BEST PRACTICES IN CONTROLLING TRADE-BASED MONEY LAUNDERING

Jyväskylä University
School of Business and Economics

Master's Thesis

2020

Author: Jyri Häyrinen
Subject: Banking and International Finance
Supervisor: Juhani Raatikainen

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

ABSTRACT

Author
Jyri Häyrinen

Title
Best Practices in Controlling Trade-Based Money Laundering

Subject	Type of work
Banking and International Finance	Qualitative Research
Date	Number of pages
6.6.2020	82

Abstract

Trade-Based Money Laundering (TBML), as one of the main money laundering methods, has gained increasing amount of attention amongst policy makers, other authorities and also private sector on how criminals are attempting to abuse international trade system. As the purpose of money laundering is to conceal the true origins of illicit gains and to make these gains to appear legitimate, the international trade system provides an attractive cover for criminals to hide their illicit gains within the sea of trade transactions occurring each day. Due to the role of banking as main facilitator of international payments and trade transactions, banks have wide access to customer and transaction data, which has shifted the responsibility of detecting potential illicit customer behaviour for the banks. As this role shift is expected to further increase responsibilities of banks to conduct stricter anti-money laundering (AML) controls in the future, the research was designed to share relevant information on how to combat against the evolving threat of TBML within banking industry.

In the recent years there have been growing amount of public cases, where internationally operating banks have failed to prevent illicit money flows and as such as they have not been able to comply with AML regulation. As the behaviour of money launderer constantly changes according to the underlying regulation and circumstances, banks are obliged to identify emerging money laundering trends and to develop matching controls for their prevention. The intention of this research was to improve understanding within banks on how TBML can be mitigated in a way that all relevant banks could share the same amount of information related to this emerging threat. This research was meant to fill the informational gap by identifying potential TBML red flag indicators, also defined as risk indicators, of how banks can detect TBML methods, and most importantly the research explores what are the best practices of controlling these risks. The research was conducted by collecting red flag indicators from available AML resources and by requesting financial institutions to response to the research questionnaire with their current best-known practices in controlling against TBML risks.

The research emphasized how evident Know-Your-Customer (KYC) processes are for banks to detect any abnormal customer behaviour, and how the risk-based approach has become a guiding principle for implementing AML controls. As the international trade system and transmittance of payments is highly data-driven many of the controls for fighting against TBML are relied on developing digital solutions within bank systems. Nonetheless, the research further brought out the importance of sharing knowledge of

TBML typologies to all relevant staff from client-facing units to transaction monitoring teams. As the progress in AML regulation is expected to transfer criminals to more sophisticated money laundering operations, there exists increased incentives for banks to gain knowledge on TBML methods and how they can be controlled.
Key words Trade-Based Money Laundering, Anti-Money Laundering, Risk-Based Approach
Place of storage Jyväskylä University Library

TIIVISTELMÄ

Tekijä Jyri Häyrinen	
Työn nimi Best Practices in Controlling Trade-Based Money Laundering	
Oppiaine Banking and International Finance	Työn laji Laadullinen Tutkimus
Päivämäärä 6.6.2020	Sivumäärä 82

Tiivistelmä

Trade-Based Money Laundering (TBML) yhtenä merkittävimpänä rahanpesu mekanismina on herättänyt viime vuosien aikana monien päättäjien, viranomaisten sekä pankkisektorin kiinnostuksen miten rikolliset pyrkivät laittomasti hyödyntämään kansainvälistä kauppaverkostoa omien etujensa tavoitteluun. Huomioiden miten rahanpesun pohjimmaisena tarkoituksena on laittomien varojen alkuperän häivyttäminen ja niiden saaminen takaisin normaaliin talouden kiertoon, kansainvälisen kaupan laaja transaktioiden verkosto tarjoaa houkuttelevan peitteen rikollisten toiminnalle. Pankeilla on merkittävinä tilisiirtojen ja kauppa transaktioiden toteuttajina laaja pääsy asiakastietoihin sekä kauppatietoihin, jonka vuoksi pankkien mahdollisuudet tunnistaa asiakkaiden epäilyttävät liiketoimet ovat lisänneet pankkien roolia TBML:n estämisessä. Tiukentuvan rahanpesu regulaation aikakaudella pankkien velvollisuudet TBML:n sekä muiden rahanpesu mekanismien estäjänä odotetaan korostuvan. Tämän tutkimuksen tarkoituksena oli jakaa pankki sektorin sisällä tietoa, miten pankit voivat vastata TBML:n kasvavaan uhkaan.

