



# **PREVENTION OF MONEY LAUN- DERING IN A FINANCIAL INSTITU- TION**

Customer Due Diligence

Keijo Kauppinen

Bachelor's Thesis  
December 2013  
Degree Programme in  
International Business

TAMPEREEN AMMATTIKORKEAKOULU  
Tampere University of Applied Sciences

## ABSTRACT

Tampereen Ammattikorkeakoulu  
Tampere University of Applied Sciences  
International Business

KEIJO KAUPPINEN:

Prevention of money laundering in a financial institution  
Customer due diligence

Bachelor's thesis 59 pages, appendices 9 pages  
December 2013

---

Money laundering – emphasis on customer due diligence – as a final thesis topic was developed during my practical training as a banking advisor at Nordea Bank Finland. The topic was a current issue at work especially due to tightening legal obligations but also due to sanctions given to Nordea Group in Sweden for neglecting proper customer due diligence procedures. Not only was the topic current and important to the commissioner but also very interesting when connected to international business studies. The goal of the thesis was study the interrelationship of the parties involved: Finnish Act on money laundering and customer due diligence; party subject to the law; the customers of the party. How the law obliges the party to know its customers more thoroughly; how the party obtains information from the customer; how the customers react and experience the thorough interviewing when opening a new customer relationship.

The Finnish Act is very strict concerning customer due diligence. If it cannot be properly followed, a new customer relationship cannot be opened nor a transaction executed. There are numerous different money laundering methods and the scale of it represents an OECD 2009 study, where the amount of illicit money laundered globally in 2009 was evaluated to be 2.7% of the global GDP. Major issues facing financial institutions are: Identifying the origin of the funds; how a company's account will be used (what kind of traffic will be expected); and transparency of ownership. While the studies showed that major situations that caused suspicion was connected to incoming funds and money transfers, a survey conducted in the Nordea corporate branch among the employees supported this study. The major question in the survey was what kind of questions generated avoidance among customers and the most common answer was origin of the funds and future account traffic. The other survey was conducted in order to gain knowledge about customers' experience in the Nordea corporate branch. It is generally considered that the numerous questions in the interviewing might be irritating to the customers, but the survey results indicate contrary opinions.

In order for the interviewing to be smooth and comfortable, a conversational approach could be used. Customer service skills are highlighted in how the questions are asked. The main focus in obtaining information should be in knowing how the banking services/products will be used and where the funds are originating. This enables the detection of suspicious activity on both transparent and non-transparent companies.

---

Key words: money laundering, act on money laundering, customer due diligence

## TABLE OF CONTENTS

1	INTRODUCTION .....	5
1.1	Background information .....	5
1.2	Objective .....	6
1.3	Methodology .....	7
2	THE COMMISSIONER.....	8
2.1	Nordea Group .....	8
2.2	Nordea Bank Finland plc. ....	9
3	DEFINITION OF MONEY LAUNDERING .....	11
3.1	Origin of the term .....	11
3.2	Money laundering .....	11
3.3	Aggravated money laundering.....	12
3.4	Conspiracy for the commission of aggravated money laundering.....	12
3.5	Negligent money laundering.....	12
3.6	Money laundering violation.....	13
4	PREVENTION OF MONEY LAUNDERING .....	14
4.1	Introduction to legal obligations .....	14
4.1.1	Parties subject to reporting obligation .....	15
4.2	Customer Due Diligence.....	16
4.2.1	Identifying and verifying the customer .....	17
4.2.2	Identifying the beneficial owner .....	18
4.2.3	Obtaining information and on-going monitoring.....	19
4.2.4	Data keeping.....	20
4.2.5	Simplified customer due diligence.....	21
4.2.6	Enhanced customer due diligence .....	21
4.3	Reporting .....	24
4.3.1	Secrecy obligation and derogations concerning the secrecy obligation .....	25
4.4	Suspending and refusing to conduct a transaction.....	25
4.5	Training and protecting employees.....	26
4.6	Failure in customer due diligence and reporting obligation .....	26
4.6.1	Liability for damages .....	26
4.6.2	Violation of customer due diligence .....	27
4.6.3	Violation of the obligation to report money laundering.....	27
5	MONEY LAUNDERING IN PRACTICE.....	29
5.1	Statistics .....	29
5.2	Three-stage process of money laundering .....	32

5.2.1	Placement .....	32
5.2.2	Layering .....	33
5.2.3	Integration .....	34
5.3	Unusual activity .....	35
5.3.1	Unusual money flows.....	36
5.3.2	Ownership .....	39
5.3.3	Business .....	40
5.3.4	International trade .....	41
5.3.5	Service providers.....	43
5.3.6	Summary of unusual activity .....	43
5.4	High-risk countries .....	44
5.4.1	The Basel AML Index 2013.....	44
5.4.2	FATF High-risk and non-cooperative jurisdictions .....	46
5.5	Money laundering cases in Nordea.....	47
6	CUSTOMER SURVEY – NORDEA CORPORATE BRANCH .....	49
6.1	Basis for the survey.....	49
6.2	Corporate customers .....	49
6.3	Employees of the Nordea corporate branch.....	51
7	CONCLUSION .....	55
	REFERENCES.....	58
	APPENDIX.....	60
	Appendix 1. Europe – The Basel AML Index 2013 ranking (Min. 0 Max. 10).....	60
	Appendix 2. Basic Information Form.....	61
	Appendix 3. Questionnaire about customer identification at Nordea corporate branch – customers .....	64
	Appendix 4. Questionnaire about establishing a customer relationship at Nordea corporate branch – employees.....	66

# 1 INTRODUCTION

## 1.1 Background information

Globalization is a phenomenon that has been around for decades now – not to mention the colonial era centuries ago. There is nothing new about businesses willing to expand their markets and investments beyond national borders with the objection of gaining growth and increasing revenues, or due to the negative factors in the home market. While companies have been globalizing, the world has become smaller and smaller for the individual human beings too. The perfect example of this is the European Union: Free movement of goods and services, not to mention people (workforce and travellers). Europe has become a unified community where people from different countries can easily move to another country to work and live.

Without a doubt, the European Monetary Union is a result of an on-going globalization that has provided a single currency (euro) to be used in different countries in Europe. This has made the trade even easier within the European countries. Even though the previously mentioned attributes of the EU are “old news”, they are a great example of how the world is getting unified and smaller.

As a down-side of the globalization, in the European Union the free movement of goods and services has made it easier for criminal activity to go beyond national borders. Obviously, there has always been smuggling of illegal substances, human trafficking – to name a few – but without a doubt the integration of the world has enabled criminal activity to increase and become an issue that doesn't take into account national borders.

Concerning the banking sector, there has been an on-going process of creating the ‘Single Euro Payments Area’ (SEPA), the European Union is executing. The purpose of this is to create a unified payment system within the European countries instead of the old national systems (Finanssialan Keskusliitto, 2012). At this point, there are 32 countries part of the SEPA payments. In practice this means that within the countries that are a part of the European Monetary Union, cross-border payments can be done with national terms and conditions. IBAN account numbers and SWIFT codes are the most visible sign of this.

While working in Nordea Bank Finland plc. as an intern - More specifically in a corporate branch - a few main issues have always been present at work and of main concern: knowing the customer and its actual business; identifying the person representing the corporate customer and the beneficial owners; and legal reporting obligation to the authorities when recognizing unclear business transactions and activities – with the goal of identifying possible money laundering cases.

When I started working at Nordea, in my everyday work I tried to look for possible thesis topics related to international business. I wanted the topic to be interesting and related to current issues in today's world – more specifically issues facing the financial institutions. This is when the topic idea of money laundering and customer due diligence came up. While it's strongly bound to legal issues and theory is based on what is said in the law books, the real world is connected to financial institutions that are used in the money laundering process. This makes it very important to investigate the topic and find out how the financial service providers are used in the money laundering process.

## 1.2 Objective

The goal of the thesis is to investigate the current state and relationship between the parties bound and subject to the law on prevention of money laundering:



FIGURE 1. Applicable parties

1. Legal obligation: How the Finnish Act obliges specific parties on customer due diligence procedures and reporting suspicious business activity.
2. Party subject to the reporting obligation: How Nordea Bank Finland plc. is executing proper measures in “knowing your customer” principle – aim on preventing money laundering.
3. Customer: How a customer needing the financial services experience customer due diligence in real life.

The emphasis is on how customer due diligence is working in practice: identification of potential, risky customers and businesses, which services/products are used in the money laundering process, what is the connection between them and how a financial institution (Nordea) can make it more efficient to identify unclear businesses and transactions.

### **1.3 Methodology**

The thesis is conducted with qualitative research methods. The theory is based on the legal obligations (The Finnish Act on prevention of money laundering 503/2008), and other literature search. The literature search will be done through online legislation database and other online sources, but also through article search for example in public libraries.

In order to gain knowledge about the current state of the commissioner's customer due diligence procedure, a customer survey will be executed. The customer survey is sent to new corporate customers who have established a customer relationship in Nordea corporate branch Tampere (Nordea Bank Finland plc.) during the summer 2013. The purpose of this survey is to gain feedback on how the customers have experienced the tightening obligations for the parties subject to the reporting obligation to know their customers more thoroughly.

Another survey is conducted in the Nordea corporate branch to gain knowledge about how the employees of Nordea corporate branch have experienced the meetings with new potential customers: What have been the challenges in customer due diligence, what kind of questions have raised irritation among customers, what questions have customers more eagerly avoided.

## 2 THE COMMISSIONER

### 2.1 Nordea Group

Nordea Group is the biggest financial institution in the Northern Europe – having a market capitalization about EUR 36bn and total assets EUR 626bn<sup>1</sup>. The Chief Executive Officer is Christian Clausen and the Chairman of the Board is Björn Wahlroos. See table 1 for the top five shareowners of Nordea Group. (Nordea, 2013.)

TABLE 1. Top 5 shareowners (Nordea, 2013)

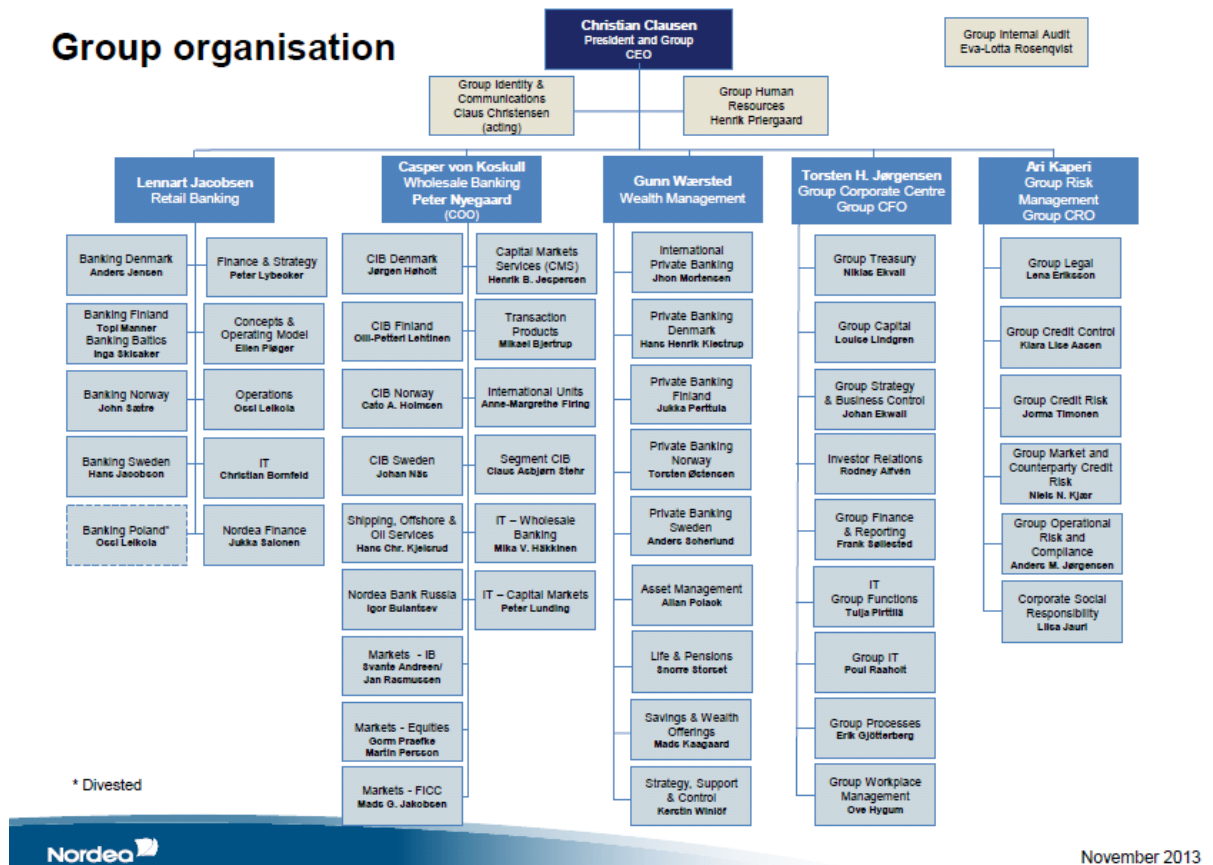
Owner	Holding
1. Sampo plc.	21.4 %
2. Nordea Fonden	3.9 %
3. Swedbank Robur Funds	3.3 %
4. Alecta	2.0 %
5. Norwegian Petroleum Fund	1.9 %

Nordea is operating in the following countries: Finland, Sweden, Norway, Denmark, Estonia, Latvia, Lithuania, Russia and Poland – covering the Northern Europe. Nordea is also present in the following countries: Luxembourg, United States, United Kingdom, Singapore, and Germany. Nordea is listed “on the NASDAQ OMX Nordic Exchange in Stockholm, Helsinki and Copenhagen”. Nordea Group has approximately 11 million customers in the Nordic region and about 30,000 employees. (Nordea, 2013.)

Nordea Group’s organization is divided into five sections: Retail banking, Wholesale Banking, Wealth Management, Group Corporate Centre, and Group Risk Management. In the next page is the Group’s official organization chart. See figure 2.

<sup>1</sup> For detailed key ratios visit:  
<http://www.nordea.com/About+Nordea/Nordea+overview/Facts+and+figures/1081354.html>





November 2013

FIGURE 2. Organization chart (About Nordea - Nordea, 2013)

## 2.2 Nordea Bank Finland plc.

Nordea Bank Finland plc. is a subsidiary of Nordea Group. Nordea Bank Finland plc. has about 128,000 corporate customers and 2.5 million household customers. Branches are in 235 locations (2012). The average number of employees in Nordea Bank Finland was in 2012 7,312 (FTEs). See table 2 for Nordea Bank Finland's ratings in 2012. (Annual Report 2012 – Nordea.)

TABLE 2. Nordea Bank Finland plc. ratings (Annual Report 2012, Nordea)

Moody's Investors Service	Aa2
Standard & Poor's	AA –
Fitch	AA –
DBRS	AA

Nordea Bank Finland plc. offers financial services and products concerning daily banking activities: Account and payment services, debit and credit cards, internet and mobile services; housing and other loans, investment services – to name a few.

