HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Veres Viktória
info.vveres@gmail.com

ANTI MONEY LAUNDERING AND TERRORIST FINANCING IN PRACTICE WITH THE EYES OF AN ONLINE FINANCIAL BUSINESS

Absztrakt

Ez az írás egy EU tagállam, Ciprus példáján keresztül mutatja be a pénzmosás és a terrorizmus finanszírozása megelőzésére vonatkozó szabályozást. A szerző e szabályozás legfontosabb rendelkezéseit foglalja röviden össze egy gyakorlati példán keresztül: egy online pénzügyi szolgáltatást nyújtó bróker cég szemszögéből. A cikk egy olyan kutatás része, amely a pénzmosást és illegális pénzműveleteket a katasztrófák zavargások és háborúk összefüggésében vizsgálja.

This article examines an EU member state, Cyprus example of the Anti-Money Laundering regulations. The author looks at and summarizes the most important provisions of law from practical considerations, outlines the problems and implementation opportunities related from an online financer service provider (broker) view. This article is bases to a research of money laundering and illegal financial transactions in times of disasters, riots and wars.

Kulcsszavak: *biztonság, pénzmosás elleni szabályozás, pénzmosás elleni küzdelem, internetes broker ~ safety, money laundering legislation, anti-money laundering practice, online broker*

1. INTRODUCTION

„Money laundering is a threat to the good functioning of a financial system; however, it can also be the Achilles heel of criminal activity."[1]

Money Laundering and Terrorist financing is not only a serious threat to economy and business but at large it has a negative impact to society, therefore combating is international responsibility at all level[2].

As the financial system`s complexity has been rapidly growing and changing for example payment methods used more and more frequently for cross border transactions and support customer anonymity and quick movement of money `…a national system must be flexible enough to be able to extend countermeasures to new areas of its own economy`3. These new areas include especially handling the e-society and e-commerce that enables criminals to perform illegal activities in a widely sophisticated way.

Different countries have similar approach towards AML and TF, but the counties of the European Union have taken extra efforts and actions to customize their approach and actions even in their legislation. The AML regulations are very similar in the member states as they are implemented from the same root, the actual money laundering Directive the European Parliament and the Council in the European Union.4 Among other initiatives, the member states require companies registered under their territory to comply with the provisions of the law and report yearly, monthly and on demand to relevant institutions, these institutions share their data if needed. The directive is based among other on the Financial Action Task Force (FATF) recommendations, which working groups are dedicated to work out up-to-date recommendations on Money Laundering and Terrorist Financing related issues from multiple sectors.

The article takes into consideration the Prevention and Suppression of Money Laundering Activities Law N188(I)/22075 in Cyprus and the Directive of Prevention of Money Laundering and Terrorist Financing DI144-2007-086 of the Cyprus Securities and Exchange Commission.7

---

[1] Financial Action Force: Money Laundering FAQ
http://www.fatf-gafi.org/document/29/0,3746,en_32250379_32235720_33659613_1_1_1_1,00.html 2011

[2] Definition of ML and FT: WorldBank Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism Second Edition and Supplement on Special Recommendation IX http://siteresources.worldbank.org/EXTAML/Resources/396511-1146581427871/Reference_Guide_AMLCFT_2ndSupplement.pdf 2011 2011

[3] Financial Action Force: Money Laundering FAQ
http://www.fatf-gafi.org/document/29/0,3746,en_32250379_32235720_33659613_1_1_1_1,00.html 2011

[4] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Text with EEA relevance) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:01:EN:HTML

[5] Law Office of the Republic of Cyprus: The Prevention And Suppression Of Money Laundering And Terrorist Financing Laws Of 2007 and 2010
http://www.law.gov.cy/law/mokas/mokas.nsf/All/8019B1816F17B4CCC22577A6002BF960/$file/AML%20consolidated%20law%20188_I__2007,%2058_I__2010_final%2030.7.pdf?OpenElement

[6] Cyprus Securities and Exchange Commission:
Directive Dι144-2007-08 & Dι144-2007-08(A) Of The Cyprus Securities And Exchange Commission For The Prevention Of Money Laundering And Terrorist Financing
http://www.cysec.gov.cy/Downloads/Directives/InvestmentFirms/2009/DI144-2007-08.pdf

7 From here the expressions like Law or Legislation will refer to these 2 implemented in Cyprus based on the 3rd ML Directive of the European Union.