Viimeisten vuosien aikana julkisuuteen on levinnyt useita rahanpesuun liittyviä uutisia, joissa kansainvälisesti operoivat pankit ovat epäonnistuneet laittomien rahasiirtojen estämisessä ja näin ollen laiminlyöneet rahanpesusäännösten noudattamista. Rahanpesijän luonteeseen sisältyy olennaisena osana muokkautuminen olemassa olevaan regulaatioon sekä olosuhteisiin, jonka vuoksi pankkien tehtävänä on jatkuvasti päivittää tietämystä uusien rahanpesu mekanismien osalta ja arvioida parhaita käytänteitä rahanpesun estämiseen. Tutkimuksen tavoitteena on lisätä kaikkien pankkien ymmärrystä tähän yhteiseen ongelmaan ja siihen, miten TBML riskejä saadaan kontrolloitua. Tutkimuksen toteutustapana oli kerätä eri rahanpesun estämiseen liittyvistä lähteistä TBML riski indikaattoreita, jonka jälkeen pankkeja pyydettiin tutkimuskyselyssä kuvaamaan tämän hetken parhaita käytänteitä, miten pankit kontrolloivat kyseisisiä riski indikaattoreita.

Tutkimuksen aikana korostui miten keskeinen rooli Asiakkaan Tuntemisella (KYC) on potentiaalisten epäilyttävien liiketoimien tunnistamisessa, ja kuinka riskiperusteisesta lähestymistavasta on muodostunut tärkein ohjesääntö rahanpesun estämisen kontrollien laatimisessa. Pankkien vastaustenkin perusteella monet TBML kontrollit keskittyvät digitaalisten ratkaisujen kehittämiseen pankkijärjestelmän sisällä, joiden avulla suuresta tilisiirtojen ja kaupan rahoituksen datan määrästä on mahdollista tunnistaa potentiaaliset epäilyttävät tapahtumat. Digitaalisten ratkaisujen kehittämisen lisäksi tutkimus osoitti, miten tärkeää on jakaa tietoja TBML mekanismeista kaikkien liiketoiminta yksiköiden välillä korostaen roolia asiakasvastuullisten ja transaktioiden monitoroinnista vastaavien yksiköiden kohdalla. Jatkuvasti kehittyvän rahanpesun estämisen regulaation odotetaan siirtävän rikollisia entistä sofistikoituneempiin rahanpesu operaatioihin, jonka vuoksi pankeilla on kasvava tarve kerätä tietoa TBML mekanismeista ja etenkin siitä, miten niitä voidaan kontrolloida.

Asiasanat
Trade-Based Money Laundering, Rahanpesun Estäminen, Riskiperusteinen Arviointi

Säilytyspaikka
Jyväskylän Yliopiston Julkaisukirjasto

CONTENTS

1 INTRODUCTION

1.1 What is Trade-Based Money Laundering?

The Financial Action Task Force (FATF), the inter-governmental body setting standards for anti-money laundering, counter terrorist-financing and other financial crime prevention, has defined trade-based money laundering (TBML) as "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins" (FATF, 2006, p.5). An important difference to other money laundering techniques is the use of goods and services that can be transferred from one jurisdiction to another by making a contract between two parties. If actual market value of the goods and services differs significantly from the one used in the transaction, an illegal money transfer – a money laundering scheme – is created. In these kinds of schemes, criminal organizations or terrorist financiers' illicit money does not have to be in liquid forms such as cash, checks or balances on bank accounts, as the falsification of trade documents of goods and services, and their values, can also represent the illicit gains (Cassara, 2016). Essentially, the mechanism can be exploited by colluding parties or alternatively without other party knowing the underlying purpose of the transaction, in which at least the other party is aiming to create a legitimate cover for an illicit payment.

It can be stated that the TBML is not solely a mechanism to launder illicit money gained by committing to a predicate offence, and instead the mechanism can also be exploited for other purposes. Varied forms of TBML are used by many white-collar criminals and corporate business for monies that may be obtained legally, and the purpose is to evade taxes or to arrange capital flight schemes (Naheem, 2017). Furthermore, TBML techniques can also be used for the purpose of terrorist financing and evading of sanctions, which additionally increases the layers of TBML. Due to the complexity of TBML schemes, it has become a difficult task for both banking and academic fields to reach a common definition for TBML. It has been stated that the definition by the FATF is not sufficiently accurate, as it does not clarify whether TBML refers to domestic or to international trade, if goods and services are both included and whether it includes terrorism financing or tax evasion even if money is not from illicit origins (Soudijn, 2014). For the purpose of this research, the FATF definition is mainly applied to the transfer of goods in the money laundering context.

1.2 What is the magnitude of the problem?

The FATF has stated that there are three main methods criminals and terrorist financiers are using to hide the origins of their illicit money and to integrate them back to the economy; the first one is using the financial system in form of wire transfers, the second one includes the use of cash, and the third method includes

the movement of goods or services in international trade system (FATF, 2006). Due to the FATF attention, and the progress achieved on anti-money laundering and counter-terrorist financing controls on both transfers of money and also in cash transactions, there has been an increase in the attractiveness for criminals to use TBML methods and to increase the level of sophistication on money laundering methods.

