transaction monitoring policies and procedures is vital for detecting unusual or suspicious transaction that may lead to the money laundering and terrorism financing activities. In order to be able to implement the proper transaction monitoring policies and procedures the companies shall maintain up-to-date client information, subscribe to a number of verification and identification compliance software, sanction lists, apply corruption perception CPI, BPI and Basel AML Index in their transaction monitoring portfolios. The trust office should be able to confirm the initial source of wealth of the client, monitor the incoming and outgoing funds, set up necessary measures to evaluate possible risks and frame proper reporting policies regarding the unusual and suspicious transaction. Finally, the trust companies should integrate the transaction monitoring policies and procedures in their daily business and consider them as an integral part of the business.

References

1. The Guardian, " What are the Panama Papers? A guide to history's biggest data leak" (News Article, 5 April 2016) <https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers> last accessed 24 April 2017.
2. Organized Crime and Corruption Reporting Project (OCCPR), "The Russian Laundromat" <https://www.reportingproject.net/therussianlaundromat/> last accessed on 24 April 2017.
3. Forbes, "The Best Countries for Business 2017", <https://www.forbes.com/best-countries-for-business/list/#tab:overall> last accessed on 24 April 2017.
4. Trust Offices (Supervision) Act of 17 December 2003 (Wet toezicht trustkantoren (Wtt)). See in Dutch at: < http://wetten.overheid.nl/BWBR0016189/2015-01-01> last accessed 24 April 2017.
5. Money Laundering and Terrorist Financing (Prevention) Act of 18 July 2008 (Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) Article 16. See in Dutch at: <http://wetten.overheid.nl/BWBR0024282/2016-08-11> last accessed on 24 April 2017.
6. Dutch Central Bank, "Concept Good Practices Transactiemonitoring bij Trustkantoren" (DNB Oktober2016) 4, see in Dutch at <http://www.toezicht.dnb.nl/binaries/50-235823.pdf> last accessed on 24 April 2017.
7. Regulation on sound operational management relating to the Act on the Supervision of Trust Offices of 15 July 2014 (Regeling integere bedrijfsvoering Wet toezicht trustkantoren 2014 (Rib-Wtt)), see in Dutch at: <http://wetten.overheid.nl/BWBR0035369/2015-01-01> last accessed on 24 April 2017.
8. FIU Nederland, <https://www.fiu-nederland.nl/en/meldergroep/261> last accessed on 24 April 2017.
9. Michael Shepard from Delloite Financial Advisory Services LLP, "AML Risk Assessments & Suspicious Activity Transaction Monitoring" (28 July 2009, Presentation). See at: <http://c.ymcdn.com/sites/www.iib.org/resource/resmgr/imported/20090728Presentation_Shepard.pdf> last accessed 24 April 2017.
10. ComplyAdvantage, "What is AML Transaction Monitoring" <https://complyadvantage.com/knowledgebase/anti-money-laundering/transaction-monitoring/ > last accessed on 24 April 2017.
11. Pricewater house Coopers, "From source to surveillance: the hidden risk in AML monitoring system optimization" (September 2010) 2-3.