The commissioner for this final thesis is a Nordea corporate branch located in Kauppakatu 4, Tampere. The branch is only for corporate customers and altogether there are about 70 employees in the branch and both small and medium sized companies and large companies are included. Nordea corporate branch's market share in Tampere is approximately 40% (about 10 000 customers). (Turunen, J. 2013.)

### **3 DEFINITION OF MONEY LAUNDERING**

#### **3.1 Origin of the term**

Money laundering is a term used to describe the process of disguising the origin of illegally obtained funds and the criminal's identity. The origin of the term 'money laundering' dates back to the 1920s and 1930s, even though the term itself was used decades later. The mafia in the United States used laundromats as a shelter for their illegal businesses. The illegal origin of funds was concealed and disguised as legal business revenues with the help of these laundromats; false bookkeeping was a tool in the process. (Heikinheimo, 1999.)

#### **3.2 Money laundering**

It was only until 1994 when money laundering was criminalized in Finland as a separate criminal activity (National Bureau of Investigation) (Keskusrikospoliisi). Before an act can be categorized as money laundering, a preliminary crime must have taken place – a crime where the funds to be washed are originating. The Finnish Criminal Code (39/1889, Chapter 32) categorizes money laundering into five categories based on the seriousness and attributes of the offense: Money laundering, aggravated money laundering, conspiracy for the commission of aggravated money laundering, negligent money laundering, and money laundering violation.

In its basic form The Criminal Code defines money laundering as following (39/1889, Chapter 32, Section 6):

- 1) A person who receives, uses, converts, conveys, transfers or transmits or possesses property acquired through an offence, the proceeds of crime or property replacing such property in order to obtain benefit for himself or herself or for another or to conceal or obliterate the illegal origin of such proceeds or property or in order to assist the offender in evading the legal consequences of the offense or
- 2) A person who conceals or obliterates the true nature, origin, location or disposition of, or rights to, property acquired through an offense, the proceeds of an offense or property replacing such property or assists another

in such concealment or obliteration, shall be sentenced for money laundering to a fine or to imprisonment for at most two years – attempt is punishable. (Criminal Code 39/1889.)

### **3.3 Aggravated money laundering**

A more serious crime is called ‘aggravated money laundering’. According to the Criminal Code (39/1889, chapter 32, section 7), money laundering is defined as ‘aggravated’ when the value of the property is considerably high, or when the money laundering actions have been intentional. The sentence for aggravated money laundering can be imprisonment between four months up to six years. (Criminal Code 39/1889.)

### **3.4 Conspiracy for the commission of aggravated money laundering**

In Criminal Code (39/1889, chapter 32, section 8) conspiracy for the commission of aggravated money laundering is described as following:

A person who agrees with another on the commission of aggravated money laundering directed at the proceeds of the giving of a bribe, the acceptance of a bribe, or aggravated tax fraud or aggravated subsidy fraud directed at the tax referred to in chapter 29, section 9, subsection 1(2), or at property replacing such proceeds, shall be sentenced for conspiracy for the commission of aggravated money laundering to a fine or to imprisonment for at most one year. (Criminal Code 39/1889)

Money laundering as a criminal activity can also be used in situations where the legal origin of the funds is to be disguised. An example of this would be tax fraud (mentioned earlier) or terrorist financing. The purpose in this case is the concealment of the illegal application of the funds rather than the origin. (Huhtamäki, 2000.)

### **3.5 Negligent money laundering**

The fourth type of money laundering is called negligent money laundering. According to the Criminal Code (39/1889, chapter 32, section 9) negligent money laundering is defined as: “A person who through gross negligence undertakes the actions referred to

in section 6 (in the previous page) shall be sentenced for negligent money laundering to a fine or to imprisonment for at most two years”.

This negligence might refer to a situation where a person receiving illegally obtained funds or other property has not made appropriate measures before accepting property – for example without any suspicion accepted property from known/unknown or otherwise unclear origin and transfers them forward.

### **3.6 Money laundering violation**

The most minor degree of money laundering is called ‘money laundering violation’. In such a case, the value laundered or other relevant circumstances are considered to be of low value or petit, and the sentence is a fine (Criminal Code 39/1889, chapter 32, section 10).

## 4 PREVENTION OF MONEY LAUNDERING

### 4.1 Introduction to legal obligations

The Finnish Act on Detecting and Preventing Money Laundering and Terrorist Financing (503/2008) is defining the rules, obligations, and investigation methods for the parties involved in fighting against money laundering. The Finnish Financial Supervisory Authority (Finanssivalvonta) is the official body that monitors that the applicable parties are following the rules and guidelines assessed by the act.

According to the Financial Supervisory Authority, customer due diligence is the main factor in the act on prevention of money laundering (Financial Supervisory Authority, 2010). This means that parties that are bound by the law, should know their customers, beneficiaries, owners, company structures, type of businesses – and when detecting suspicious transactions report to the authorities.

Figure 3 represents the interrelation between the party subject to the reporting obligation and the legal bodies (Financial Supervisory Authority, 2010):

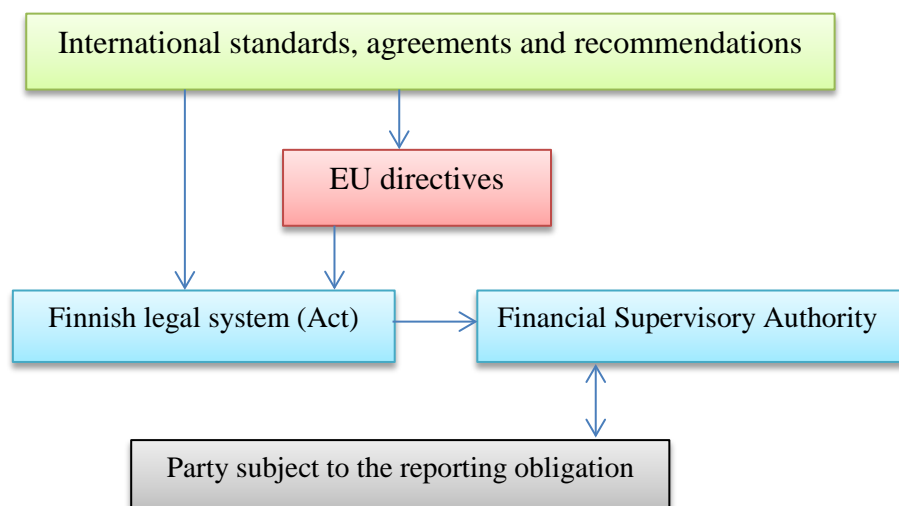


FIGURE 3. Relationship chart

#### **4.1.1 Parties subject to reporting obligation**

In the Act on Detecting and Preventing Money Laundering and Terrorist Financing (503/2008) the following parties are involved and obliged to report any suspicious and unusual business activity (Chapter 1, Section 2):

1. Credit institution and branches of foreign credit institutions (121/2007)
2. Investment firms and branches of foreign investment firms (747/2012)
3. Management companies, custodians and branches of foreign management companies (48/1999)
4. The Central Securities Depository and account operators (749/2012)
5. Pawnshops (1353/1992)
6. Insurance companies (Insurance Companies Act 1062/1972) and pension insurance companies (Act on Pension Insurance Companies 354/1997)
7. Insurance association (Insurance Associations Act 1250/1987)
8. Branches of foreign insurance companies (Act on Foreign Insurance Companies 398/1995)
9. Insurance intermediaries (Act on Insurance Mediation 570/2005)
10. Gaming operators (Lotteries Act 1047/2001)
11. Corporations running gaming activities
12. Real estate businesses and apartment rental agencies (Act on Real Estate Businesses and Apartment Rental Agencies 1075/2000)
13. Auditors (Auditing Act 459/2007)
14. Chartered public finance auditors / Chartered public finance auditing corporations (Act on Chartered Public Finance Auditors 467/1999)
15. Businesses or professions providing tax advice
16. Payment institutions (Act on Payment Institutions 297/2010)
17. Branches of foreign payment institutions (Act on the Activities of a Foreign Payment Institution in Finland 298/2010)
18. Businesses or professions performing external accounting functions
19. Businesses or professions dealing in goods; payments are made in cash of EUR 15,000 or more (single or multiple linked transactions)
20. Service providers (trust and company service providers)

## 21. Advocates and their assistants (Advocates Act 496/1958)

- \*Buying, selling, planning or execution of real property and business entities
- \*Managing of client money, securities or other assets
- \*Opening or management of bank, savings or securities account
- \*Organization of contributions for the creation, operation or management of companies
- \*Creation, operation or management of foundations, companies or similar corporations

22. Foreign credit institutions, investment firms, management companies, insurance companies, and payment institutions' representative operating in Finland without a branch (907/2011)

## 4.2 Customer Due Diligence

Customer due diligence is one of the most important areas in detection and prevention of money laundering in a financial institution. According to the Act on Detecting and Preventing Money Laundering and Terrorist Financing (503/2008, chapter 2, section 6, subsection 2): “If parties subject to the reporting obligation cannot carry out the measures laid down for customer due diligence, they may not establish customer relationships or carry out transactions”. The law concerning the matter is very self-explanatory; the phrase “...*may not establish customer relationships or carry out transactions*” is using a strict prohibition instead of phrases such as “should not” or “would be better if not”. If customer due diligence is not fulfilled and a customer relationship is opened or a transaction executed, then it is clearly a violation of the Act.

Risk-based assessment is a widely used phrase in prevention of money laundering. The Act on Detecting and Preventing Money Laundering and Terrorist Financing (503/2008, chapter 2, section 6, subsection 3) states:

Parties subject to the reporting obligation shall have in place such risk management procedures related to money laundering and terrorist financing that are commensurate with the nature and size of their business. When assessing the risks of money laundering and terrorist financing, parties subject to the reporting obligation shall take account of the risks of money laundering and terrorist financing that are related to their sector,



their products, their services, technological development, their customers and the customers' business and transactions.

When relating the previous definition of risk-based assessment to Nordea Bank Finland plc. and the financial sector, it is clear that the company should put major effort on this matter due to their high position.

There are three major areas of risks related to money laundering and terrorist financing facing the financial sector (The FATF Recommendations, 2012): Customer risk; geographical risk (especially countries with sanctions, embargos, or known to be subject to corruption and other criminal activity etc.); product/service risk in relation to the party subject to reporting obligation. Obviously, those risks do not imply the consequences should money laundering occur, but areas that should be considered as a part of money laundering.

#### **4.2.1 Identifying and verifying the customer**

The first step in customer due diligence is to identify and verify the customer. According to the Act (503/2008, Chapter 2, Section 7) customer identification and verification must be done when:

- \*Opening customer relationships
- \*Single or multiple linked transactions equals to or exceeds EUR 15,000
- \*Connected to casino activities
- \*Suspicious transactions
- \*Reliability doubts concerning the previous identification data
- \*Gaming activities when an amount of EUR 3,000 or more is involved in the stake
- \*Customer using representatives
- \*Before the customers have control over the assets or other property involved in a transaction or before the transaction has been concluded
- \*Cash payments over EUR 1,000 (Payer Information Regulation)

The Financial Supervisory Authority states in Standard 2.4, that the identification and verification must be done from "a reliable and independent source" – The Finnish authority. Documents that are recognized as valid proof of identification are: Driving license, passport, identification card, alien's passport and refugee travel documents, SII (Kela) card (with photo), foreign national passport, ID card acceptable as travel docu-

ment. However, a party subject to the reporting obligation shall decide itself which documents it accepts as valid identification proof. (Standard 2.4, Section 61.)

Verifying the identity of a legal person (a company), updated information from the Trade Register and other source is required (Financial Supervisory Authority, Standard 2.4, section 65). This information contains information about the current state of the company such as: owners, management, company structure etc.

#### **4.2.2 Identifying the beneficial owner**

A beneficial owner is usually associated with the owner(s) of a company or a member of a private person's estate. According to the Act (503/2008), beneficial owners shall also be identified, excluding a few exceptions listed here:

(2) a) A company or corporation whose securities are admitted to public trading referred to in the Securities Markets Act (495/1989) or to similar trading in another EEA State.

b) Also, the beneficial owner does not have to be identified if the customer is a company or corporation whose securities are admitted to trading corresponding to public trading in a State other than an EEA State, or if the company or corporation is subject to disclosure requirements which are similar to the disclosure requirements laid down in Directive 2004/39/EC of the European Parliament and of the Council on markets in financial instruments, amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC, hereafter the Markets in Financial Instruments Directive.

(3) Beneficial owners of pooled accounts held by advocates or other bodies providing legal services in Finland or another EEA State, provided that the information on the identity of the beneficial owners is available, on request, to credit institutions.

(4) Beneficial owners of pooled accounts held by advocates or other bodies providing legal services in a State other than an EEA State, provided that:

a) The information on the identity of the beneficial owners is available, on request, to credit institutions; and

b) Advocates or other bodies providing legal services are subject to obligations equivalent to those laid down in this Act and are supervised for compliance with these obligations.

(5) Beneficial owners of pooled accounts that are related to the duties of an attorney or to such duties that are carried out by advocates or other bodies providing legal services and that do not fall within the scope of application of this Act. (503/2008, Chapter 2, Section 8.)

### **4.2.3 Obtaining information and on-going monitoring**

Monitoring as a part of proper customer due diligence is essential in terms of recognizing unusual and suspicious transactions based on information gained when establishing a customer relationship. Monitoring is mainly based on the nature of the business and how the customer is intending to use the services/products (503/2008, Chapter 2, Section 9). In order to effectively execute monitoring, obtaining information on the customer is essential – this is the source where future monitoring and assessment of potential unusual activity is based on. Risk-based assessment focuses more on product/services and businesses that are considered to possess risk.

Other obligations laid down in the Act (503/2008) are:

Parties subject to the reporting obligation shall arrange monitoring that is adequate in view of the nature, extent and risks of the customers' transactions in order to ensure that the transactions being conducted are consistent with the parties' experience or knowledge of the customers and their business.

Parties subject to the reporting obligation shall pay particular attention to transactions which are unusual in respect of their structure or extent or the size or office of the parties subject to the reporting obligation. The same also applies if transactions have no apparent economic purpose or if they are inconsistent with the parties' experience or knowledge of the customers. If necessary, measures shall be taken to establish the source of funds that are involved in a transaction. (503/2008, Chapter 2, Section 9.)

Section 73 of the Standard 2.4, obliges the supervised entities to obtain also the following information in order to fulfill customer due diligence: "Information regarding the customer's behavior in relation to transactions, products and services needed, and the nature and extent of the customer's business; the company structure, beneficial owners, representatives, financial status and source for the funds".

#### 4.2.4 Data keeping

Data keeping is an integral part of customer due diligence. Since knowing the customer is an on-going process, previously acquired data must be available in order to evaluate the current state of the relationship: Are there any changes in the behavior, transactions, beneficial owners etc. Table 3 represents the information that should be kept safe five years after the end of the customer relationship according to the customer due diligence (503/2008, chapter 2, section 10, subsections 2 – 3):

TABLE 3. Information to be kept safe (Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008)

<b>Customer/Representative/Beneficial owner</b>	Name
	Date of birth
	Personal identity code
<b>Legal person</b>	Full name
	Registration number
	Registration date
	Authority
<b>Board of directors/Decision-making body</b>	Full name
	Date of birth
	Citizenship
<b>Type of business</b>	
<b>Identification document</b>	Name of the document
	Number of the document
	Issuing authority
	A copy of the document
<b>Customer not present</b>	Information on the procedure and sources for identification
<b>Customer's transactions</b>	Nature and extent of the business
	Financial status
	Grounds for the use of transactions/service
	Origin of the funds
<b>Foreigner</b>	Citizenship
	Travel document with the previously listed data

Obviously data keeping's major purpose is to provide the authorities a data base to support their investigation should a suspicion arise.