For the purpose of constructing a framework of how large of an issue money laundering is in the global scale, the discussion could be commenced by some of the estimates provided by international authorities. In a study conducted by the United Nations Office on Drugs and Crime (2011), it was estimated that in the year of 2009 alone, all criminal proceeds equaled to around 3.6 per cent of global GDP, converting to approximately $2.1 trillion, from which the amount of money laundered equaled to $1.6 trillion. These estimates are in line with the previous statements from the year 1998 generated by the International Monetary Fund (IMF), which had estimated the range of money laundered to remain between 2% to 5% of global GDP (UNODC, 2011). Due to the illegality of money laundering transactions, there exist no scientific data on the actual scale of the issue, and as these estimates are merely expressing the approximate magnitude of the issue, the estimates should be treated with caution (FATF, 2019). The same issue applies to the magnitude of TBML, since taking a holistic view to the whole mechanism is made impossible due to the lack of accurate statistics. Nevertheless, it can still be argued with confidence that acquired criminal proceeds followed by money laundering operations provide a serious threat to the global economy.

The Global Financial Integrity (GFI), a non-profit organization established in Washington D.C., has further investigated the illicit financial flows related to TBML, and especially on one of its primary methods, trade misinvoicing (Cassara, 2016). The study conducted by the GFI (2019) focused on the illicit financial flows between advanced economies and in the total of 148 developing or emerging economies during the years from 2006 to 2015. By applying data from two different databases, derived from both the IMF and the UN, the research estimated the potential illicit flows to be around 20 to 30 percent of total trade in the developing countries during the ten-year tenure (GFI, 2019). The connection this research makes to exploitation of TBML in the developing countries is related to the misinvoicing of trade transactions, as the research concludes the share of trade misinvoicing to be approximately 87 percent of the total illicit financial flows (GFI, 2019). Due to the significant share of trade associated with illicit intentions, especially governments and their citizens in developing countries become victims to various TBML mechanisms, which furthermore highlights the magnitude of this problem.

One of the main reasons why criminals might be willing to exploit TBML, especially as the controls for cash and wire transfers have become stricter, is the continuously increasing amount of global trade. Based on the report by the World Trade Organization (2018), the level of world merchandise exports and world

commercial services exports in the year of 2017 equaled to $17.73 trillion and $5.28 trillion, respectively. In comparison to the year of 2015, when the same trade amounts equaled $16.2 trillion and $4.68 trillion, it underlies the global trend of how international merchandise and services trade has gained its importance (WTO, 2016). From a money laundering perspective, the increasing volumes of global trade accompanied by advanced technology provide an attractive cover for criminals to layer illicit funds, either by smuggling of cash or by transporting of goods, through the use of trade transactions that might appear legitimate (Asia/Pacific Group on Money Laundering, 2012). As it belongs to the modus operandi of a money launderer to decrease the level of suspicion raised on the chosen laundering activities, the concealment of illicit gains under the high volume of global trade decreases the probability of getting caught.

The difficulty of measuring global money laundering is the lack of accurate statistics, but at least there are some estimates that help to identify how successfully criminals are captured and how much of the illicit funds are confiscated. According to the estimation by UNODC (2011), the success rate of seizing illicit money was less than 1% out of all illicit money flows during the year of review, further emphasizing the problem related to global money laundering. The US State Department data from the year 2010 from 62 countries confirmed these estimates in which the total of $3.1 billion of illicit money related to money laundering were only seized, resulting around 0.2% of estimated money laundered in global scale (UNODC, 2011). Similar findings are provided by Baker (2005) as in his research the total amount of illicit funds flowing to the US was annually estimated at $250 billion, and out of that amount authorities were able to seize in its best years only around $250 million. According to this estimation, the chances of being captured are 0.1% of all money laundering operations, which clearly states that criminals are confronted by extremely low probabilities of getting caught. Even though it is part of criminal nature to constantly seek new ways to launder money and to circumvent regulations, while making it more difficult for authorities to capture these people, it can be stated that current controls are not in a sufficient level in order to combat against money laundering.

1.3 How is TBML executed?

The initial step of how TBML mechanism is started includes committing to an invoice fraud, where two parties enter into a fraudulent contract by commonly agreeing on the terms of the contract. The key aspect is the cooperation between a buyer and a seller, in this case an exporter and an importer of goods or services, who are able to manipulate the invoice and the supporting documents based on their own preferences (Cassara, 2016). The same view is shared by Baker (2005), who states that "anything that can be priced can be mispriced", and furthermore concludes that "this is by far the most frequently used device for transferring dirty money" (p.25).

The basic TBML techniques for committing invoice fraud according to FATF (2006) are determined as;

1) Over-and under-invoicing of goods and services
2) Multiple invoicing of goods and services
3) Over-and under-shipping of goods and services
4) Falsely described goods and services
5) Phantom shipments

At least one of these techniques might be used in order to legitimize illicit gains, and also if trading partners are planning to increase the complexity of the trade transaction, several of these techniques can be implemented. These techniques are mainly discussed for the trade of goods, but still similar methods can be applied to invoices on services.