The legislation aims safer financial environment for customers, helps to combat money laundering and terrorist financing, on the other hand companies in the private sector are struggling with the resources to be allocated to these tasks especially in times of financial crises, disasters and political crisis's. Therefore it is essential to make companies interested in AML and TF besides the fact that they are exposed to fines and imprisonment.

This article examines the legislation from operational overview, considers the most relevant provisions of the law and outlines some possible problems and implementation opportunities connected to them from an online broker company and its customers view.

Companies in the brokerage sector or those providing online financial services are more likely involved in the Layering phrase of money laundering than in the Placement or Integration part therefore the assets must be focused on this[8],[9] and also these companies have to cope with the fact that there is no face-to-face interaction with the customers and that most of the transactions are carried out online.

In practice there are 3 key elements on company level to combat money laundering and terrorist financing to avoid the abuse of the company systems for layering ML: risk approach based right procedures and IT solutions to flag suspicious transactions, employee awareness and suspicious client or transaction reporting.

This article will be followed by a research of money laundering and illegal financial transactions in times of disasters, riots, civil wars, etc.

Basic provisions of legislation discussed in this article

The basic provisions of ML and TF of the examined legislation among others are the following for companies[10]:

- Appoint an independent Money Laundering Officer (MLCO)
- Create, maintain and implement an Anti Money Laundering Manual (AML)
- External and internal reporting of suspicious transactions to the relevant authorities
- Report cash transactions to the relevant authorities
- Create, implement, maintain and monitor procedures into the operating systems and control to make sure that the established and implemented procedures prevent the abuse of the Company`s systems for Money Laundering and Terrorist Financing purposes.
- Maintain, monitor and record customer information and transactions in a way that helps to spot suspicious activity
- Evaluate 3rd party dependencies
- Examine new products and markets to combat AML and TF risks arising from the company`s new activities

[8] Money Laundering FAQ 2011
http://www.fatf-gafi.org/document/29/0,3746,en_32250379_32235720_33659613_1_1_1_1,00.html
[9] More on the 3 stages of ML: International Money Laundering Information Bureau
http://www.imlib.org/page5_mlstgs.html
[10] Cyprus Securities and Exchange Commission:
Directive Dι144-2007-08 & Dι144-2007-08(A) Of The Cyprus Securities And Exchange Commission For The Prevention Of Money Laundering And Terrorist Financing
http://www.cysec.gov.cy/Downloads/Directives/InvestmentFirms/2009/DI144-2007-08.pdf

- Improve employee awareness by regular trainings, distribute the AML Manual, make sure employees understand their obligations

ANTI MONEY LAUNDERING AND TERRORIST FINANCING IN PRACTICE

Appointment of Money Laundering and Compliance Officer (MLCO)

Companies under this legislation are obligated to appoint MLCO and ensure that its function is independent. The MLCO is responsible to carry out the provisions of law by actively participating in the company`s policymaking, business development, moreover to create, implement, maintain and monitor procedures of the operating systems and control in order to identify risks arising and take necessary steps.

The employment of an MLCO might cause problems especially for small and medium companies as this profession requires complex legal, economic, business, financial and physiology knowledge and strong personal skills. The MLCO function as full time profession is relatively new therefore there is a shortage at the labor market of well educated and experienced employees. As a result the salary expectation of this profession puts a pressure on small and medium sized, especially new companies. Moreover in order to successfully fulfill its tasks the MLCO is to be trained and needs to train, this is also an addiction to the company costs.