#### 4.2.5 Simplified customer due diligence

Risk-based assessment provides tools to recognize exceptions in customer due diligence. Based on the risk, customer due diligence can be divided into three categories: Simplified customer due diligence, customer due diligence, and enhanced customer due diligence (Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008).

In simplified customer due diligence after assessing the risk concerning the customer, product, service or transaction (503/2008, chapter 2, section 12), the process of identification/verification of the customer/beneficial owner; obtaining information; data keeping can be ignored. This is the case only with the following parties (Section 13 & 14):

\*Finnish authority or: municipality, SII, Bank of Finland (Standard 2.4, Section 99)

\*Credit, financial, payment institution, investment firm, management or insurance company that is duly authorized in Finland or another EEA State

\*A credit institution, financial institution, investment firm, management company or insurance company duly authorized in a State other than an EEA State that is subject to the obligations equivalent to those laid down in this Act and is supervised for compliance with these obligations; or

\*A branch located in an EEA State of a credit institution, financial institution, investment firm, management company or insurance company duly authorized in a State other than an EEA State.

\*Customer is a company or corporation whose securities are admitted to public trading under the Securities Markets Act or to similar trading in another EEA State, or if the customer is a company or corporation whose securities are admitted to trading corresponding to public trading in a State other than an EEA State and the company or corporation is subject to disclosure requirements which are similar to the disclosure requirements laid down in the Markets in Financial Instruments Directive. (503/2008, chapter 2, section 13-14.)

#### 4.2.6 Enhanced customer due diligence

Enhanced customer due diligence – as the name indicates – is connected to customers and products/services/transactions possessing a higher risk of money laundering. In

such a case, more detailed information should be obtained from the customer. According to the Act on Detecting and Preventing Money Laundering and Terrorist Financing (503/2008), the following cases require enhanced customer due diligence:

1. Non-face-to-face identification (503/2008, chapter 2, section 18)

Not always can a customer be physically present in a negotiation and for this reason it is not reasonable to withdraw from a transaction. However, this requires more careful verification process in order to prevent money laundering and other malpractice and the following obligation is laid down in the Act:

1. Verify the customer's identity on the basis of additional documents, data or information obtained from a reliable source.
2. Ensure that the payment of the operations is made from the credit institution's account or to the account that was opened earlier in the customer's name.
3. Verify the customer's identity by means of an identification device or qualified certificate referred to in the Act on Strong Electronic Identification and Electronic Signatures (617/2009) or by other means of electronic identification that ensures information security and is verifiable. (503/2008, chapter 2, section 18, subsections 1-3.)

Especially section 3 – more commonly known as a bank's net bank profile – is constantly getting more users and recognition as an identification/verification method because of its high security standards.

2. Correspondent banking relationships (503/2008, chapter 2, section 18)

All banks around the world need corresponding banking relationships in order to transfer funds internationally. Enhanced customer due diligence is needed because customers abroad are not identified and verified by the local bank but by the corresponding bank. The following obligation concerning correspondent banking relationships is laid down in the Act (503/2008):

- 1) If a credit institution concludes a contract on the handling of payments and other assignments (correspondent banking relationship) with a credit institution located in a country outside the EEA, the credit institution shall

obtain sufficient information about the respondent institution before concluding the contract.

2) The credit institution shall assess the respondent credit institution's reputation, the quality of supervision it performs and its anti-money laundering and anti-terrorist financing measures. The senior management of the credit institution shall give its approval for establishing a correspondent banking relationship. The contract shall explicitly lay out the customer due diligence obligations to be fulfilled.

3) If an investment firm, payment institution, management company or insurance company concludes a contract on an arrangement similar to that in subsection 1, parties subject to the reporting obligation shall observe the provisions of this section. (503/2008, chapter 2, section 19.)

### 3. Politically exposed persons (503/2008, chapter 2, section 20)

Politically exposed persons require enhanced customer due diligence due to their participation in politics that has the possibility of exposing to corruption and bribery. Section 20 in the Act lays down the following:

1) Parties subject to the reporting obligation shall have appropriate risk-based procedures to determine whether the customer is holding, or has held, an important public position in another State (politically exposed person).

2) If the customer is or has been a politically exposed person or a family member, or a person known to be a close associate, of such a person:

(1) The senior management of the parties subject to the reporting obligation shall give its approval for establishing a customer relationship with such a person;

(2) Parties subject to the reporting obligation shall establish the source of wealth and funds that are involved in the customer relationship or transaction; and

(3) Parties subject to the reporting obligation shall conduct enhanced ongoing monitoring of the customer relationship.

3) A person is no longer considered a politically exposed person when he or she has not held an important public position for at least one year.

### 4. Shell banks

According to the Financial Supervisory Authority, there should be no business relationship between a party subject to reporting obligation and a shell bank due to the *exceptionally* high risk of money laundering and terrorist financing. The Financial Superviso-

ry Authority has set this to be binding for all the supervised entities. (Financial Supervisory Authority, Standard 2.4, Section 91 and 92.)

The Standard 2.4 identifies a shell bank with the following attributes:

- \*Authorized by a state known as a “tax haven”
- \*No financial activities in the state where authorized
- \*Not present in any state
- \*No public supervision
- \*Unknown owners and beneficial owners
- \*Unknown information on financial position and activities

According to the Financial Supervisory Authority, when assessing appropriate customer due diligence method the party should use enhanced customer due diligence also in other cases than listed in the Act – should a situation so demand – but no exceptions are allowed when dealing with simplified customer due diligence (Standard 2.4. p.18). An example of this would be a connection with a state having poor measures on anti-money laundering procedures (503/2008, Chapter 2, Section 17).

### **4.3 Reporting**

The reporting obligation concerning the parties becomes topical when the monitoring process reveals suspicion concerning the true nature of a transaction or when the actual nature of the business is debatable. The reporting obligation binds the parties to report any suspicious activity regardless of whether any evidence concerning legal offence is available or not. The National Bureau of Investigation’s task is to initially investigate the true nature behind a certain transaction or business. The Act on Prevention of Money Laundering and Terrorist Financing (503/2008) obligates the parties to report to the Financial Intelligence Unit (503/2008, chapter 3, section 23, subsection 1).

Enhanced reporting obligation becomes topical when the customer has connections to countries that don’t meet the minimum requirements in prevention of money laundering and terrorist financing (503/2008, Chapter 3, Section 24). The following criteria are listed in Section 24:



-The customer doesn't provide them (parties subject to reporting obligation) with an account they have requested in order to fulfill the obligation to obtain information

-Parties consider the account to be unreliable

-No sufficient information is received regarding the grounds for the transaction and on the origin of the assets

-The legal person cannot be identified

-The beneficial owner or the representative cannot be identified or established in a reliable manner

#### **4.3.1 Secrecy obligation and derogations concerning the secrecy obligation**

Banking secrecy is a strict obligation for the financial sector. In simplicity, it protects the customers' and their financial data from external parties. Banking secrecy is one of the major issues concerning international money laundering and offshore companies; a reason why tax havens are popular is the strict banking secrecy that makes it highly difficult for the authorities to gain information about the clients.

In Finland this is not the case – withdrawing information from the authorities. The reporting obligation obliges the parties to report any suspicious transactions, though they would normally be under the protection of banking secrecy (503/2008, chapter 3, section 25). The Act only allows this with the purpose of detecting and preventing possible money laundering (Subsection 5).

#### **4.4 Suspending and refusing to conduct a transaction**

If the on-going monitoring has revealed suspicious activity or suspicion rose in the beginning of the customer relationship the supervised entities have the legal permission to suspend and refuse to execute a transaction (503/2008, chapter 2, section 26). Even a suspicion justifies this. A suspension order can also come from the Financial Intelligence Unit (Rahanpesunselvittelykeskus) and is valid up to five working days.

## **4.5 Training and protecting employees**

As it is already mentioned, the Act 503/2008 defines the law on which anti-money laundering procedures are based on and the Financial Supervisory Authority is monitoring that parties subject to the reporting obligation is following the Act – through the Code of Conduct (Standard 2.4) – it is the supervised entity's responsibility to develop internal risk management procedures to ensure that the requirements concerning customer due diligence are met. This includes a proper training of the employees, protection of the employees who report a suspicious transactions, and internal instructions concerning obtaining information and reporting obligation (503/2008, chapter 6, section 34).

## **4.6 Failure in customer due diligence and reporting obligation**

Based on the seriousness of the money laundering crime, should the supervised entity fail to meet the obligations laid down in the Act, can the consequences be serious. If failing in proper anti-money laundering procedures become public information, it inevitably has an impact on the company's publicity, image and reliability. In addition to the impact on the company's image, there are also legal consequences.

### **4.6.1 Liability for damages**

Should a party subject to the reporting obligation fail in proper customer due diligence, the liability for damages is as following:

Parties subject to the reporting obligation are liable for the financial loss sustained by their customers as a result of clearing a transaction, reporting a suspicious transaction or suspending or refusing to conduct a transaction, only if the parties have failed to carry out such customer due diligence measures as can be reasonably required of them, considering the circumstances. (503/2008, Chapter 6, Section 39, Subsection 1.)

#### **4.6.2 Violation of customer due diligence**

In addition to liability for damages, there are legal consequences for failing in customer due diligence:

Anyone who deliberately or through negligence fails to fulfill the obligation to conduct customer due diligence laid down in sections 6–9 or 17–21 or the obligation to keep records of the customer due diligence data laid down in section 10 shall be sentenced for violation of customer due diligence to a fine, unless a more severe punishment for the act is provided elsewhere in the law. (503/2008, chapter 6, section 40.)

#### **4.6.3 Violation of the obligation to report money laundering**

If a party subject to the reporting obligation fails to report any suspicious activity, the violation and its consequences are described as:

Anyone who deliberately or through negligence fails to make a report under section 23 or 24, discloses such reporting in violation of the prohibition under section 25, or fails to fulfill the obligation to obtain information under section 9(3) and, therefore, does not realize the existence of the reporting obligation referred to in section 23 or 24 shall be sentenced for violation of the obligation to report money laundering to a fine. (503/2008, chapter 6, section 42.)

The act is highly aligned with The Financial Action Task Force (FATF) Recommendations that are “universally recognized as the international standard for anti-money laundering and countering the financing of terrorism (AML/CFT)” (FATF, 2013, p.7). The FATF states that:

The mandate of the FATF is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related threats to the integrity of the international financial system”. (FATF Recommendations 2013, p.7.)

Financial Supervisory Authority along with the Finnish law is setting the requirements for customer due diligence but it is the party’s obligation to set internal procedures to meet these requirements. Financial Supervisory Authority has established a code of conduct called ‘Standard 2.4 Customer Due Diligence – Prevention of Money Launder-

ing, Terrorist Financing and Market Abuse'. This Code of Conduct talks about risk management procedures with the goal of: Identifying risks related to customers, products and services; assessment of the current risk management procedures – suitability and effectiveness; link different customer groups with appropriate customer due diligence procedures and provide proper internal instructions and employee training; organizing the operations; on-going monitoring.

## 5 MONEY LAUNDERING IN PRACTICE

### 5.1 Statistics

According to Financial Intelligence Unit, preliminary crimes associated with money laundering are in Finland mainly connected to drug trafficking and financial crimes (Rahanpesurikokset oikeuskäytännössä VI, 2012). What is important to acknowledge is that not all preliminary crimes are committed in Finland but in another countries, and Finland can just be an intermediary in international money laundering.

According to the United Nations on Drugs and Crime (UNODC) 2009 report, the share of money laundering on a global scale is roughly estimated to be around 2.7% of the global GDP or about \$1.6 trillion. Of the global illegal money flows, only 1% is seized or frozen (UNODC, 2011). This reveals the ugly truth about global money laundering and how difficult it is to combat against it. The UNODC 2009 report also evaluates the percentage of criminal proceeds to be about 3.6% of the global GDP or USD 2.1 trillion in 2009.

The Annual Report 2012 – National Bureau of Investigation, Financial Intelligence Unit, states that the reporting obligation is aimed at three categories: Suspicious business activity, suspicious money transfers, and terrorist financing. Table 4 represents the amount of these reports in 2012:

TABLE 4. Types of reports - Rahanpesunselvittelykeskuksen vuosiraportti 2012 (Financial Intelligence Unit, National Bureau of Investigation)

Types of reports	Amount of reports	Amount of transactions
Suspicious business activity	2 911	9 797
Suspicious money transfer	166	43 511
Terrorist financing	9	7
<b>Total</b>	<b>3 086</b>	<b>53 315</b>

Table 5 in the next page represents the deviation of reports and transactions between the parties subject to the reporting obligation. It reveals which parties due to the reporting

obligation have had more situations that have caused a report to be filed. Notify the inconsistency between the amount of reports and amount of transactions.

TABLE 5. Parties subject to reporting obligation - Rahanpesunselvittelykeskuksen vuosiraportti 2012 (Financial Intelligence Unit, National Bureau of Investigation)

Party	Amount of reports 2012	Amount of transactions 2012
Bank	1 205	3 145
Payment institution (e.g. currency exchange)	1 016	19 275
Gaming operator	331	5900
Insurance company	221	225
Valuable goods trader	97	97
Other source of information	63	92
Other credit- and finance institution	49	24 441
Finnish authority	42	52
Finnish police authority	21	19
Lawyer/solicitor	15	25
Auditing institution	12	26
Realtor	5	5
Investment company	4	7
Accounting institution	3	5
Foreign authority	2	1
Foreign police authority	0	0
Pawnshop	0	0
Auctioneer	0	0
<b>Total</b>	<b>3 086</b>	<b>53 315</b>

Identifying suspicious transactions is a key element in detection of possible money laundering cases. Therefore it is important to acknowledge what types of transactions have raised most suspicion. Table 6 in the next page represents the type of transactions that has raised suspicion towards business activity. It is not mentioned in detail in the 'Rahanpesunselvittelykeskuksen vuosiraportti 2012' what the section 'other suspicious business activity' actually includes.

TABLE 6. Suspicious business activity - Rahanpesunselvittelykeskuksen vuosiraportti 2012 (Financial Intelligence Unit, National Bureau of Investigation)

Suspicious business activity	2012
Other suspicious business activity	2409
Account transfer	545
Cash deposit	433
Currency transfer	311
Cash withdrawal	229
Article sale	127
Fund rotation	63
Currency exchange	44
Cash transit	28
Insurance	23
<b>TOTAL</b>	<b>4212</b>

The deviation concerning the amount of funds in the transactions reported is illustrated in table 7. In roughly 95% of the transactions reported, the amount of the funds were under EUR 10 000, which can be surprising considering the amount of illicit money that is to be washed.

TABLE 7. Deviation of funds - Rahanpesunselvittelykeskuksen vuosiraportti 2012 (Financial Intelligence Unit, National Bureau of Investigation)

Amount of funds in the reports	2012
Less than 10 000€	50 829
10 000 – 35 000€	1793
35 000 – 85 000€	331
85 000 – 170 000€	147
Over 170 000€	215
<b>TOTAL</b>	<b>53 315</b>

Since money laundering is international phenomena and cross-border payments should be monitored, table 8 in the next page represents the information regarding international money transfers and their deviation according to the reports.