Over-and under-invoicing. Illicit transfer of value by over- and under-invoicing is one of the oldest techniques to launder money, and it is still a common practice today. The core of this technique is the misrepresentation of goods being traded between an importer and an exporter in order to transfer value or settle accounts between them, where the shipment of goods, whether actually executed or not, functions as a cover for illicit money (Cassara, 2016). As each good traded internationally has a fair market price, which indicates on how much the seller should be approximately charging on its buyer, the over- or under-invoicing for the same goods enables the transfer of additional value to one of the trading parties. In order to simplify the method, if one wants to move money out of a country, importing goods at overvalued prices or exporting goods at undervalued prices compared to the fair market prices completes the task (Cassara, 2006). In another way around, if one wants to move money into a country, importing goods at undervalued prices or exporting goods at overvalued prices, this can easily be arranged between trading partners (Cassara, 2006). It would not make any economic sense to over- or under-invoice goods, unless these trading parties would be colluding on the transaction, which is why the technique is used and meanwhile, it makes it difficult for financial institutions and competent authorities to detect. Due to the fact that there are jurisdictions around the world which are less rigorous on their money laundering controls, it provides organizations a channel for setting up foreign affiliates or colluding with foreign companies to transfer illicit money by sending mispriced commercial invoices (FATF, 2006).

Multiple invoicing of goods and services. Another modus operandi to launder illicit funds is the issuance of multiple invoices for the same shipment of goods or services, whether fictitious or not. Under this technique, the multiple invoicing also justifies for multiple payments between associated parties, and in many cases, there are number of financial institutions used to complete the multiple payments with the aim to add more complexity to the transactions (FATF, 2006). When compared to the over- or under-invoicing technique, the multiple invoicing technique does not necessarily require mispricing of goods or services as the traded goods can be appropriately priced based on their fair market prices, and the issuance of multiple invoices justifies the transfers of illicit money. Even

though the implementation of this technique would be detected in a financial institution, in customs agency or in other competent authority, the associated trading partners could provide some legitimate reasons for these types of transactions. Some of the possible excuses to justify these multiple payments are cases where the payment terms might have been changed later on, there have been changes to payment instructions or there have been late fees related to unsuccessful prior payments (FATF, 2006).

Over-and under-shipping of goods and services. One alternative way to make both trading parties to benefit from a trade transaction is to change the quantity of goods on the trade documents compared to actual quantities being shipped. Even if the traded goods or services are priced according to the underlying fair market prices, the misstatement of quantities shipped provides a channel to transfer value across borders, in a similar way as with the mispricing of goods. In practice, the short shipping of goods has a similar effect for an exporter as the over-invoicing for the same shipment, as the additional value is transferred back to the exporter (Cassara, 2016). If on the other hand the same exporter has an intention to move value to the importing country, the over-shipping of goods works in the similar way as the under-invoicing of goods as the additional value is transferred to the buyer in the importing country (Cassara, 2016).

Falsely described goods and services. The basic techniques of TBML include the misstatement of prices, quantities and also qualities of either goods or services, and the false descriptions are related to the misstatement of quality in an invoice. By implementing this method, criminals are aiming to obfuscate the customs authorities by misstating the information in shipping and customs documents compared to the actual contents of a shipment (FATF, 2006). As an example, if an exporter is actually shipping relatively expensive goods to another country, but the invoice and shipping documents state that these goods are inexpensive items, the additional value can be transferred to the importing country unless the shipment is more carefully inspected and blocked by authorities. The utilization of this method enables criminals to falsely describe the quality of an item in the same category of goods as what's actually being shipped, or alternatively these shipped goods can be completely different items (FATF, 2006). Both goods and services provide added difficulties for the detection of TBML since both of these can be traded based on bilateral price negotiations, and especially for services it becomes difficult to estimate a fair market price.

Phantom shipments. The last basic technique to transfer value is the arrangement of phantom shipments, which in practice means there are no goods or services actually shipped or offered between trading partners. This technique relies on the falsification of trade documents to seem to be legitimate and to cause least amount of suspicions in order to function as a cover for payment (Cassara, 2016). Without any actual goods being shipped or services offered, the misstatement of price, quality or quantity in invoices is not required under this technique, but it

becomes more difficult to provide any further evidence if the transaction raises suspicions and ends up under investigation.

1.4 How is TBML influencing the banking sector?

The connection between the banking sector and TBML is either related to banks offering credit facilities for trading purposes, entitled as trade finance, or handling of payments between trading counterparties. According to a report by International Chamber of Commerce (2018), which as an organization promotes international trade and functions as the largest business organization in the world, states that the share of trade transactions financed by trade finance is approximately 20% as the majority of trade is financed on open account at 80% of cases. From TBML perspective both of these ways to finance trade transactions are relevant as the banks are intermediating the flow of money in both occasions, but there is further clarification required to understand their roles.