The MLCO shall be involved into the company`s life wherever risks of ML and TF may arise such as when a company develops a new product, introduces a new payment method, or penetrates into a new market. There might be an opposition from the various departments to coordinate with the MLCO on these issues. Understanding the importance of the MLCO involvement of the department managers is essential and must be built and developed from the beginning. Most importantly the successful combat against ML and TF lies in the hands and responsibility of the management in order to assign sufficient resources to these functions.

Anti Money Laundering Manual (AML Manual) and Employee Training

Every company falling under the mentioned legislation must create and update on a regular bases a Manual that describes the company`s AML and TF practices, procedures and measures. This Manual must be distributed, thought and understood by all employees of the company.[11]

AML manuals are usually too long and complex to expect employees to read and take right consequences. Trainings are effective ways to communicate the legislation, AML and TF obligation, needs and procedures. Companies carrying out operations in more branches or countries must find cost effective ways. For example yearly one on-site training, and online training for new employees between on-site training periods. Not only the distribution of the AML manual and training is essential, but the establishment of a dynamic knowledgebase with case studies and examples contribute to the goals. For example knowledgebase and circulars are a good way to update employees dealing with customers from the Middle East on the increasing risks and vulnerabilities following the political crises.

Companies must make sure that their employees understand and follow the AML Manual, but most importantly that they are aware of their obligations such as how not to get part of

---

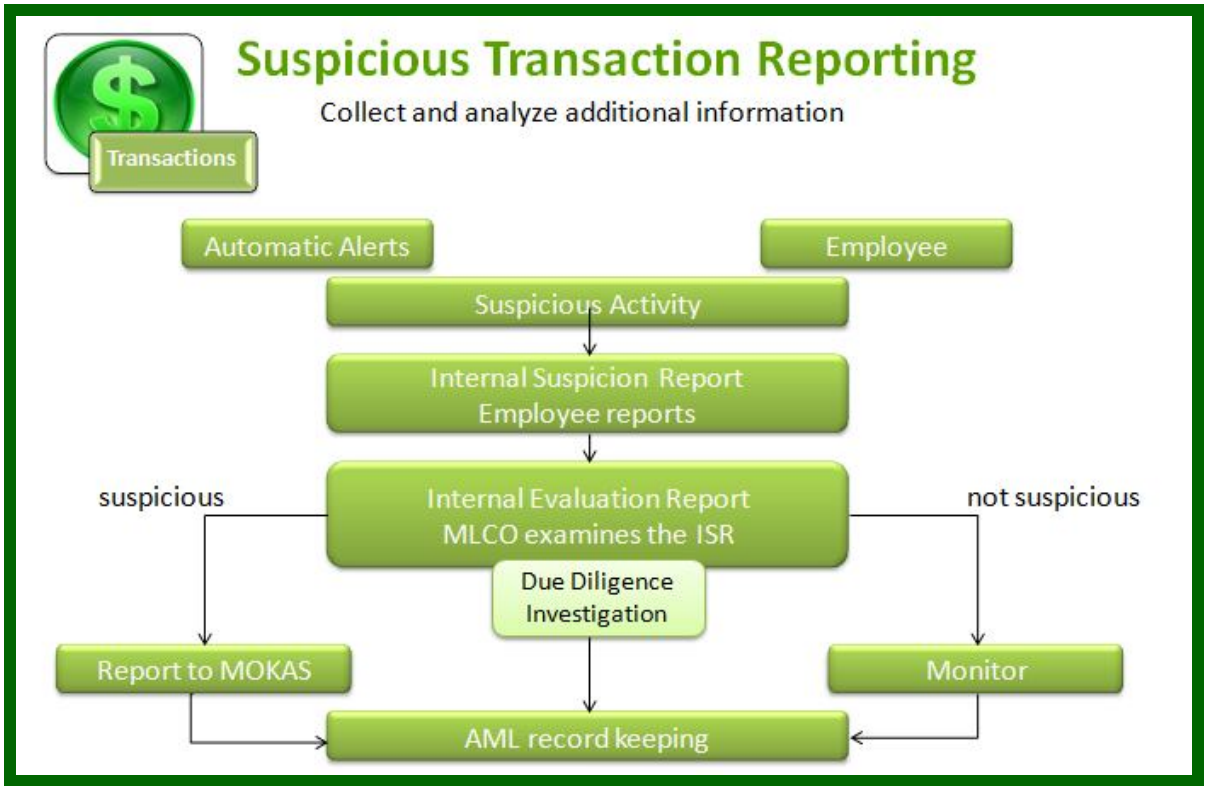
11 Cyprus Securities and Exchange Commission:
Directive Di144-2007-08 & Di144-2007-08(A) Of The Cyprus Securities And Exchange Commission For The Prevention Of Money Laundering And Terrorist Financing
http://www.cysec.gov.cy/Downloads/Directives/InvestmentFirms/2009/DI144-2007-08.pdf section VIII