TABLE 8. Cross-border transactions - Rahanpesunselvittelykeskuksen vuosiraportti 2012 (Financial Intelligence Unit, National Bureau of Investigation)

<b>International transactions</b>		
	<b>Amount</b>	<b>EUR</b>
To Finland	17 310	45 116 506
From Finland	5917	53 231 521
<b>TOTAL</b>	<b>23 227</b>	<b>98 348 027</b>

The data in table 7 and 8 provides a clear picture about the state concerning the transactions. What is important to acknowledge, is the fact that these are all connected to the reports of ‘unclear business transactions’. Funds transferred to Finland include a high number of single transactions: An average of EUR 2 606 per transaction; whereas funds transferred from Finland are done in fewer number of transactions: An average of EUR 8 996. This could indicate that smurfing-technique has been used in another country and the funds are gathered together in Finland to be sent forward.

## 5.2 Three-stage process of money laundering

Money laundering methods can vary significantly since the international actions in prevention of money laundering are constantly developing; the criminals also need to develop more versatile methods. However, internationally and universally money laundering is considered to follow the following three-stage process of ‘placement, layering, and integration’ (FATF, 2013).

### 5.2.1 Placement

The most critical phase in money laundering process is called the ‘placement’. The placement phase is the most difficult part for the criminals because it includes dealing with the authorities or parties subject to reporting obligation. On the other hand, placement phase is the most critical phase in prevention of money laundering because once the funds are successfully invested in the financial system, the tracing is more difficult.



One of the methods used in the placement phase is called 'smurfing'. In this process a large amount of funds is fractioned and deposited in smaller transactions and by many people into several institutions (Rahanpesurikokset oikeuskäytännössä, 2012). This complicated method is very difficult to identify because smaller transactions does not raise suspicion as easily.

The oldest method of the placement phase is to physically transfer the money to another country. Canadian About Business Crime Solutions Inc. lists the following placement methods in their website:

- \*Loan repayment with illegal funds
- \*Using the illegal funds in gambling activities
- \*Cross-border currency smuggling
- \*Purchasing foreign currency with the illegally obtained funds

Obviously, money deposits into an account are not the only way of placing funds in the financial system. In addition to the previously mentioned foreign currency exchange, also bank cheques can be purchased, but this would require numerous transactions with smaller amounts and that could raise suspicion. Usually bank cheques are used to make a bigger payment (purchase of a car or an apartment).

The Financial Action Task Force states in their website section F.A.Q. that “At the placement stage, for example, the funds are usually processed relatively close to the under-lying activity; often, but not in every case, in the country where the funds originate” (FATF 2013).

### **5.2.2 Layering**

Since money laundering is not a single action operation, a series of stages is required to diminish origin of the funds. Depositing money into a bank account is not enough but rather the first stage. Once the funds are in the bank account or for example in a form of foreign currency, the second phase called 'layering' can be executed. The term layering describes the process since there will be multiple "layers" in disguising the source. If smurfs have deposited the money into bank accounts, the term layering would mean for

example transferring the money into other bank accounts and eventually across the borders. The funds could be invested to funds or to public shares and be eventually sold. See figure 4 for an example.

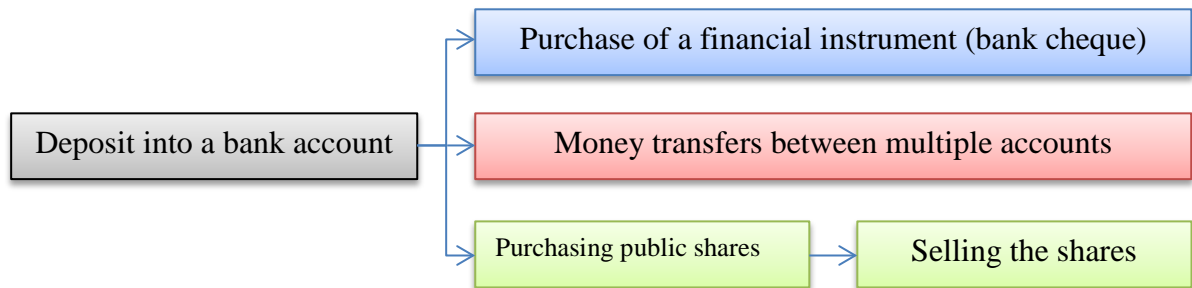


FIGURE 4. Example of layering

Concerning the layering stage, the Financial Action Task Force states that “with the layering phase, the launderer might choose an offshore financial center, a large regional business center, or a world banking center – any location that provides an adequate financial or business infrastructure” (FATF 2013). The basis for this is the strict banking secrecy within these off-shore countries – Access to customer data base can be very challenging to the authorities.

### 5.2.3 Integration

Integration is the final phase of the generally acknowledged three-stage process of money laundering. The purpose of the final stage is to return the funds to the criminal disguised as legitimate business revenue to be used for personal benefits or future investments on criminal activity.

The following figure 5 in the next page – created by OECD (The Organization for Economic Co-operation and Development) – represents the three-stage process in a simplified way (Money laundering Awareness Handbook for Tax Examiners and Tax Auditors, OECD 2009):

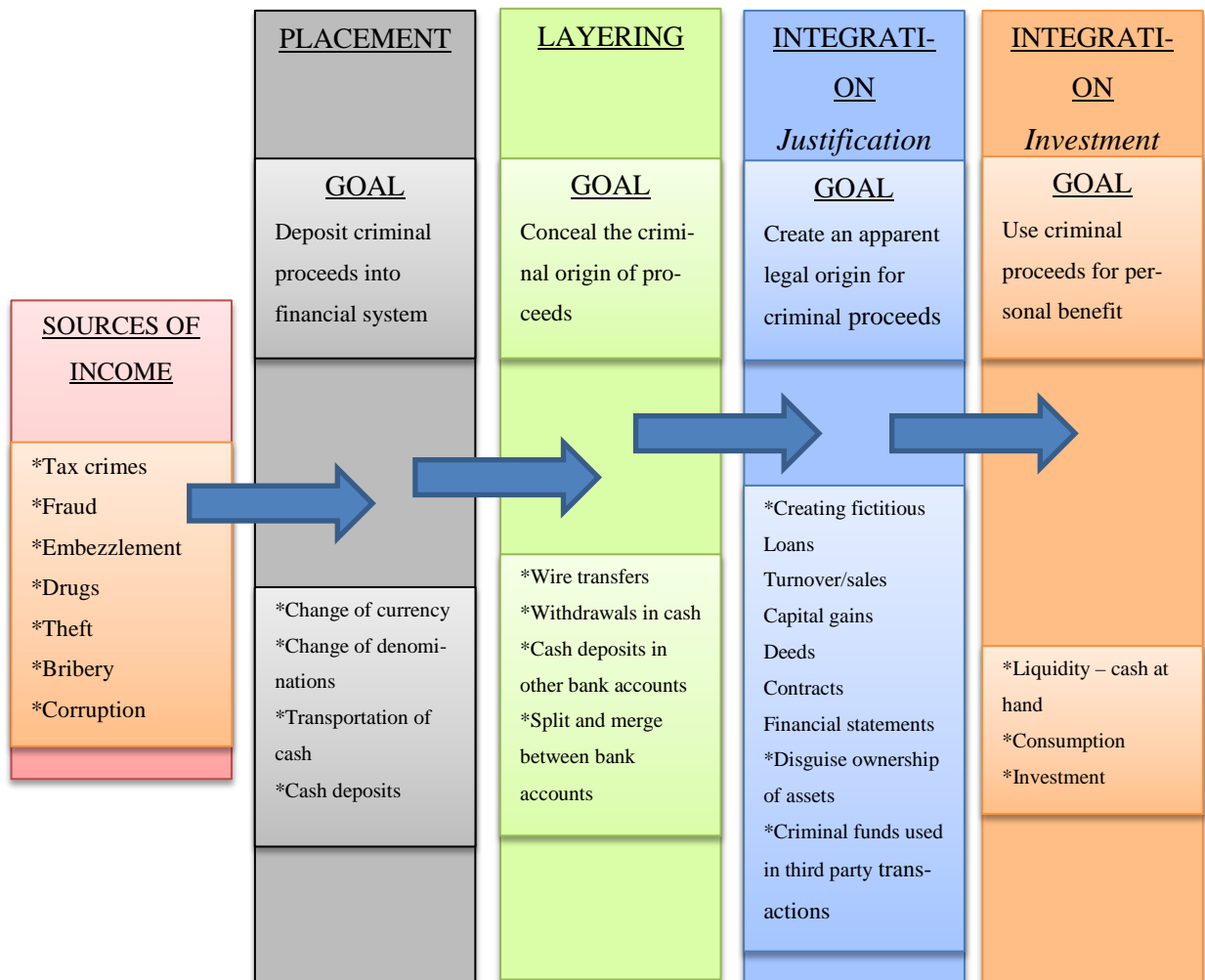


FIGURE 5. Overview of the three-stage process of money laundering (OECD, 2009, modified)

### 5.3 Unusual activity

Since the basis for the customer due diligence is built on customer identification/verification and obtaining information on the customer and its business, the follow-up is the assessment of this information with the actual activity. The Organization for Economic Co-operation and Development (OECD) has published in 2009 'Money Laundering Handbook for Tax Examiners and Tax Auditors' especially targeted to enable easier recognition of unusual transactions which is the basis for prevention of money laundering. It is important to acknowledge what are the most common types of unusual activities in order to recognize them when opening new customer relationships or executing transactions.

According to the OECD Handbook, factors that can indicate unusual activity are: unclear origin of the funds (no documentation); parties are not identified or are unclear; activity does not match with the customer profile; no economical/logical explanation. “Unusual means that a transaction differs from the norms of a certain industry or the habits of an individual, taking into account their background, normal activities or declared income” (OECD 2009, p.16).

The handbook categorizes the detection of unusual transactions into seven categories: Indicators on individuals; indicators on tax return examination and pre-audit; indicators on auditing; indicators on real estate; indicators on cash; indicators on international trade; indicators on loans; indicators on service providers (OECD, 2009). In this final thesis not all of the seven categories are covered but those relevant to the daily banking operations.

According to the FATF Recommendations (2012) the assessment of unusual activity is based on three risks: Customer risk, geographical risk (especially countries with sanctions, embargos, or known to be subject to corruption and other criminal activity etc.), product/service risk in relation to the party subject to reporting obligation.

### **5.3.1 Unusual money flows**

Since illicit funds are more commonly in the form of cash, monitoring the movement of cash and electronic money transfers is vital in prevention of money laundering. Some indicators on unusual money flows are: Depositing large amount of cash into a bank account without relevant documentation (origin of the funds) (OECD 2009, p.36); origin of the funds is located in a risk country (OECD 2009, p. 36); making large cash payments; payments to risk countries (geographical risk – FATF Recommendations 2012).

When it comes to money flows, in a transparent business the two parties in the transaction should be established and identified. This means that for example when a business is executing import or export, the money flows are not transferred to/via a third party who has nothing to do with the business – especially alarming when the money transfers are directed to irrelevant offshore companies (OECD, 2009).

Another aspect of unusual money flows in business transactions is fast-moving funds. In such situation, three or more parties are involved in a transaction and the middle-man is merely a phase whose bank account is used as a temporary shelter before the funds are transferred forward (OECD, 2009).

A basis for evaluation of unusual activity and transactions would be connected to the industry standards or customer profile – what are the basic trends and attributes of an industry/customer. As an over-exaggerated example a video rental possessing valuable denominations (EUR 100–500) or a store possessing currency not used as an official currency in the country (OECD, 2009).

Obviously, the origin of funds can reveal information that can lead to suspicion – especially funds originating from ‘black-listed countries’. Travelers rarely carry huge amount of foreign currency back to the home country, unless they have been carried or smuggled by car or other means. Suspicion would rise in any case when trying to exchange foreign currency back to own currency if the sum is huge or the origin of funds unusual. The denomination of the funds – whether foreign or not – must be also evaluated in terms of normality connected to the industry or the individual. When connecting cash with the bank (a person is depositing money into a bank account), should the customer refuse to explain the origin of the funds (with relevant documentation), the possibility of an unusual transaction should not be excluded. Another important factor related to the unknown origin is (can also be separated from) is large amount cash a customer is depositing to an account or is making such a payment (OECD, 2009).

Money transfers have been topical recently – especially cases where funds in the form of cash have been sent via special money transfer offices to high risk countries. ‘The Economist’ published an article in July 20th 2013 called ‘*African money transfers – let them remit*’ (Volume 408, Number 8845). The story of the article was that a British retail bank Barclays has decided to close bank accounts of about 250 money transfer offices. The reason for this according to the article was that the offices have not presented proper background checks of their customers. Also ‘Helsingin Sanomat’ published an article about Nordea Bank Finland plc. closing a bank account of a money transfer company who is transferring money to Somalia. In both cases (Barclays and Nordea) the explanation was to prevent money laundering and terrorist financing (Helsingin

Sanomat, 2013). Especially risky are money transfers to risk-profile countries; the following attributes should raise suspicion: country known for drug producing, inadequate money laundering procedures, high level of banking secrecy (OECD, 2009).

The OECD Handbook categorizes laundering of cash the following:

1. Converting the cash into other denominations or currencies using exchange offices, banks, the black market and through the use of cash driven businesses
2. Physical movement and transportation by car or plane using couriers, specialized value transportation companies
3. Depositing money in the banking system through the use of “straw men” (nominees), the use of cash driven businesses or the use of the “smurfing” technique
4. Creating an appearance of a legitimate origin by creating fictitious loans or fabricating cash turnover
5. Making cash purchases. (Money Laundering Awareness Handbook... OECD 2009, p.36-37.)

When it comes to cash deposits, ‘smurfing’ is a method used in money laundering. The illicit funds are deposited by many persons into many different bank accounts – as illustrated in figure 6 (the next page) – and again transferred forward nationally or internationally. The basic idea of ‘smurfing’ is to not raise any suspicion connected to large cash amounts (OECD, 2009).