The Wolfsberg Group (2017), a non-governmental association formed by thirteen global banks, has defined trade finance as "the provision of finance and services by financial institutions for the movement of goods and services between two points, either within a country or cross border" (p.6). As trade transactions are generally between a buyer and a seller, who in some cases may not have conducted any business with each other before, they are in search of further trust between them before conducting a transaction by including banks as intermediates. In many occasions, the buyer is not willing to pay for goods until they are shipped or received, while creating a demand for the seller to have some assurance in the form of trade finance (Naheem, 2017). Some of the standard trade finance products offered by banks include Documentary Credits, Documentary Bills for Collections, Demand Guarantees and Standby Letters of Credit, which are accompanied by other trade related documents such as invoices, transport documents or certificates of origin (The Wolfsberg Group, 2017). Due to the fact, that banks are not involved with the actual shipment of goods and services, and neither on the inspection of them, the important role for banks is to examine the consistency of information provided on these varying credit and trading documents. Furthermore, as a characteristic of trade finance transactions, there are usually many parties involved in the process of assessing credit and trading documents, in which the correspondent banking networks become essential. A correspondent bank can be defined as a financial institution providing account services to other financial institutions with the purpose of intermediating third-party payments and trade finance transactions, but also offering cash clearing, liquidity management, and also credit or investment facilities in another currency (The Wolfsberg Group, 2017). As an example, a correspondent bank might have agreed on a deal with a respondent bank to wire transfers or submit trade finance documents on behalf of the respondent bank's customer to another counterparty. The inclusion of trade finance products in a particular transaction provides an opportunity for a bank to make a closer investigation on the contents of

the trade agreement increasing the probability of discovering any suspicious activity. Despite the fact that documentary trading provides more information on a trade transaction, only 20% of world trade is financed by this method leaving the major part of transactions outside this type of monitoring.

In most cases of international trade, the trading parties do not require any credit facilities from banks in order to successfully complete trade deal. This is called trade in open account terms. Under this mechanism, the buyer and seller commonly accept on the trade terms, and the transfer of money is arranged as a clean or netting payment by using the formal banking system (The Wolfsberg Group, 2017). In general, it can be expected that such trading relationship is built on trust, and due to the nature of the relationship there is no need for an intermediary. The open account trade provides serious difficulties for banks to conduct any further assessment related to anti-money laundering efforts, when the clean payment does not offer additional information of what are the underlying reasons for particular transactions (The Wolfsberg Group, 2017). The execution of open account payments provides a channel for traders of goods or services to implement previously mentioned TBML techniques, including the phantom shipments, to make an invoice fraud and by creating a credible cover for an underlying payment. Without any supporting documentation, there are less risk indicators of how a bank could identify and to further understand the reasoning behind this type of transaction, when the bank is only left to rely on its standard anti-money laundering procedures (The Wolfsberg Group, 2017). Additionally, the opportunity to create a falsified invoice increases the risks of two parties colluding with each other, and by the use of complex corporate structures the trading parties can also be controlled by the same individuals.

1.5 Research Objective

There exists an increasing concern on the next trends of how criminals are exploiting financial system for their own benefit, as for example brought to attention by the release of Panama Papers and Paradise Papers in the recent past. As discussed earlier, TBML is one of the most attractive ways for criminals today to hide their illicit gains, and their money laundering mechanisms still rely on the use of the financial system. Therefore, the objective for this research is to increase awareness on TBML methods solely from an anti-money laundering perspective, and especially in the context of financial institutions. The research question can be specified as identifying potential TBML red flag indicators, also defined as risk indicators, of how a financial institution can detect TBML methods, and most importantly the research aims to discover best practices of controlling these risks within financial institutions.

The research is conducted by requesting internationally operating financial institutions to reply on the research questionnaire. For the purpose of this questionnaire, several TBML red flags were collected from available resources and the research respondents were asked to share effective measures to control each of

these TBML risks based on their experience. In order to achieve more holistic understanding of TBML controls and to increase incentives for respondents to share their knowledge, the complete anonymity for their responses was ensured. As one of the research goals was to increase awareness and to share knowledge within the financial industry, the information related to best controls were meant to be publicly shared in order to improve TBML controls in every financial institution.

This master's thesis is structured to next shift focus on theoretical background on the role of risk management in banking, especially focusing on AML as part of the operational risks. Theoretical background further touches upon the concept of asymmetrical information and how AML efforts can be considered as a task for banks to resolve problems related to adverse selection and moral hazard. Then, this master's thesis continues to discussion over sound management of money laundering risks, and what are the key elements of managing TBML risks within financial institutions. The focus is on internal processes and governance, as risk assessment, customer due diligence, ongoing and transaction monitoring, three lines of defence, and the role of correspondent banking and trade finance providers are introduced. After representation of research data and methodology, the master's thesis moves on to the main findings in form of questionnaire results and their analysis. This segment introduces all the red flags collected from different AML publications and their matching controls defined by the research respondents. After the analysis segment, the research is concluded with summarization of key findings of how TBML can be mitigated within banks and what are the next steps of fighting against this mechanism. Furthermore, the research questionnaires are included in the Appendices.