ML and TF, how to spot and who to report suspicious customers and transactions. Employees who understand the real meaning of `dirty money` and the flow of the ML activity are more likely to report suspicious activity: at trainings it is important to emphasize something that they are sensitive to, for example that the dirty money can come from child abuse or human trafficking and by not taking steps they indirectly might help these criminals.

Reporting

Companies and employees are obligated for internal and external reporting and cash transaction reporting to an appointed person and relevant authorities.[12]

- Internal Reports: Internal Suspicion Reports are done by employees who suspect that a customer might use the company for ML and TF purposes, the money laundering officer must evaluate these reports, perform due diligence and decide if it is to be reported to the relevant authorities. The main problem with these reporting is that in practice employees with commission based salaries are not interested in reporting suspicious transactions as it can lead to losing customers and commission while the reporting (filling the Internal Suspicion Report forms, participating and providing information for internal evaluation) and follow ups might cause further inconvenience for them. Therefore, the MLCO must find the right procedures and monitoring to enforce the Law. The below slide shows the recommended flow of the suspicious transaction reporting from any employee of the company through the MLCO to the relevant Unit MOKAS in Cyprus.



1. picture. Suspicious Transaction Reporting Flow
Prepared by the author[13]

[12] Law Office of the Republic of Cyprus: The Prevention And Suppression Of Money Laundering And Terrorist Financing Laws Of 2007 and 2010, section 69

- External Reports:
  - Suspicious Transaction reports to relevant authority (based on the evaluated Internal Suspicion Reports)
  - Annual reports to relevant authority[14]
  - In Cyprus, the Relevant Authority (CySec) will not reflect the result of the review of the report to the Company and do not give recommendations to improve specific procedures. Companies can use the services of local External Auditors for this purpose before submitting the report, further costs apply.
  - Cash transaction Reports above a specific amount set in legislation[15]
  - Online companies obligated to issue monthly reports are facing problems with what kind of transaction in considered cash. In practice companies should consider Western Union, MoneyGram, etc transactions as cash, therefore include them into reporting.

Operational solutions for preventing Money Laundering

This part of the article describes the recommended policies and measure taken by online financial companies regarding combating ML and TF including new and existing clients, transactions, new products, new markets, etc.