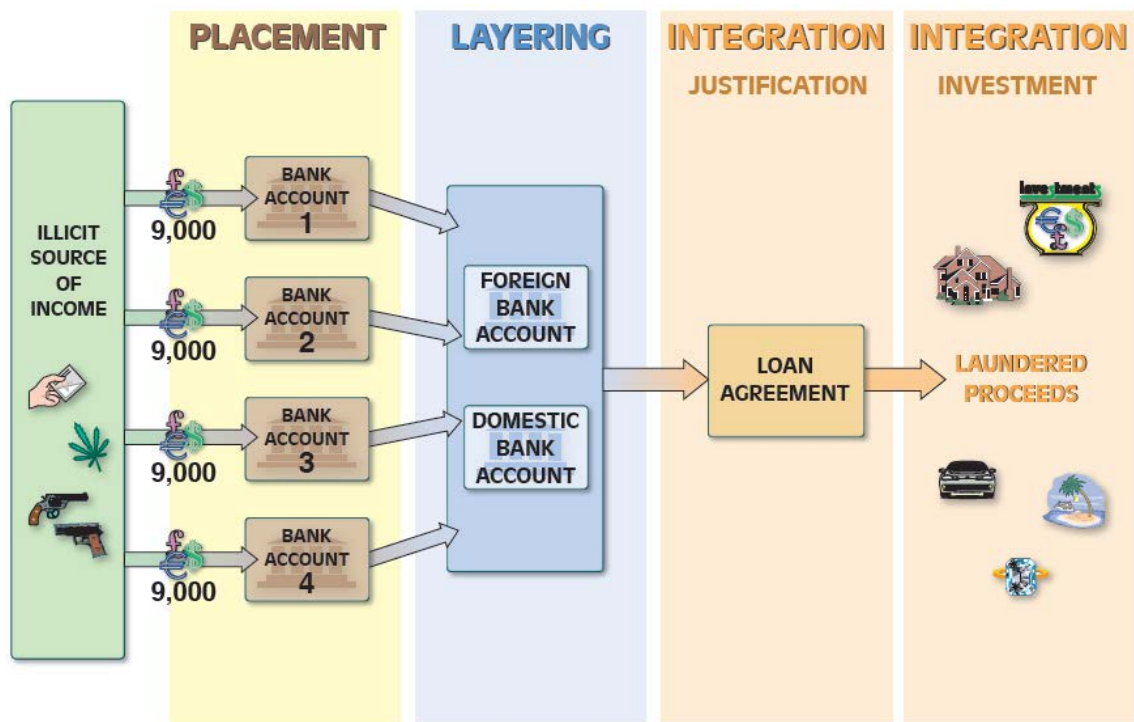


FIGURE 6. Structuring 'Smurfing' - Money Laundering Awareness Handbook (OECD, 2009, p.37)

### 5.3.2 Ownership

Non-transparent ownership should already raise suspicion about the real nature of the business. There is also the possibility of the use of offshore companies in disguising the true owners. The OECD Handbook also lists the following factors:

Ownership by relations/partners of criminals; International structure with no apparent commercial, legal or tax benefits; Purchase or sale of the companies' shares at a price far above or below estimated value; Companies/directors registered at a foreign company service provider's address. (Money Laundering Awareness Handbook...OECD 2009, p.23.)

In non-transparent ownership cases, tax havens can be used. The strict banking securities give a shelter for the owners who do not want to be identified. Figure 7 in the next page provides an example of how non-transparent ownership can be used in international money laundering.

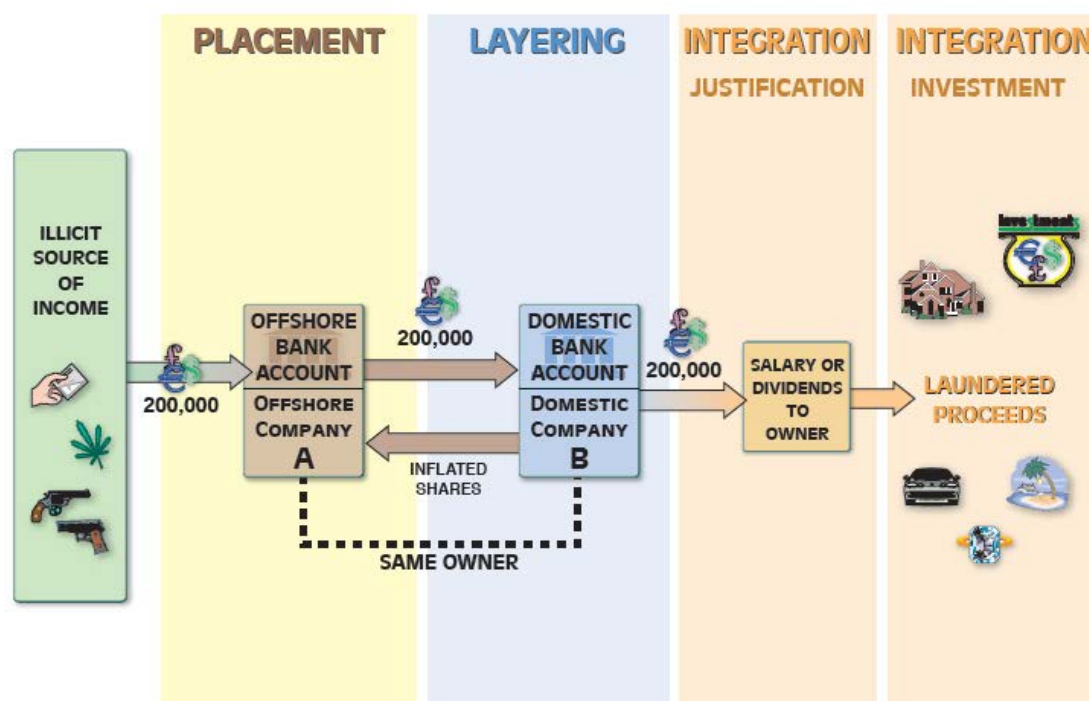


FIGURE 7. Non-transparent ownership - Money Laundering Awareness Handbook (OECD, 2009, p.25)

In Figure 7 the steps are (OECD, 2009):

1. Illicit funds are deposited into an offshore bank account owned by the criminal
2. Funds are transferred to the domestic bank account as a “purchase of shares” of a company that is also owned by the same criminal.
3. Funds transferred forward in ‘integration’

Another aspect regarding the ownership of the company is the lack of expertise. When having a business meeting with a customer and he/she indicate lack of experience or knowledge about his/her actual business, suspicion should arise. Obviously, there is the possibility that a new/young entrepreneur is overconfident about the skills and should therefore seek professional help for creating a valid business idea or is merely used as a middle-man in concealing the true owners. (OECD 2009, p.27.)

### 5.3.3 Business

The company’s actual business can reveal relevant information. For example a company is identified as a part of logistics and warehousing business but is actually providing information technology services. Another clue concerning unusual activity is a business



having transactions that are not based on any commercial activity or daily business operations (OECD 2009, p.27). The questions in such a case would be what is the ultimate purpose of this transaction? Also the following list provided by the OECD Handbook (2009, p.27) reveals some typical unusual activity found in auditing or other business situations:

- \*Transactions or agreements without relevant supporting documents
- \*Transactions with offshore companies
- \*Transaction with suspected criminals or their parties
- \*Non-transparent/non-identifiable customers, creditors or lenders
- \*Transactions with business associates or customers that share a common address
- \*Transactions identified as asset sales but assets cannot be substantiated

#### **5.3.4 International trade**

Due to the international attributes of money laundering and preliminary crimes (for example drug trafficking) companies operating on a global scale are therefore more vulnerable to international money laundering simply because payments in export and import are cross-border transactions. Bookkeepers and auditors have a better access to export/import documentation and can therefore more easily recognize unusual activity but it is also important to bank personnel whose customers in this business to acknowledge some common types of techniques.

According to the OECD Money Laundering Awareness Handbook, the following methods are commonly used in international money laundering: invoicing (under/over); different goods imported/exported than in the documents; multiple billing; non-existing delivery or fictitious invoices (OECD 2009, p.40). In table 9 can be seen examples of invoicing used in money laundering.

TABLE 9. Invoicing - Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors (OECD 2009, p.39)

	Method	Qualification	Shifting of value
<b>Import</b>	Over-invoicing	Expensive imports	In money abroad
	Under-invoicing	Lucrative imports	In goods to the homeland
<b>Export</b>	Over-invoicing	Lucrative exports	In money to the homeland
	Under-invoicing	Cheap exports	In goods abroad

The following figure 8 illustrates the process of under-invoicing in practice (OECD, 2009). This gives an example how the funds to be washed can be in the form of stolen goods. The preliminary crime in this example could be for example theft or fraud.

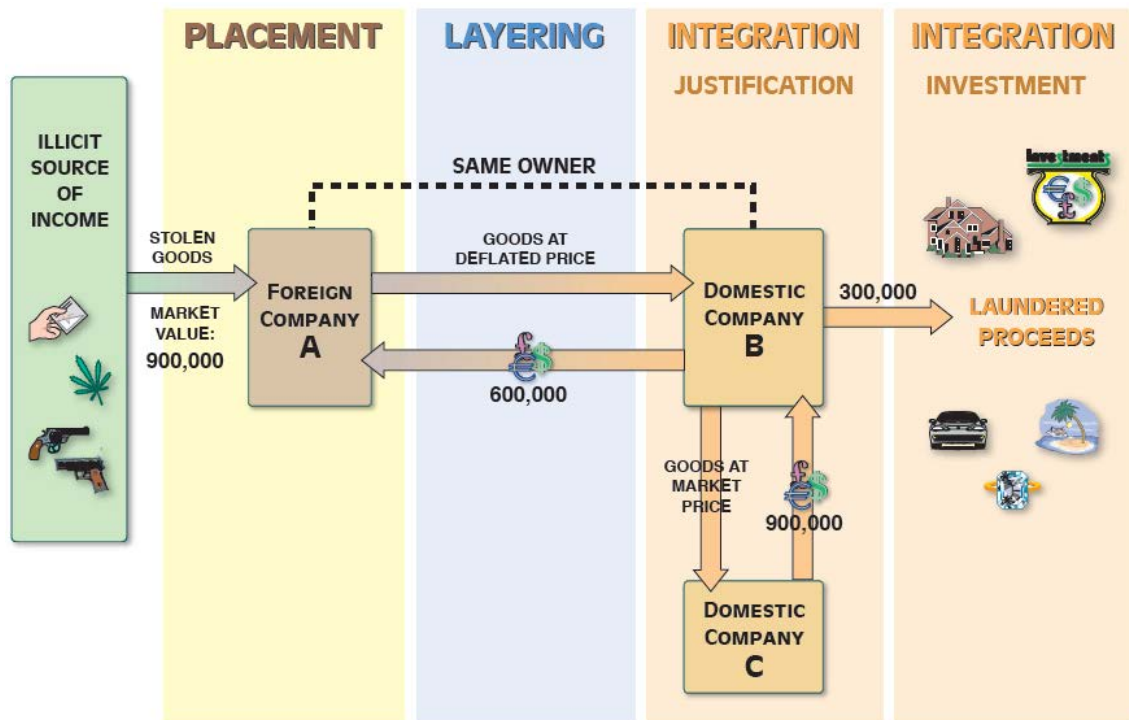


FIGURE 8. Trade-based money laundering - under-invoicing - Money Laundering Awareness Handbook (OECD, 2009, p.40)

In order to detect unusual activity in international trade, the OECD Money Laundering Awareness Handbook suggests to keep an eye on the following factors: The origin/destination of the goods; who is the buyer or supplier and what kind of business they have; transportation methods; international trade documents (description of goods); pricing (market value vs. book value); financing/payment methods. (OECD 2009, p.41.)

### 5.3.5 Service providers

Service providers in this context are companies who are offering special services to customers such as: legal services, financial advice, and trust and company services (OECD 2009, p.47). Especially trust and company services refer to a legal entity establishing a new business and arranging everything ready to be sold to a customer. In this case the buyer is receiving a company where all the paperwork is done and the company has a legitimate existence.

When connecting this context into the banking sector, a service provider can set up a bank account and other banking services before selling the company to a customer. This means that the buyer considers that he/she doesn't have to go through the customer due diligence in the bank. This is a very common situation for entrepreneurs who have lost their credit information.

### 5.3.6 Summary of unusual activity

Unusual activity and money laundering can be in many different forms and detection of them can be tricky. According to the 'Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors' (OECD, 2009), some major activities connected to different areas (for example international trade, money flow etc.) can be identified. Table 10 summarizes some of the unusual activities.

TABLE 10. Common unusual activity (Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors - OECD 2009)

Unusual possession (assets, currency etc.)	Unclear origin of funds
Unusual income	Quick movement of funds in a bank account
Unusual debt	Unusual destination
Non-transparent ownership	Unusual financing
Non-transparent customers	Offshore companies involved
Unusual money flows	Deviation from company/industry standards
No supporting documentation	

## 5.4 High-risk countries

To identify high-risk countries related to money laundering enables detecting unusual activity during monitoring – this is especially the case with international trade and cross-border money transfers. In this chapter, two reports are investigated: High-risk and non-cooperative jurisdictions – FATF Public Statement 2013; and The Basel AML Index 2013 – Basel Institute on Governance.

The term high-risk country refers to a country with at least one or more of the following attributes (OECD Handbook, 2009):

- 1) A country is known to be a producer or exporter of illegal substances or possesses a high rate of other criminal activity;
- 2) A country is lacking anti-money laundering regulations or is poorly executing proper measures;
- 3) A country has a strict banking secrecy and non-transparency

### 5.4.1 The Basel AML Index 2013

The Basel AML Index 2013 doesn't reveal countries which have the highest rate of money laundering but rather evaluates countries' vulnerability and risk to money laundering. According to the Index, the evaluation is based on the following factors<sup>2</sup>: money laundering and terrorist financing risk; corruption risk; financial transparency and standards; public transparency and accountability; political and legal risk (Basel Institute on Governance, 2013).

The world map in the next page (figure 9) reveals geographical areas that possess more risk of money laundering to be Asia, Africa, and Central and South America.

---

<sup>2</sup> See The Basel AML Index 2013 - <http://index.baselgovernance.org/index/Index.html#introduction> for the methods and grounds for the ranking

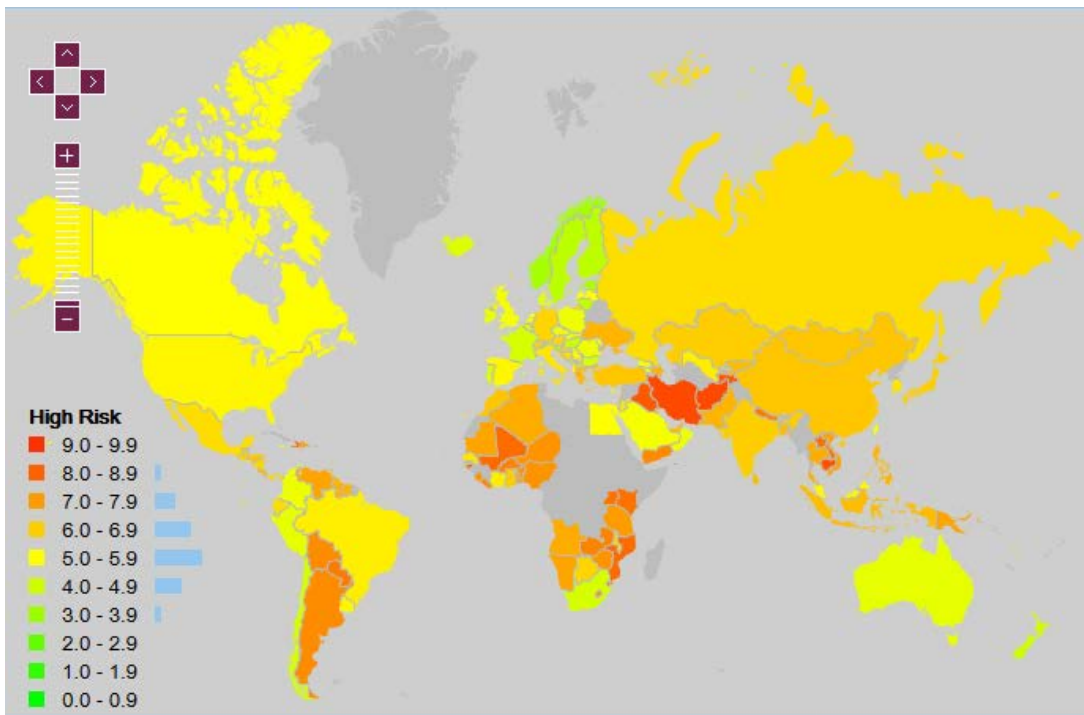


FIGURE 9: Country map (Basel Institute on Governance – 2013, <http://index.baselgovernance.org>)

The following three figures represent Basel AML Index ranking: Top 10 Global, Top 10 Europe, and Bottom 10 Global. The higher the score, the riskier the country is and vice versa. The scale is from 0 to 10.