2 THEORETICAL BACKGROUND

2.1 Risk Management of Money Laundering in Banking

An initial step to any money laundering operation is committing to a predicate offence, which may vary from drug trafficking to trading of illegal weapons and eventually targeting to illegal profits. Through the act of money laundering, which can be defined as the process of disguising the illicit origin of criminal proceeds, it becomes possible for the criminal to acquire profits without revealing the source of its criminal proceeds (FATF, 2019). Due to the fact that the predicate offences for money laundering can be exploited by a wide range of criminals including organized crime groups and white-collar criminals, the possible damage created by successful money laundering operations can truly carry serious con-

sequences for the society as a whole. It wasn't until the mid-1990s, when the globalization of financial markets shifted the problem of money laundering from domestic authorities to international scale, as the national borders didn't control the movements of money anymore and as the financial system became globally interconnected (Bergström, Helgesson & Mörth, 2011). Due to the existence of diverse legal and financial systems around different countries, the global response on the issue included the establishment of the Financial Action Task Force (FATF) in 1989 and its 40 recommendations were designed to set international standards to combat against money laundering (FATF, 2012). One of the most influential responses to combat this issue has been the criminalisation of money laundering, where several governments have taken steps to combat money laundering by establishing effective anti-money laundering regimes (FATF, 2019). Such regimes include both the governmental and the private sector awareness of tackling the problem, where regulatory tools such as giving investigative powers to authorities for confiscating criminal proceeds and building the framework for exchange of information between different stakeholders are aimed for fighting this problem (FATF, 2019). Traditionally, the role of fighting against problems such as money laundering has been the responsibility of sovereign governments, although recently the private sector mainly in the form of banking sector has gained higher importance on anti-money laundering efforts.

The underlying change in roles between public and private sector regarding anti-money laundering efforts has been mainly driven by the development of modern states towards regulatory states. As stated by Bergström et al. (2011), "regulation of risks becomes the most important tool for governance in a situation when the power of states is transformed", particularly when states continue liberalizing the public sector, meanwhile opening up opportunities for the private sector (p. 1046). In terms of anti-money laundering efforts, some authority from the public actor has been outsourced to the private actor, which raises a problem for the public actor of how to make the private actor accountable for the decisions it makes (Bergström et al., 2011). This setting is described by Bovens (2006) as the relationship between "an actor and a forum, in which the actor has an obligation to explain and justify his or her conduct, the forum can pose questions and pass judgements, and the actor may face consequences" (p.9). In such setting, an actor is entitled as the banking sector and a forum as the regulating authorities. From a banks' perspective, the increased accountability of anti-money laundering efforts leads into increased costs and on the other hand may lead into direct reduction of revenues. Due to the fact, that banks may not have financial incentives to control money laundering, the response on controlling this dilemma is offered in the form of risk-based approach in anti-money laundering regulation. One argument for creating the risk-based approach is that while authorities lack information from private sector – banks – have much better access to it and by monitoring their client information may be, if correctly motivated, more efficient in revealing criminals (Bergström et al., 2011). In addition to shifting information gathering to private sector, the risk-based approach has also given banks new

responsibilities on setting standards and goals for dealing with customers. According to Bergström et al. (2011), the risk-based approach "presupposes the existence or establishment of routines and systems that react whenever a customer makes transactions that are out of the ordinary", and "it further creates a need to find or construct standards of normality that can be applied to day-to-day operations" (p. 1051). This role as a standard setter can function as a sufficient control for anti-money laundering purposes, but on the other hand, it can create problems for some customers even though no criminal action is observed as banks have the power to rule out transactions which they interpret as suspicious (Bergström et al., 2011). Additionally, one of the characteristics of introducing risk-based approach is the rule for Customer Due Diligence (CDD) and risk assessment, and as the banks are expected to complete their own quality assurance, "this extra burden on the private sector is turned into benefits regarding reputational benefits or rather avoidance of reputational risks of not fulfilling the international requirements as drawn up mainly by the FATF and the BCBS" (Bergström et al., 2011). Consequently, as the transfer of responsibility has created new roles for the private sector, it is evident to demonstrate how the public and private sector have cooperated on these duties in the recent past.