Operational measures to prevent ML deals with issues related to money laundering and terrorist financing and include the assessments of the current weaknesses. Measures and procedures undertaken by the Company in order to prevent money laundering and terror financing should be based on the relevant legislation of Prevention of Money Laundering and Terrorist Financing. The policies and procedures include steps to be taken by the different operating teams in the Company in order to be able to identify possible Money Laundering and Terrorist Financing activities. However, usually the directives are not tailored for online flow of money. Implementation of such regulation into operational procedures in online financial services might be not cost effective, the risks that companies might take by not complying with the law depends on the company`s illegality tolerance. Using the right assessment tool to understand our compliance risk fitness, the risk based method can help a company to find the right balance to deal with risks arising from non-compliance with the legislation.[16]

---

[13] Slide was prepared by the author for company AML and TF training purposes, picture of the $ sign was taken from http://greenconduct.com/jobs/wp-content/uploads/2011/03/6a00d8341ee15453ef0147e30fc69a970b-800wi.jpg

14 United Kingdom example of how to build an annual report, same can be used in Cyprus or any other EU country: Joint Money Laundering Steering Group MLRO Annual Report http://www.jmlsg.org.uk/other-helpful-material/article/mlro-annual-report

[15] Law Office of the Republic of Cyprus: The Prevention And Suppression Of Money Laundering And Terrorist Financing Laws Of 2007 and 2010 sections 60

[16] Open Compliance and Ethics Group (OCEG): Compliance Risk Fitness: Assessing and Treating the Real Risks to Compliance webinar held 2/6/2011 http://www.oceg.org/event/compliance-risk-fitness-assessing-and-treating-real-risks-compliance

Risk based approach

Companies shall implement the risk based approach[17] into their policies and procedures in order to manage risks in an effective and affordable way. The Risk based approach includes the identification, recording and evaluation of combination of triggers and indicators of various Risks which may be related to money laundering and terrorist financing. These can be categorized as the following:

- Risks based on Client`s account type and nature (Corporate accounts, customers from high risk countries)
- Risks based on Client`s behavior (non communicating clients, clients unwillingness to provide identification documents, transactions that are flagged by Automatic system – (as described in point 8 below)
- Risks based on the Client`s initial communication with the Company (clients introduces by third person, branches outside of the Republic, managed accounts)
- Risks based on the Company`s Services and financial instruments (3rd party payments, large and high frequency of transactions)

In order to manage the above mentioned risk categories, the Company should define measures and procedures to be approved by the MLCO and performed by the various teams of the Company. For examples:

- Client Risk Categorization
- Identification Verification
- Due Diligence Procedures
- Transaction monitoring (deposits, withdrawals, money movements)
- Ongoing monitoring of high risk clients, etc

Client categorization

Client categorization is not only provision of law, but also utilized as a tool for the risk management. The division of clients into different risk levels groups enables the risk analyst to cope with high volumes and focus on relevant customers and apply different monitoring and verification procedures for each risk group.

The categorization of the clients and ML prevention processes are based among others, on the type of the client, his geographic location, economic profile, personal information, trading activity, and the funding methods he uses. The risk analysis uses own discretion for categorization. Though regulation gives clear instruction on how to categorize Customers but it cannot be effectively applied at online brokers: all non face-to-face customers should be considered as high risk clients and enchanted due diligence must be performed.[18]

In order to keep the economic sense 4 levels of risk categorization are recommended

- Low risk clients with low-risk results in client identification and due diligence
- Normal risk clients:_for example_clients from EEA countries using EEA registered financial institutions for all kind of money flow

[17] Directive Dι144-2007-08 & Dι144-2007-08(A) Of The Cyprus Securities And Exchange Commission For The Prevention Of Money Laundering And Terrorist Financing Part IV

[18] Directive Dι144-2007-08 & Dι144-2007-08(A) Of The Cyprus Securities And Exchange Commission For The Prevention Of Money Laundering And Terrorist Financing Fourth Appendix

- High risk clients with enhanced client identification and due diligence measures: for example countries that have not implemented FAFT recommendations, `Enhanced customer due diligence measures must be taken in all other instances which due to their nature entail a higher risk of money laundering or terrorist financing.`[19]
- Not acceptable customers, for example customers from groups or countries who are under UN embargo

Client Acceptance Policy

The MLCO is responsible to apply all previsions of the Client Acceptance Policy assisted by other departments and to ensure that the Risk based approach is implemented.