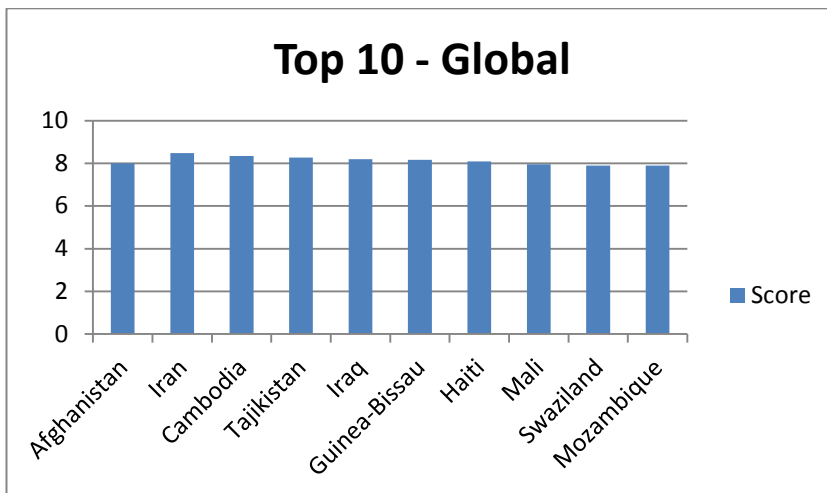


FIGURE 10. Top 10 riskiest countries (Basel Institute on Governance, 2013)

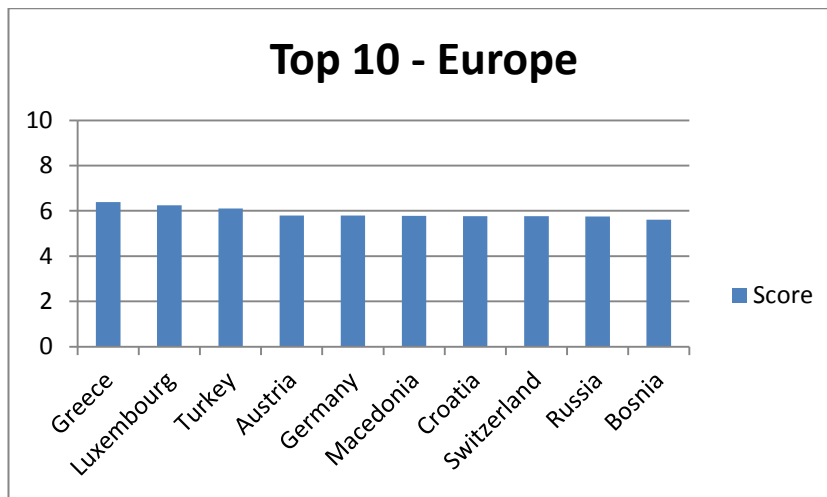


FIGURE 11. Top 10 Europe (Basel Institute on Governance, 2013)

For the whole European risk ranking, see Index 1 at the end of the thesis.

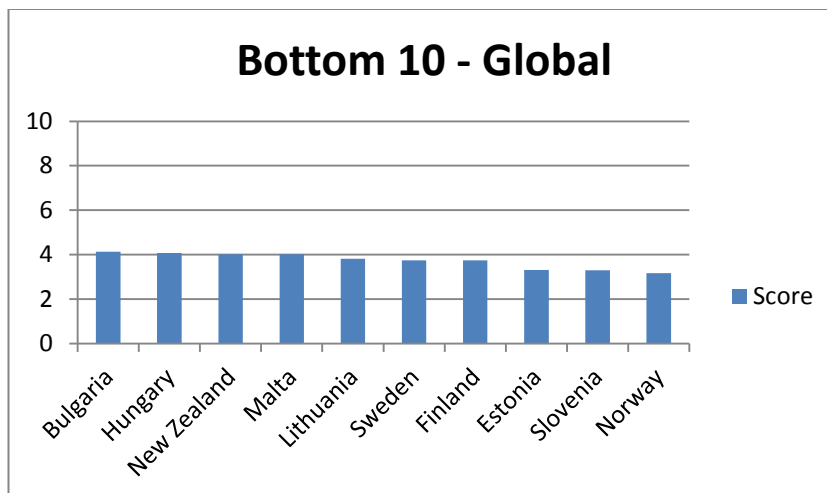


FIGURE 12. Bottom 10 Global (Basel Institute on Governance, 2013)

#### 5.4.2 FATF High-risk and non-cooperative jurisdictions

In October 2013 The Financial Action Task Force published an updated version of the list of countries that have inadequately executed proper money laundering procedures or have deficiencies in their procedures. The list is called 'High-risk and non-cooperative jurisdictions' and is divided into two categories: Countries that have deficiencies and not made enough progress (Public Statement); Countries with deficiencies but have political commitment to the problem (Improving Global AML/CFT Compliance: on-going process).

Table 11 lists countries that have inadequate measures in prevention of money laundering and have are not committed to improve anti-money laundering procedures (FATF 2013).

TABLE 11. Countries with deficiencies/no progress (Public Statement October 2013, FATF)

Iran	Myanmar
Democratic People's Republic of Korea	Pakistan
Algeria	Syria
Ecuador	Tanzania
Ethiopia	Turkey
Indonesia	Yemen
Kenya	

Table 12 represents countries that have committed to improve their anti-money laundering and counter terrorist financing procedures but still have deficiencies.

TABLE 102. Countries with deficiencies/political commitment (Improving Global AML/CFT Compliance: on-going process - October 2013, FATF)

Afghanistan	Lao DPR
Albania	Namibia
Angola	Nepal
Antigua and Barbuda	Nicaragua
Argentina	Sudan
Bangladesh	Tajikistan
Cambodia	Vietnam
Cuba	Zimbabwe
Iraq	Mongolia
Kuwait	Morocco
Kyrgyzstan	Nigeria

## 5.5 Money laundering cases in Nordea

In 2013 Nordea Group was fined SEK 30 million (around EUR 3.5 million) for negligent of proper measures in prevention of money laundering (Kauppalehti, 2013). There is no clear evidence that Nordea Group has been a middle-man in actual money launder-

ing but according to the article and the Swedish authorities, there has been a possibility for black-listed companies and private persons to use the banking services; Nordea has also been negligent for the reporting obligation.

Another case concerning money laundering is the net bank robbery where Nordea's customers' bank accounts were robbed through malwares and the funds transferred to other bank accounts in Finland and abroad (Taloussanomat, 2010). The money laundering in this case was when the 'mules' received the illegally obtained money and transferred them forward in order to conceal the origin of the funds.



## **6 CUSTOMER SURVEY – NORDEA CORPORATE BRANCH**

### **6.1 Basis for the survey**

Two customer surveys were conducted in order to gain knowledge about the current state of customer due diligence in the Nordea corporate branch Tampere. The first survey was sent to new corporate customers that had established a customer relationship at Nordea bank during the summer 2013; the other survey included employee feedback on customer due diligence in practice. As a summary, the main focus was on how customers respond to the relevantly wide information obtaining in meetings and what the employees' perceptions about customers' behaviors are. See appendix 2 for the basic information form and for highlighted sections related to the Act (503/2008); Appendices 3 and 4 include the full questionnaires.

### **6.2 Corporate customers**

The customer survey to the new customers included four multiple questions and one open question regarding the experience when opening the customer relationship with Nordea. About 100 questionnaires were sent to small and medium sized companies and received answers were 23. A 23% reply is not very satisfactory but when reviewing the answers, similarities in opinions could however be found.

In the first question, the customers were asked how they felt about the interview concerning the company information. 52% of the respondents considered the interview to be fast and smooth; 30% considered the interview to be somewhat fast and smooth while 4% did not have an opinion; 9% of the respondents considered the interview to be slightly complex and remaining 4% felt that the interview was very complex and time consuming. See figure 13 in the next page.

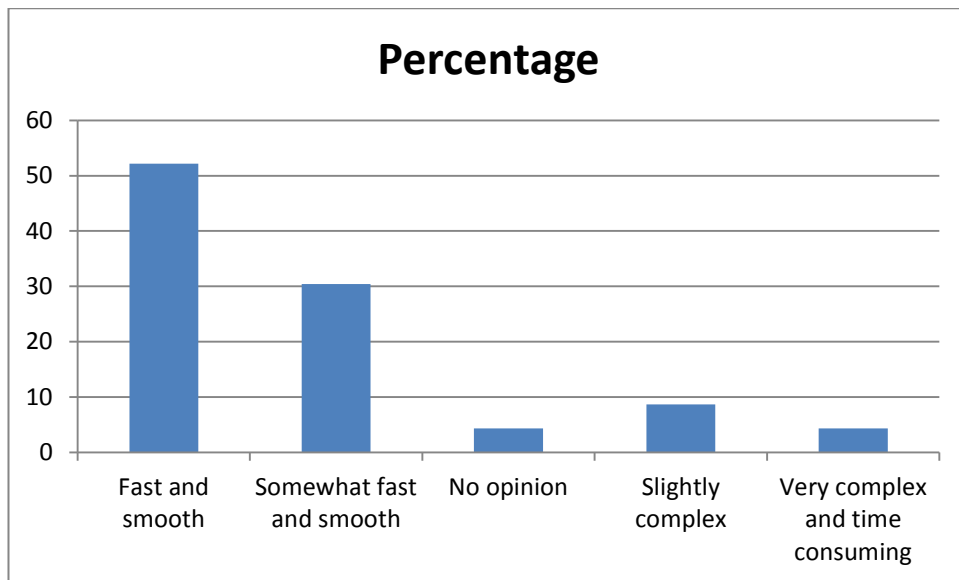


FIGURE 13. How was the interviewing when opening a customer relationship?

The second question was about what kind of impact the interview had on the customer's image about Nordea. 35% of the respondents answered the interview had a positive impact on the image; 9% replied the interview had some positive impact; 30% of the respondents were not affected by the interview; 22% of the respondents had somewhat negative impact on the image and the remaining 4% had a negative impact. Figure 14 represents the distribution of the answers.

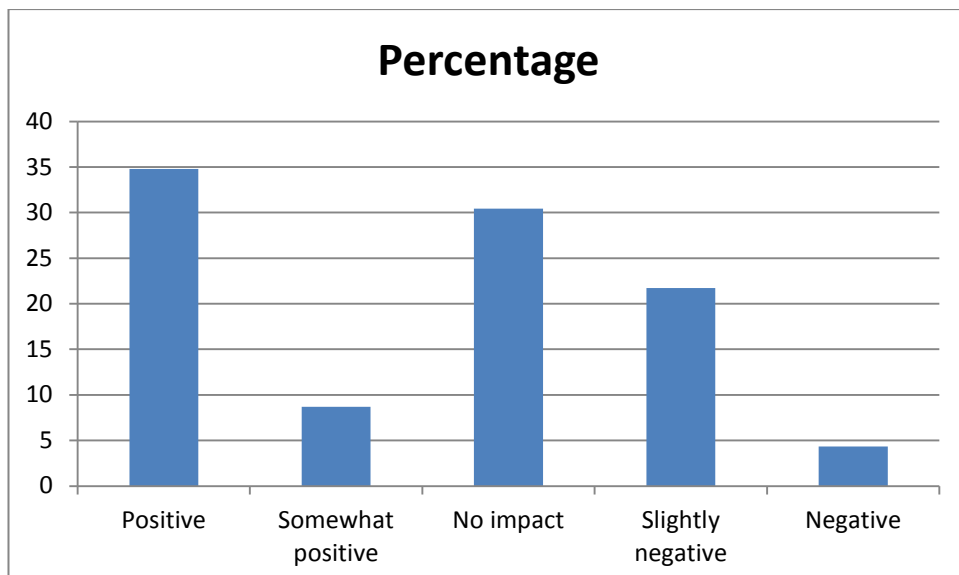


FIGURE 14. What impact did the interview have on the customer's image about Nordea?

The purpose of the third question was to find out if the employees explained properly the grounds for the questions in the basic information form (how the Act obliges Nordea to know their customers). 91% of the respondents felt that they understood why the questions were asked and 9% had no opinion. Nobody considered that they were not given a good explanation for the questions.

The fourth question asked if the customers felt that the interview included relevant and justified questions concerning the company. 48% of the respondents considered the questions to be relevant and justified; 30% agreed to some extent; 4% had no opinion and 17% disagreed to some extent. See figure 15 for the distribution of opinions.

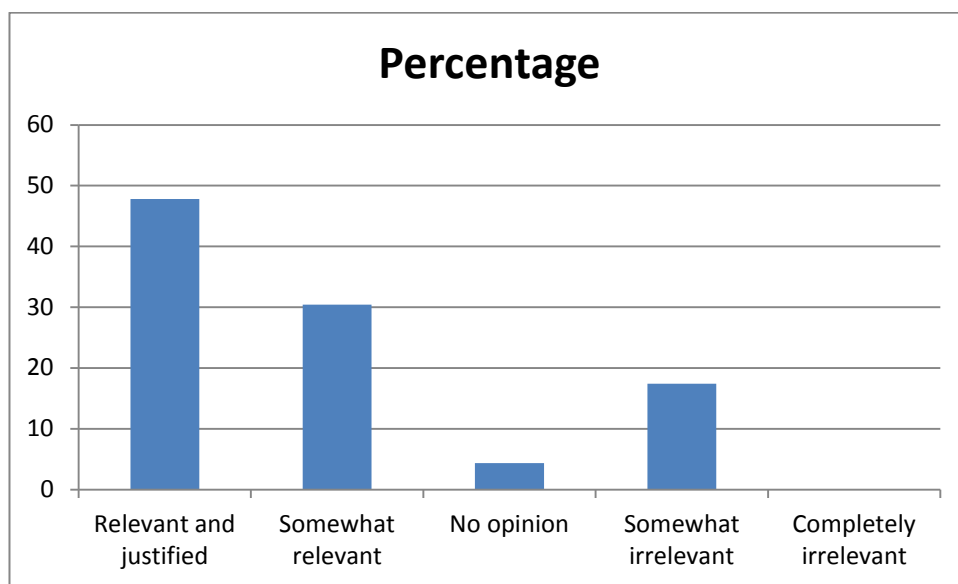


FIGURE 15. Were the questions in the interview relevant and justified?

Not all of the respondents answered in the open question. Those who answered gave mainly positive feedback on the customer relationship and the first meeting when establishing a relationship.

### 6.3 Employees of the Nordea corporate branch

The second questionnaire was about the employees perceptions about the customers when opening a customer relationship. The number of employees responding to the questionnaire was 8. These employees have clients mainly from small and medium

sized enterprises and were a chosen group because they are mostly opening new customer relationships.