In the field of financial crime prevention there have been numerous well-known cases where financial institutions have not succeeded in their obligations of controlling money laundering, which have evidently required a strong response from public authorities. One of the most prominent events occurred in Latvia in 2018, where the country's third largest bank ABLV Bank Latvia was indicted for institutionalized money laundering by the US Department of the Treasury due to transmitting illicit payments by entities under sanction exposure from countries such as North Korea, Azerbaijan, Russia and Ukraine (Neale, 2019). The accusation for institutionalized money laundering made the US authorities to appeal on Section 311 of the USA Patriot Act, which closed down the correspondent banking accounts of ABLV and as an immediate effect caused a bank run among depositors eventually leading into closure of the bank (Neale, 2019). The year of 2018 included another significant event in the field of enabling financial crime through financial institutions as Denmark's largest bank was accused of money laundering. According to the report by Danske Bank in September 2018, the total of $235 billion of suspicious transactions from former Soviet Union countries were transmitted in Danske's Estonian branch between the years of 2007-2015 (Neale, 2019). The customer group in question was the non-resident clients of Estonian branch and suspicions were also raised due to the use of corporate structures such as Scottish Limited Partnerships and UK Limited partnerships, which can be designed to hide the true beneficial owners of the parties making these transactions (Neale, 2019). The authorities have responded with criminal charges and investigations at least in Denmark, Estonia and also in the US, where prosecutors accuse Danske from failing to investigate and report suspicious transactions as they are obliged to and so that the bank's controls were not sufficient for their high-risk customers (Neale, 2019). Additionally, the scandal of Danske Bank has caused its correspondent banking partner Deutsche Bank to be involved in

the money laundering mechanism, as its US subsidiary is suspected of processing approximately four-fifths of the $235 billion worth of suspicious transactions (Neale, 2019). It has been estimated that including the flow of suspicious transactions from Danske and also other financial crime related issues, "Deutsche Bank has spent more than $18 billion paying fines and settling legal disputes since the start of 2008" (Matussek, Comfort & Arons, 2018). These cases have proven that the prevention of financial crime has to be organized sufficiently, and if a financial institution is not able to comply with its obligation of preventing financial crimes, the consequences may include facing fines, criminal charges and even closing down of their business.

The management of money laundering risks can be listed as one of the risk management roles banks are facing in addition to controlling other types of risks. In order to discuss the specific risks of TBML a clarification should be made on risks in the context of risk management in banking. In a broad sense, risks can be defined as "uncertainties potentially resulting in adverse variations of profitability or in losses", and as the main objective for banks is to maximize profits and shareholder value, there are incentives to avoid realization of risks (Bessis, 2009, p. 25). It should be clarified that risk and uncertainty do not carry a similar meaning, as the uncertainty should be interpreted as "the randomness of certain outcomes" and the risk as "the adverse effect on wealth that such outcomes have" (Bessis, 2009, p.26). Even though other types of risks in banking, such as credit risk or foreign exchange risk, might be easier to quantify and to assess the effect on wealth, it has been observed that also money laundering risks may have a very large impact to bank profitability. As an example, in the money laundering context a revelation that a bank has been exploited by criminals for channelling illicit funds with or without the knowledge of the bank can have a severe effect on the share price and on the profitability of the bank. In order to prevent realization of risks, the core element for any bank is to maintain effective risk management and to implement accurate controls. As stated by Bessis (2009), "the goal of risk management is controlling risks", and the "control is feasible when quantitative and qualitative assessments of risks exist" (p.37). The development of banking regulations has been a driver for quantifying different types of risk, and as the goal has been to set minimum capital requirements to match different levels of risk also the money laundering risks have been included as a part of the operational risks.

One important group of risks faced by banking institutions is related to operational risks, and as these risks are varied from employee misconduct to technological deficiencies, there exists a growing interest towards controlling operational risks. According to the definition by the Basel Committee on Banking Supervision (2017), operational risk contains "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events", which includes the risks of money laundering (p. 128). Due to the extensive nature of operational risks, possible losses for banking institutions may be incurred

from different sources, and the emphasis should be on improving internal processes and systems. As stated by Bessis (2009), "in the absence of an efficient tracking and reporting of risks, some important risks remain ignored, do not trigger any corrective action, and can result in disastrous consequences" (p.35). This forms the justification for capital requirements under the Basel requirements, which entails the quantification of operational risks. Furthermore, in contrast to credit or market risk, quantifying operational risks bears difficulties as "most risk factors usually identified by banks are typically measures of internal performance, such as internal audit ratings, volume, turnover, error rates and income volatility, rather than external factors such as market price movements or a change in a borrower's condition" (Casu, Girardone & Molyneux, 2006, p. 305). The identification of such risk factors provides difficulties to determine what level of operational risks are faced by a particular banking institution, and what is the level of capital charge assigned to operational risks. In general, operational risks may not be interpreted as financial risks as the main source for such risks is the failure in internal processes (Bessis, 2009). For the purpose of uncovering reasons for capital requirements and for justification of banking regulation, further discussion should be made on the risk measurement and management of banks.