The Client Acceptance Policy is the most cardinal problem of the legislation and practice. There is a conflict of objectives. The legislation requires companies not to establish business relationship with any customers before full Customer Identification Verification (see point 4 below). Also, the General Manager should approve all new Customers before performing any transactions. Customers investing 50-200 USD to try the service will unlikely want to send certified passport and utility bill copies and it is impossible for a General Manager at a company to review and approve personally 100-250 new customers a day. Companies are exposed by losing customers or not complying with the Client Acceptance Policy requirements. Lack of Customer Awareness on regulations will be mentioned later in this article at the difficulties of building an Economic Profile.

Customer Identification Procedure

Companies should apply a Customer Identification Procedure[20] using different Know Your Customer (KYC) protocols for Individual and Corporate accounts. The identification procedure is based on Know Your Customer documents and information recorded and provided by the Client at registration. Verification documents should be accepted only in colored copies.

Clients must provide Identification verification documents as per the following:

- Clear color copy of government issued Passport including written signature (government issued IDs can be accepted as well and in special cases like India, Tax Authority Card provided the photo and signature of the Client is visible)
- Clear copy of recent Utility Bill (any bill that is not older than 3 moths and comes to the trading account holders name and address of residence e.g. water bill, electric, gas, telephone etc…) or Bank Statement
- Clear color copy of both sides of the Credit Cards used to fund the account, if any (the middle 8 digits from the front and the CVV number from the back is to be masked)
- Further supporting documentation may be requested by the risk management team, if required.

[19] Law Office of the Republic of Cyprus: The Prevention And Suppression Of Money Laundering And Terrorist Financing Laws Of 2007 and 2010 section 64 (2)

[20] Law Office of the Republic of Cyprus: The Prevention And Suppression Of Money Laundering And Terrorist Financing Laws Of 2007 and 2010 section 61-62

This can be followed by transaction and trading activity review (if exists): As part of the verification process the Risk Analyst should reviews the Customers Economic Profile including trading activity, relations by computer, payment method and transaction history.

Corporate Client Identification further needs are that all corporate accounts' should undergo a special evaluation by the MLCO before any transactions are carried out.
In order to successfully verify Corporate Clients Company shall carry out a 3 step procedure:

- Identifying the Company, directors, authorized signatories, ownership structure, etc with the following documents:
  - Certificate of shareholders
  - Articles of association
  - Certificate of directors
  - Certificate of incorporation
  - Passport copy of the directors
  - Board resolution
- Identifying the Authorized Person with the same procedure as it was an Individual Client
- Requesting and examining the Power of Attorney given by the directors to an Authorized Person for authorized actions. The Authorized Person can be an employee of the Corporate Client or other such as an Introducing Broker.

World Check as Due Diligence tool[21]

Use of external data base for electronic KYC is recommended. Providers as World Check System[22] can be used in order to identify possible Politically Exposed Persons, perform passport checks, confirm that the customer is not blacklisted or committed crime. Problem with these systems might be that the data provided is not correct (from experience I can tell that for example if an incorrect passport number is uploaded for a person having the same name as a weapon smuggler can be a misleading match that can cause losing customers) so even if a positive match is showing, the case must be reviewed and investigated by the Company to close out incorrect information. In case the positive match is justified the relevant initiations must be informed to help their investigation.

Construction of Client Economic Profile

The construction of the Client Economic Profile should be defined by the MLCO, and carried out by all relevant departments. The data and information collected for this purpose should be stored in the company's systems.