As it has been established how the Finnish Act (503/2008) obliges the parties (Nordea), the first meeting with customer is not only about the customer getting products and services he/she needs but the bank to fulfill the obligation laid down in the Act. It can be a challenging task especially if the customer is irritated by the questions asked and considers the process to be complex and time-consuming. It might seem that the employee is between two fires when trying to keep the customer happy and fulfill its obligations.

The first question asked how the employees felt about asking the customers the questions in the basic information form. 13% of the respondents had no problem in asking the questions in the basic information form; 38% considered it to be somewhat easy and fluent. On the other hand, 38% of the respondents felt that it was somewhat uncomfortable and/or time-consuming to ask the questions while no one considered it to be very uncomfortable and/or time-consuming. See figure 16 for the distribution of opinions.

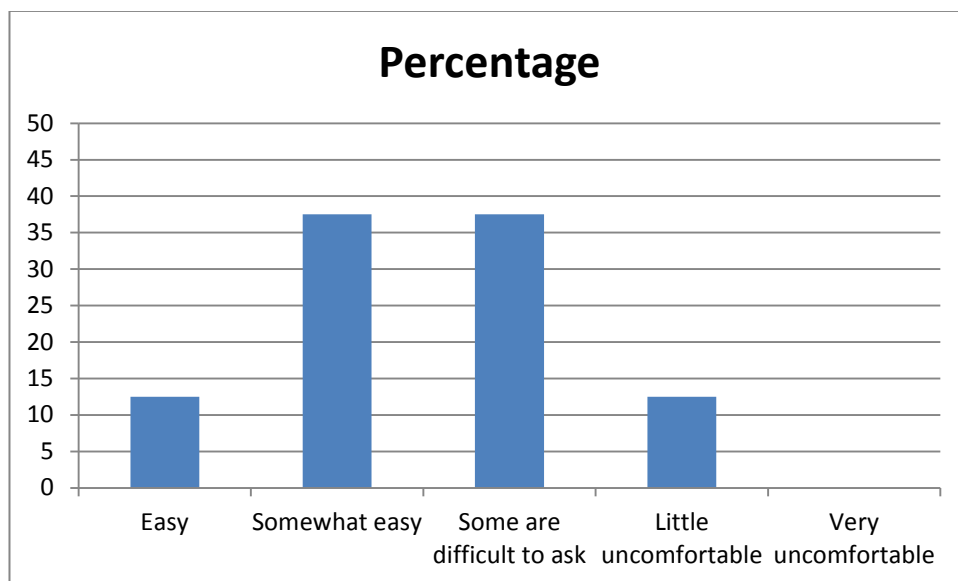


FIGURE 16. How do you feel asking the questions in the basic information form?

The second question asked how the customers respond to the multiple questions – how is their mood? 43% of the employees considered the customers feel positive about the questions and remaining 57% considered them to feel somewhat positive. None of the customers were considered to be negative towards the questions and this is in line with what the customers responded in their questionnaire.

The purpose of the third question was to find out if the employees considered the legal obligation of the customer due diligence to be easily explicable to the customers. The employee knows which Act obliges and what the obligations are. 71% of the respondents considered it to be easy to explain the grounds for the customer due diligence while remaining 29% did not.

Concerning identification of unclear business activities and suspicious transactions a question was asked about what specific questions were more commonly avoided or answered vaguely. This question excluded situation where an answer could not be given – for example accounting firm if not yet decided. Figure 17 provides the distribution regarding the question. In this question multiple choices were allowed so the figures do not represent percentage but actual numbers.

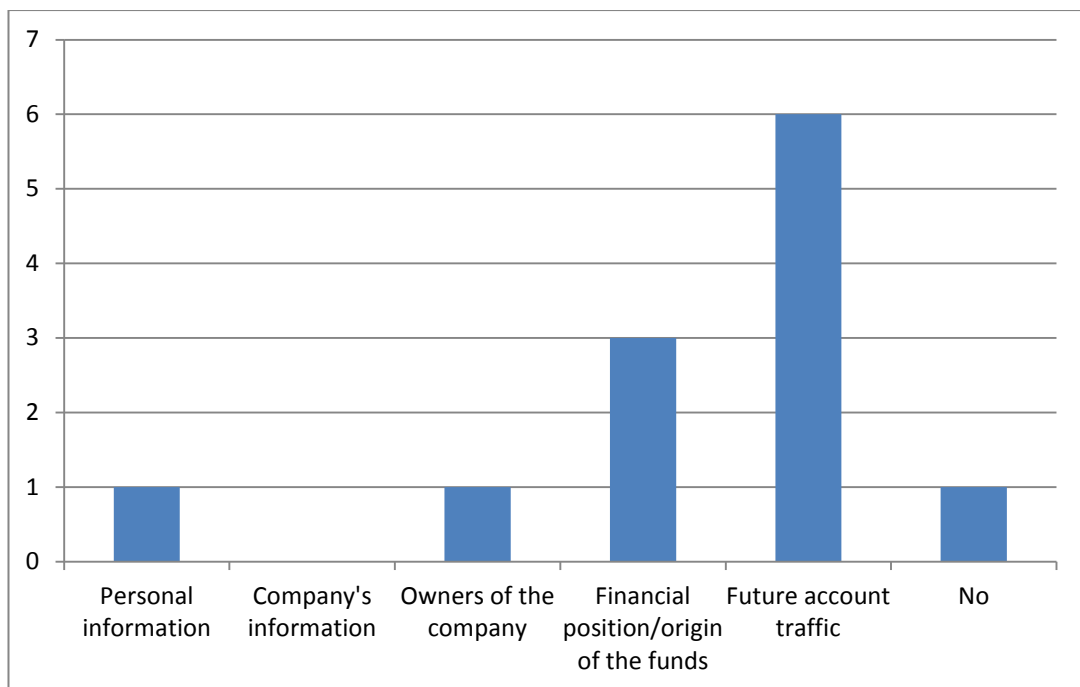


FIGURE 17. Which questions were avoided/answered vaguely?

Obviously the challenge in this question is that the Nordea basic information form asks an estimation of monthly incoming/outgoing domestic/cross-border funds. For some customers it could be difficult to answer. Since money laundering is international crime, should the customer state that no international money transfers will take place detection of such unusual activity should be easy. However, when starting a business an estimation of future income/fixed costs should be identified in order to be prepared to start the

business. It would be alarming the entrepreneur does not have an idea how much income is expected to be generated.

The most important question regarding the prevention of money laundering – especially for illicit funds to enter the financial system – is the origin of the funds. The bank must know where the funds are coming from and it is obliged by the law to have supporting documentation available (The Financial Supervisory Authority, 2010, p.30).

The fifth question asked how often a customer relationship is not established due to insufficient information provided by the customer. Four out of seven answered less often than once a month and three out of seven answered never. Other reasons for not establishing a customer relationship are negative credit information or an unauthorized person is in the meeting.

The sixth question asked how often the interview has led to reporting of suspicious business activity. It turned out that this is not a common issue at all. Two replied less often than once a month and 4 replied never.

## 7 CONCLUSION

There are two sources of pressure related to customer due diligence in a financial institution: The obligations laid down in the Finnish Act (503/2008) and possible consequences of violation of the obligations; the pressure created by the customer who might be expecting fast and smooth customer service. Financial institutions as any other businesses whose one (if not the most important) aim is to gain market share and strengthen the business face the challenge of satisfying the customer demand and attracting new customers while following the strict legal obligations.

The aim of this final thesis was to provide the commissioner with information about the threat of money laundering in a financial institution, and what is the interrelationship between the customer due diligence obligation and how the customers experience the interviewing in Nordea corporate branch. Obviously this information could be used to evaluate the process of the data obtaining and the customer service and adjust it to make it smoother and more convenient for the customer while following proper customer due diligence.

The first step for opening a new customer relationship is obtaining reliable information about the company, its actual business, true beneficial owner's, and knowledge about how the banking services/products are to be used. This is extremely essential in order to fulfill the legal obligation and to avoid potential risk related to money laundering. Transparency is the key word in knowing the company's owners and business.

The results gained from the customer survey shows that the customers mainly consider this information obtaining (interview) to be fast and smooth and to generate rather positive image about Nordea. The customers seemed to understand why the questions in the interview were asked and considered the questions to be relevant. Those, whose experience was somewhat negative, considered the interview in the meeting to be somewhat complex.

When interviewing the employees of the Nordea corporate branch, two questions in the basic information form were highlighted – in terms of customer avoidance: Questions concerning the origin of the funds/company's financial position and future account traf-

fic. If the company is entering the market and no sales have been made, it is obviously a difficult task to evaluate future sales revenue. However, in order to avoid risk the entrepreneur should have some idea about the business and what the expected revenues will be. If the entrepreneur has no idea about future sales, it indicates that he/she has done no market research and do not know what the industry is generating, or is lacking knowledge about his/her business at all. Obviously exact estimations are very difficult to make.

Another aspect of future account traffic is connected to the outgoing traffic. An entrepreneur should know what the company's fixed costs are: inventory, rent, salary etc. It should also be known whether there are any international payments or not. Should the customer answer that no outgoing international payments will be made, but later is found that there has been such, it clearly indicates an unusual activity and raises suspicion.

The origin of the funds and company's financial position was answered in the survey to be another question that was raised from the others. Naturally, due to the low number of respondents no general assumptions can be made, but the answers rather represent the evaluation of Nordea corporate branch Tampere employees (with SME customers). In order to prevent possible money laundering, the most important issue is to know where the funds are originating; supporting documentation should be available.

According to the Annual Report 2012 (Financial Intelligence Unit), the major transactions connected to suspicious activity are in the forms of account money traffic and cash deposits/withdrawals. Therefore, one of the most important questions connected to money laundering are the purpose of the banking services/future account traffic and the origin of the funds. This is because obtaining information on the owners and the actual business is not necessarily conclusive; lawfully operating businesses could still be used in a money laundering process without them even acknowledging it. What actually happens within a bank account provides more clues on whether a transaction is suspicious or not. Of course non-transparent ownership and connections to tax havens can eliminate a customer relationship at an early stage but it is only valid if such circumstances are identified.



Since the commissioner's basic information form contains a lot of questions about the business, it might take some time to cover everything. According to the customer survey the feedback on the questions were mainly positive and supporting. It is not a valid idea to neglect the basic information form with the assumption of customers getting nervous about the multiple and somewhat personal questions because in reality they are not and in any case the commissioner's employees are obliged by the law to obtain all the information. A key to good and fluent customer service is that the customer feels that the employee is interested in him/her, and this could be done through a conversational interview. The purpose of the interview is to gain answers for the basic information which can be finalized later. In order to have a proper database, all information should be saved for future evaluation – Whatever the customer answered in the questions. If some sections are left blank, it is not known whether the interviewer asked the question at all or not.

Since there is some double work in opening a new customer relationship – filling out the basic information form and entering the same information in Nordea's register – this can make the meeting seem complex and time-consuming. After assessing that a customer relationship will be opened, the information could be entered first in the register and whatever information is left out could be added to the basic information. After the meeting all the blank sections in the basic information form could be filled out. It would be important to identify sections that are not covered in the register and highlight those in the basic information form for easier and faster filling.

## REFERENCES

- Act on Detecting and Preventing Money Laundering and Terrorist Financing* (503/2008). Ministry of the Interior, Finland. Unofficial translation. Read 25.9.2013. <http://www.finlex.fi/en/laki/kaannokset/2008/en20080503.pdf>
- Grasso, P. Bellavia, E. 2012. *Mafian rahat ja miten ne pestään*. Atena Kustannus Oy. Jyväskylä.
- Heikinheimo S. 1999. *Rahanpesu – Erityisesti kriminalisoinnin ja konfiskaation näkökulmasta*. Poliisi Ammattikorkeakoulu, Espoo.
- High-risk and non-cooperative jurisdictions – October 2013*. Financial Action Task Force. Read 30.10.2013. <http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/>
- Huhtamäki A. 2000. *Rahan Jäljittäminen*. Kauppakaari Oyj, Lakimiesten Kustannusliitto. Helsinki.
- Illicit money: How much is out there?* United Nations Office on Drugs and Crime. Read 30.9.2013. [http://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money\\_-\\_how-much-is-out-there.html](http://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-_how-much-is-out-there.html)
- International Standards on Combating Money Laundering and the Financing of terrorism & Proliferation - FATF Recommendations. 2012. Read 27.9.2013. <http://www.fatf-gafi.org/topics/fatfrecommendations/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html>
- Mauno, A. 2013. *Nordealle rangaistus rahanpesussa lepsuilusta*. Kauppalehti. Read 2.10.2013. <http://www.kauppalehti.fi/etusivu/nordealle+rangaistus+rahanpesussa+lepsuilusta/201304402541>
- Mitä SEPA tarkoittaa? – Finanssialan Keskusliitto. Read 27.9.2013. [http://www.fkl.fi/teemasivut/sepa/sepan\\_maaritelma/Sivut/default.aspx](http://www.fkl.fi/teemasivut/sepa/sepan_maaritelma/Sivut/default.aspx)
- Money laundering: A three stage process*. About Business Crime Solutions Inc. Read 30.9.2013. [https://www.moneylaundering.ca/public/law/3\\_stages\\_ML.php](https://www.moneylaundering.ca/public/law/3_stages_ML.php)
- Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors*. OECD & TPA. 2009. Read 9.10.2013. <http://www.oecd.org/ctp/exchange-of-tax-information/moneylaunderingawarenesshandbook.htm>
- Neira, T., Perämaa, J., Vasara, P. 2/2003. Repo, A. 8/2012. *Rahanpesurikokset Oikeuskäytännössä VI*. Keskurikospoliisi – Rahanpesun selvittelykeskus. Read 30.9.2013. [http://www.poliisi.fi/poliisi/krp/home.nsf/files/D01EB6312D51ADBCC2257B0500454FBA/\\$file/Rahanpesurikokset%20oikeusk%C3%A4yt%C3%A4nn%C3%B6ss%C3%A4%20VI.pdf](http://www.poliisi.fi/poliisi/krp/home.nsf/files/D01EB6312D51ADBCC2257B0500454FBA/$file/Rahanpesurikokset%20oikeusk%C3%A4yt%C3%A4nn%C3%B6ss%C3%A4%20VI.pdf)

Nordea – Annual Report 2012. Read 25.9.2013.

[http://www.nordea.com/sitemod/upload/Root/www.nordea.com%20-%20uk/Investorrelations/reports/ar/Nordea\\_Annual\\_Report\\_2012.pdf](http://www.nordea.com/sitemod/upload/Root/www.nordea.com%20-%20uk/Investorrelations/reports/ar/Nordea_Annual_Report_2012.pdf)

Nordea – Facts & Figures. Read 01.12.2013.

<http://www.nordea.com/About+Nordea/Nordea+overview/Facts+and+figures/1081354.html>

*Nordea-muuleja epäillään rahanpesusta.* Taloussanomat, 2010. Read 2.10.2013.

<http://www.taloussanomat.fi/rahoitus/2010/08/24/nordea-muuleja-epaillaan-rahampesusta/201011649/12>

Nyström, E. 14.08.2013. *Suomen somalialaiset huolissaan rahalähetysten keskeyttämisestä.* Helsingin Sanomat. Read 25.10.2013.