Example of the data that can be collected and evaluated:

- Information required by Client Acceptance Policy
- Client Identification Verification
- Anticipated account turnover
- Purpose of the business relationship with the Company
- Employment history, contacting employer, verifying income
- Family status, number of people living in the same household

[21] Law Office of the Republic of Cyprus: The Prevention And Suppression Of Money Laundering And Terrorist Financing Laws Of 2007 and 2010 section 61
[22] World Check http://www.world-check.com/ 2011

- On site visit at the customers residence
- Client transaction history review at Client Identity verification and withdrawal approval

Many customers find the establishing of their Economic Profile as inconvenience, they do not want to provide this kind of information and complain that other companies do not ask for this information. There is a lack of customer education on AML and TF issues and instead of having a greater trust towards companies who comply with regulations they end the business relationship and go to another Company with less `needs`. Experience shows that even if we inform customers that building an economic profile shows that we take regulations seriously. Customers do not consider it as a positive indicator. Especially in the EU there are plenty of official materials on the requirements of regulated financial Companies (example an Appropriateness Test), Customers are simply not aware of it.[23] This resistance and non-cooperation of Customers pushes Companies towards not complying and request less information to keep customers and grow business.

Third Party Payments and double funding

Third Party transactions should not be allowed in the Company's system with the exception of the Clients and the third Party`s written authorization (Power of Attorney) and full Identification Verification. The Company cannot allow deposits from corporate accounts to individual accounts and any private transactions funding corporate account. In such events, the MLCO shall instruct the finance department to refund the money to the same source and will notify the account owner to refrain from such transactions in the future.

Automatic system Alerts:

Money laundering activities can be limited by a set of automatic system alerts and flags of accounts and transactions which are triggered by similar indicators below:

- Apply automatic deposit limitations. In order to release the deposit limits from the account, the MLCO should accept the client.
- Identify and flag Name Conflicts: last and first name of the Credit Card holder are different from the customer name as registered in our system.
- Identify and flag Bin conflicts: client`s country in registration form does not match the Credit Card issuer country.
- Limit the number of allowed eWallet accounts used in the system from the last risk review by maximum 2
- Deposit country Conflict: Client tries to deposit from a country different than the country he has registered from.

The system shall be designed to limit the number of credit cards that are used by the client based on the rules set by the MLCO.

First transaction and deposit manual review

The Company should set monitoring procedures on Customers' deposits. Reviews should apply on all Customers' first deposits. Additional reviews can be carried out in case of alerts

[23]Committee of European Securities Regulators (CESR) A consumer's guide to MiFID Investing in financial products http://www.cesr-eu.org/popup2.php?id=4984

that are generated by the company's proprietary risk system or in case of alerts that are received by the payment service providers. Security reviews are performed by the Risk, Operations and Payment departments. The following deposit characteristics can trigger more detailed investigation:

- Indication for possible fraud by the payment processor (example - decline by the bank due to stolen credit cards)
- Third party payments – the account holder name is different from the owner of the deposited funds.
- Aggressive trading and wrong contact details.
- Multiple accounts connected to the same means of payment.
- Too many transactions, too complex deposit pattern
- Too many declined transactions
- Multiple deposit methods used on the same account
- Sleeping Money – customer deposited but not touching the money
- Too frequent in and outgoing payments
- Change in the deposit behavior - small transactions followed by a not justifiable high deposit

Companies with that integrated multiple regulated e-payment service providers or credit card payment services allow its clients to deposit and withdraw funds from their accounts in real time or almost real time. Regulated e-wallets such as Paypal, MoneyBookers and Neteller are performing identification verification checks to their clients according to European standards, but at the same time allow their clients to shop online securely without disclosing the payment methods that have been used to fund their e-wallet accounts. Most of the Company risk management and verification models relays on verification of ownership of the payment methods but not on verification of the origin of the funds as it would cause not bearable costs for the risk management.

Withdrawal processes

The Company should use identification verification and withdrawal policies in order to protect its Customers and prevent contributing to money laundering activities when sending funds. One of such policies that can be used by the Company in the withdrawal process is as following:

Predefined approval protocol that includes list of authorizations required (MLCO, Trading manager, General Manager) based on amount of money that is requested to be withdrawn. As a rule, withdrawal requests should be processed to the original means of payment that has been used by the Customer to fund his trading account. If the Customer has deposited via credit card or e-Wallet, the payment team must strive to pay the client back to the same cards or e-wallet account. If circumstances prevent the company from transferring the withdrawals to the original means of payment, the owner of the trading account will be requested to provide alternative payment method (by default – wire transfer details).

Withdrawal requests should be manually approved by Risk Department. The following information should be reviewed:

- Withdrawal request amount
- Withdrawal method
- Customer verification
- Copies of all Credit Cards used in our system are provided

- Customer country of origin of the funds and the Client, transaction history

Limited cash withdrawal payments shall be processed and all funds are to be processed via regulated financial entities that are following additional AML protocols. Special attention should be given in cases of large withdrawal requests from high risk countries like Malaysia, Indonesia, Pakistan, Bangladesh, Iran, Iraq, etc. and in cases of large withdrawal requests on accounts with limited trading activity relatively to the amount of funds deposited in the account.

SUMMARY

There are plenty of issues that have not been reflected in this article such as Partner AML and TF risk management, AML program for branches outside of the EEA, customers with specific needs or statuses, etc, but it gives a short overview on the complexity and additional resource needs of implementing AML and TF regulation to Company levels. It is obvious that Companies have difficulties to allocate enough resources and knowledge to create, enforce, maintain and monitor measures to all levels of the company. Countries and Regulatory Bodies should consider the characteristics of online financial service providers when designing the provisions, as to fully comply with the present legislation can lead to an uneconomic operation, loosing market, customers and competitiveness. The key is to ensure that the Company (with the help of the MLCO) establishes, maintains and improves a professional AML policy that is respected and followed by all employees, a policy that prevents money launderers to abuse the Company`s system, also can be supported with resources and do not harm the online based business model.

References:

[1] Financial Action Force: Money Laundering FAQ http://www.fatf-gafi.org/document/29/0,3746,en_32250379_32235720_33659613_1_1_1_1,00.html 2011

[2] WorldBank Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism Second Edition and Supplement on Special Recommendation IX http://siteresources.worldbank.org/EXTAML/Resources/396511-1146581427871/Reference_Guide_AMLCFT_2ndSupplement.pdf 2011 2011

[3] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Text with EEA relevance) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:01:EN:HTML

[4] Law Office of the Republic of Cyprus: The Prevention And Suppression Of Money Laundering And Terrorist Financing Laws Of 2007 and 2010 http://www.law.gov.cy/law/mokas/mokas.nsf/All/8019B1816F17B4CCC22577A6002BF960/$file/AML%20consolidated%20law%20188_I__2007,%2058_I__2010_final%2030.7.pdf?OpenElement

[5] Cyprus Securities and Exchange Commission: Directive Dι144-2007-08 & Dι144-2007-08(A) Of The Cyprus Securities And Exchange Commission For The Prevention Of Money Laundering And Terrorist Financing http://www.cysec.gov.cy/Downloads/Directives/InvestmentFirms/2009/DI144-2007-08.pdf

[6] International Money Laundering Information Bureau
http://www.imlib.org/page5_mlstgs.html

[7] Picture of the $ sign was taken from http://greenconduct.com/jobs/wp-content/uploads/2011/03/6a00d8341ee15453ef0147e30fc69a970b-800wi.jpg

[8] Joint Money Laundering Steering Group MLRO Annual Report
http://www.jmlsg.org.uk/other-helpful-material/article/mlro-annual-report

[9] Open Compliance and Ethics Group (OCEG): Compliance Risk Fitness: Assessing and Treating the Real Risks to Compliance webinar held 2/6/2011
http://www.oceg.org/event/compliance-risk-fitness-assessing-and-treating-real-risks-compliance

[10] World Check http://www.world-check.com/ 2011

[11] Committee of European Securities Regulators (CESR) A consumer's guide to MiFID Investing in financial products http://www.cesr-eu.org/popup2.php?id=4984