<http://www.hs.fi/kotimaa/Suomen+somalialaiset+huolissaan+rahal%C3%A4hetysten+keskeytt%C3%A4misest%C3%A4/a1376364669191>

*Rahanpesun torjunta* – Keskusrikospoliisi. Read 24.10.2013.

<http://www.poliisi.fi/poliisi/krp/home.nsf/pages/ABD14634404812EEC2257586005034F1?opendocument>

*Standard 2.4 – Code of Conduct.* Financial Supervisory Authority. Read 24.10.2013.

[http://www.finanssivalvonta.fi/en/Regulation/Regulations/Financial\\_sector/2\\_Code\\_of\\_conduct/Documents/2.4.std3.pdf](http://www.finanssivalvonta.fi/en/Regulation/Regulations/Financial_sector/2_Code_of_conduct/Documents/2.4.std3.pdf)

The Basel AML Index 2013. Basel Institute on Governance. Read 16.10.2013.

<http://index.baselgovernance.org/index/Index.html>

*The Criminal Code of Finland (39/1889).* Ministry of Justice, Finland. Unofficial translation. Read 25.9.2013. <http://www.finlex.fi/en/laki/kaannokset/1889/en18890039.pdf>

*What is money laundering.* Financial Action Task Force. Read 4.10.2013

<http://www.fatf-gafi.org/pages/faq/moneylaundering/>

The Economist. July 20 2013, volume 408, number 8845. *African money transfers – let them remit.* London.

Turunen, J. 2013. Personal interview at Nordea corporate branch, Tampere.

## APPENDIX

### Appendix 1. Europe – The Basel AML Index 2013 ranking (Min. 0 Max. 10)

Country	Score
	6,39
Greece	
Luxembourg	6,24
Turkey	6,11
Austria	5,79
Germany	5,79
Macedonia	5,78
Croatia	5,76
Switzerland	5,76
Russia	5,75
Bosnia	5,61
Italy	5,54
Albania	5,43
Serbia	5,19
Spain	5,18
Moldova	5,06
Cyprus	5,03
The Netherlands	5,01
Latvia	4,93
United Kingdom	4,81
Slovakia	4,76
Czech Republic	4,74
Poland	4,74
Romania	4,68
Ireland	4,63
Denmark	4,49
Montenegro	4,46
Portugal	4,3
Iceland	4,28
Belgium	4,23
France	4,23
Bulgaria	4,13
Hungary	4,07
Malta	4,01
Lithuania	3,81
Sweden	3,75
Finland	3,74
Estonia	3,31
Slovenia	3,3
Norway	3,17

Appendix 2. Basic Information Form

1(3)

**Basic information, corporate customer** 1 (3)

Branch number and name

dd.mm.yyyy

Name of the employee

Customer ID

The legislation binding banks, including the Act on Preventing and Clearing Money Laundering and Terrorist Financing, requires that a bank must know its customers. If a customer is new or has been passive for a long while, the bank ensures that it knows the customer by saving the customer's information using the basic information form and, if necessary, by asking the customer to deliver different kinds of additional statements. The bank does not establish a business relationship without sufficient information. When an existing customer relationship is active, the basic information form ensures that the basic information is documented appropriately. Consequently, the basic information form must be filled in or updated also when the customer is active if the form has not been filled in earlier.

**Company's basic information**

Company's official name		Business Identity Code	
Street address		Postal code	City
Domicile	Country of registration	Country of taxation	Telephone number
Address in the locality where the customer does its banking		Places of business elsewhere (localities)	
Main industry	Industrial classification TOL/NACE	Belongs to a group (fill in section 1 of the appendix) <input type="checkbox"/> No <input type="checkbox"/> Yes, what group	
Internet address		Marketing name if not the same as official name	
Name of contact person		Position	
Telephone number		E-mail address	

**Company to be established**

Missing documents	Agreed delivery date
Names of future owners	Starting date of operations

**Owners' details (person or corporation holding over 25% of the shares or voting rights)**

If the owner is a corporation, fill in section 1 in the appendix or ask an ownership chart from the customer

Owner's name	Personal identity number or date of birth	Holding %
Nationality or domicile <input type="checkbox"/> Finland <input type="checkbox"/> other, what	Business Identity Code	
Owner's name	Personal identity number or date of birth	Holding %
Nationality or domicile <input type="checkbox"/> Finland <input type="checkbox"/> other, what	Business Identity Code	
Owner's name	Personal identity number or date of birth	Holding %
Nationality or domicile <input type="checkbox"/> Finland <input type="checkbox"/> other, what	Business Identity Code	
Owner's name	Personal identity number or date of birth	Holding %
Nationality or domicile <input type="checkbox"/> Finland <input type="checkbox"/> other, what	Business Identity Code	

Continue in a separate appendix, if needed.

**Politically exposed persons (PEP)**

PEP refers to a person who has acted over the past 12 months or is acting now in a prominent position in the service of another state. A person is considered a PEP also if his or her close relative or close business partner is a PEP.

Is the company's representative a PEP? <input type="checkbox"/> No <input type="checkbox"/> Yes, fill in section 2 in the appendix.	Is one of the owners a PEP? <input type="checkbox"/> No <input type="checkbox"/> Yes, fill in section 2 in the appendix.
Is one of the board members a PEP? <input type="checkbox"/> No <input type="checkbox"/> Yes, fill in section 2 in the appendix.	Is the managing director a PEP? <input type="checkbox"/> No <input type="checkbox"/> Yes, fill in section 2 in the appendix.
Is one of the persons authorised to sign for the company a PEP? <input type="checkbox"/> No <input type="checkbox"/> Yes, fill in section 2 in the appendix.	Is a close relative or a business partner of any of the aforementioned persons a PEP? <input type="checkbox"/> No <input type="checkbox"/> Yes, fill in section 2 in the appendix.

**Basic information, corporate customer** 2 (3)

Branch number and name

dd.mm.yyyy

Name of the employee

Customer ID

**Information on accounting firm and accountant**

Name of accounting firm	Telephone number
Name of accountant	Telephone number
Name of auditor/auditing firm	Telephone number

**Operations in Finland**

Number of employees	Estimated turnover (thousand per year)	Financial period (dd Month - dd Month)
---------------------	--	--

Description of operations (incl. business idea, description of main product or service, is the product or service offered to consumers or other companies)

Financial situation (equity, debts, cash reserves, financial and commercial undertakings, such as rent liabilities, franchising costs and leasing liabilities)

Origin of the funds of the company to be established and the new customer customer relationship (amount, where and from whom did the funds come from – if needed, the customer's separate statement on the origin of the funds, including necessary documents)

Do the operations involve one or several of the following (fill in the corresponding sections in the appendix)?

- |  |  |   |
|--|--|---|
| <input type="checkbox"/> Payment transmission (3 and 4)    | <input type="checkbox"/> Currency exchange (3 and 4) | <input type="checkbox"/> Gambling or betting (3 and 4)  |
| <input type="checkbox"/> Payday loans (3 and 4)            | <input type="checkbox"/> Construction (3)            | <input type="checkbox"/> Provision of financial or investment services (3 and 4)                  |
| <input type="checkbox"/> Cleaning (3)                      | <input type="checkbox"/> Second-hand trade (3)       | <input type="checkbox"/> Association activities, especially fund raising (4 and 5)                |
| <input type="checkbox"/> Real estate brokerage (3)         | <input type="checkbox"/> Restaurant business (3)     | <input type="checkbox"/> Foreign companies, a subsidiary or branch of a foreign company (3 and 6) |
| <input type="checkbox"/> Significant operations abroad (7) |  |   |

**Business partners**

Most important Finnish business partners (names)

Most important foreign business partners (name and country)

**Description of payment traffic**

Incoming payments		Outgoing payments	
Estimate of incoming <u>domestic</u> payments	Estimate of incoming <u>foreign</u> payments	Estimate of outgoing <u>domestic</u> payments	Estimate of outgoing <u>foreign</u> payments
payments per month _____	payments per month _____	payments per month _____	payments per month _____
euros per month _____	euros per month _____	euros per month _____	euros per month _____
From which countries		To which countries	
How they are related to operations		How they are related to operations	

**Basic information, corporate customer** 3 (3)

Branch number and name

Name of the employee

Need for banking services/products

Customer ID



Scope of banking				
Main banker	Principal need for banking with Nordea			
Financing	<input type="checkbox"/> No	<input type="checkbox"/> Nordea	<input type="checkbox"/> Elsewhere, where	Total, euros
Investment	<input type="checkbox"/> No	<input type="checkbox"/> Nordea	<input type="checkbox"/> Elsewhere, where	Total, euros
Insurance	<input type="checkbox"/> No	<input type="checkbox"/> Nordea	<input type="checkbox"/> Elsewhere, where	
Accounts	<input type="checkbox"/> No	<input type="checkbox"/> Nordea	<input type="checkbox"/> Elsewhere, where	
Cash Management	<input type="checkbox"/> No	<input type="checkbox"/> Nordea	<input type="checkbox"/> Elsewhere, where	
Online banking	<input type="checkbox"/> No	<input type="checkbox"/> Nordea	<input type="checkbox"/> Elsewhere, where	
Cards	<input type="checkbox"/> No	<input type="checkbox"/> Yes	Corporate cards in use	
Foreign banks	<input type="checkbox"/> No	<input type="checkbox"/> Yes, where		
Other, what				

**Received documents**

<input type="checkbox"/> Extract from Trade Register	<input type="checkbox"/> Articles of Association	<input type="checkbox"/> Financial statements	<input type="checkbox"/> Minutes	<input type="checkbox"/> Partnership agreement
<input type="checkbox"/> Specimen signatures	<input type="checkbox"/> Group's organisation and ownership chart	<input type="checkbox"/> Separate statement on the origin of funds, if needed		
<input type="checkbox"/> Business plan	<input type="checkbox"/> Letter of reference, from whom			
<input type="checkbox"/> Power of attorney	<input type="checkbox"/> Other, what			

**Documents acquired by the bank**

Suomen Asiakastieto inquiries			Date
<input type="checkbox"/> Credit information	<input type="checkbox"/> Board member information	<input type="checkbox"/> Corporate connections of owners and beneficial owners	

**Company representative at the meeting**

Name (last name, first names)		Personal identity number or date of birth	Authorisation to sign for the company <input type="checkbox"/> No <input type="checkbox"/> Yes
Address in Finland		<input type="checkbox"/> permanent <input type="checkbox"/> temporary, reason:	
Address abroad		<input type="checkbox"/> permanent <input type="checkbox"/> temporary, reason:	
Tel (home/work)	Mobile phone	Position in the company	
E-mail address		Nordea's customer <input type="checkbox"/> No <input type="checkbox"/> Yes	
Identity verified <input type="checkbox"/> Driver's licence <input type="checkbox"/> Passport <input type="checkbox"/> Identity card		Issuer, number, date and country	

**Person filling in the form**

Place and date	
Signature and name in block letters of the person identifying the customer	Approver's signature and name in block letters

Appendix 3. Questionnaire about customer identification at Nordea corporate branch – customers

The purpose of the questionnaire was to find out how customers experience the questions about customer identification and business information when opening a new customer relationship.

1(2)

**KYSELY ASIAKKAAN TUNNISTAMISESTA YRITYSKONTTORISSA - HENKILÖASIAKAS**

Tämän kyselyn tarkoitus on selvittää miten asiakkaat kokevat yritysasiakkaan tunnistamiseen liittyvät kysymykset Nordean yrityskonttorissa.

Kysymyksiin 1 – 4 vastataan valitsemalla parhaiten kuvaava vaihtoehto. Kysymys 5 antaa mahdollisuuden antaa kirjallista palautetta/tuntemuksia ensitapaamisesta Nordeassa. Kysymykset käsitellään nimettömästi.

**1. Mikä seuraavista kuvaa parhaiten tuntemuksianne kun Teiltä kysyttiin liiketoiminnasta Nordean yrityskonttorissa?**

1 = Sujuva ja nopea

2 = Jokseenkin sujuva

3 = En osaa sanoa

4 = Hieman monimutkainen

5 = Todella monimutkainen ja aikaa vievä

**2. Vaikuttiko liiketoiminnasta esitetyt laajat kysymykset kuvaanne Nordeasta seuraavasti:**

1 = Negatiivisesti

4 = Hieman positiivisesti

2 = Hieman negatiivisesti

5 = Positiivisesti

3 = Ei vaikutusta

(continues)





Appendix 4. Questionnaire about establishing a customer relationship at Nordea corporate branch – employees

The purpose of the questionnaire was to find out how the employees experience the interviewing and what perceptions they have about customers when asking the questions.

1(3)

**KYSELY ASIAKASSUHTTEEN PERUSTAMISESTA NORDEAN YRITYSKONTTORISSA**

Tämän kyselyn tarkoitus on selvittää miten Nordean työntekijät kokevat asiakassuhteen perustamisprosessin Nordeassa ja mitä haasteita siihen liittyy.

Kysymyksiin 1 – 4 ja 6 vastataan valitsemalla parhaiten kuvaava vaihtoehto. Kysymykset 5 ja 7 antavat mahdollisuuden kirjoittaa vapaasti omia kokemuksia. Kysymykset käsitellään nimettömästi.

**1. Miten koet perustietolomakkeen kysymysten esittämisen uusille/vanhoille asiakkaille?**

1 = Helppoa ja sujuvaa

4 = Hieman epämiellyttävää ja/tai aikaa vievää

2 = Jokseenkin sujuvaa

5 = Todella epämiellyttävää ja/tai aikaa vievää

3 = Jotkut kysymykset ovat hankala esittää asiakkaalle

**2. Miten asiakkaat suhtautuvat lomakkeen kysymyksiin?**

1 = Negatiivisesti (aiheuttaa ärtymystä ja kyseenalaistamista)

2 = Hieman negatiivisesti (vastaavat vastahakoisesti)

3 = Hieman positiivisesti (jotkut kysymykset ohitetaan)

4 = Positiivisesti (vastaavat mielellään)

(continues)

**3. Onko laillinen peruste asiakkaan tunnistamisvelvoitteelle helposti selvitettävissä asiakkaalle?**

1 = Ei (et ole varma mihin lakitekstiin velvoite perustuu ja/tai vaikea löytää oikeita sanoja)

2 = Kyllä (tiedät miten laki velvoittaa ja/tai asiakas hyväksyy kyseenalaistamatta)

**4. Onko kysymyksiä jotka useimmin ohitetaan/vastataan epämääräisesti (voimioimio useamman)?** Lukuunottamatta kysymyksiä joihin vaikea arvioida vastausta (esim. arvioitu liikevaihto)

1 = Kysymykset koskien henkilötietoja

2 = Kysymykset koskien yrityksen tietoja

3 = Kysymykset koskien yrityksen omistajia

4 = Kysymykset koskien taloudellista tilannetta/varojen alkuperää?

5 = Kysymykset koskien tulevaa tililiikennettä

6 = Joku muu, mikä?

---



---



---

7 = Ei

**4. Kuinka usein asiakassuhde jää perustamatta puutteellisesti annettujen tietojen takia?**

1 = Päivittäin

4 = Kuukausittain

2 = Viikottain

5 = Harvemmin kuin kerran kuussa

3 = Joka toinen viikko

6 = Ei koskaan

(continues)