Risk management in banks is essential for controlling against unexpected losses derived from operational risks in which both external and internal requirements influence banks in the form of regulation and risk management. A key part of risk management is development and application of risk measurement methods, which is also related to the capital requirements for banks. As defined by Cumming & Hirtle (2001), "risk measurement entails the quantification of risk exposures" and based on the variety and complexity of risks it may result in forms such as stress scenario or value-at-risk analysis (p.2). Furthermore, the general definition in the financial world for risk exposure is indicated to "a transaction which generates some risk", which can be defined "as the amount of risk, or an amount subject to loss of value, or the size of commitments" (Bessis, 2009, p.26). Due to the broad range of risks categorized under operational risks and the complexity of quantifying each of them, it may become a challenge to estimate risk exposures and there on to set accurate capital buffers for banks. Nonetheless, an inevitable need for quantifying risks not only serves as a basis for capital requirements but it also serves as a foundation for risk management in banking. In the banking context, risk management "refers to overall process that a financial institution follows to define a business strategy, to identify the risks to which it is exposed, to quantify those risks, and to understand and control the nature of the risks it faces" (Cumming et al., 2001, pp. 2-3). The risk measurement functions as a part of the comprehensive framework that is required from the risk management as the intention is to include all business lines and their related risks in the risk evaluation process to prevent any losses to a business as a whole. Although the quantification of operational risks, including the risks for money laundering, may be challenging for banks the Basel Committee has proposed alternative approaches to maintain capital adequacy within banks in order to prepare against possible realization of risks.

One of the regulatory instruments held by the financial regulators is the introduction of capital requirements, which aims to set adequate capital buffers against those characteristic risks each bank carries in their operations. The justification for public regulation is derived from the potentiality of market failure that can be caused by banks, which can be a result, inter alia, of the size of bank operations, externalities or due to asymmetric information between market participants (Freixas & Rochet, 2008). The existence of such risk factors necessitates an implementation of regulatory capital requirements, in which the Basel 2 Accord has provided three following approaches to prepare against possible losses; the basic approach, the standardised approach and the internal measurement approach. According to the basic approach the capital requirement is tied to a single factor serving as a proxy for the risk exposure, and if for example a gross income is chosen as the factor the expected capital preserved against operational risks should be equal to a standard percentage of the gross income (Bessis, 2009). In general, the basic approach takes into account overall risks a bank is bearing, and the other approaches will add further sophistication to that approach. In the standardised approach bank operations are split into specific business lines, and "within each business line, the capital charge is a selected indicator of operational risk times a fixed percentage (beta factor)", in which both the indicator and the beta factor can be different depending on the line of business (Bessis, 2009, p. 252). For the third approach, the Basel Committee proposes the use of bank's internal data to determine the adequate level of capital. The internal measurement approach introduces a loss distribution estimation, where the following inputs are required for the business lines and for related risks; "an operational risk exposure indicator, the probability that a loss event occurs and the losses given such events" (Bessis, 2009, p. 252). In practice, the supervisor determines the exposure indicator based on the specific business line's risks, and the other two components are derived from banks internal data (Casu et al., 2006). As a result, all the approaches aim to determine the capital buffers required for potential losses, and as the complexity of banking activities increase, also the added sophistication on the capital requirement model may provide more accurate approximation of actual risks.

It can be generally stated that prevention of financial crime risks has not previously been in the core of banking risk management on the same scale as for example risk management of market and credit risks, and as these risks are significantly different in their nature, they also need different risk management approaches. Credit risk can be traditionally defined as a borrower risk in which the counter party potentially fails to meet its obligations on agreed terms, and from the bank's perspective the successful credit risk management includes maximizing the risk-adjusted rate of return while maintaining the credit exposure at acceptable level (Basel Committee on Banking Supervision, 2000). Additionally, the exposure and the possible losses that adverse market movements can generate to on and off-balance sheet positions of the bank can be defined as market risks (European Banking Authority, 2018). Both credit and market risk differ from

money laundering risks as the tools for mitigating the former risks include some innovative products and techniques that have been evolving within the industry for years. For example, some of the risk management tools that may reduce risk positions, if the risks are identified early enough, include "such mechanisms as loan sales, credit derivatives, securitisation programs and other secondary loan markets" (Basel Committee on Banking Supervision, 2000, p. 17). As the credit and market risk exposure may be reduced by purchasing a derivative contract fitting one's purposes similar tools are not available for the reduction of money laundering risks. From the financial institution's perspective, the potential money laundering occurs amongst the countless number of financial transactions, which are transferred through banks on a daily basis, and which may involve unidentified and illicit financial flows. In modern times the financial transactions are mostly completed in digital forms, and consequently it has become an industry standard for financial institutions to focus on computer systems in order to identify and verify their customers, transactions and other counter parties (Budik & Schlossberger, 2015). As the search for a transaction that might potentially be considered as money laundering may feel like finding a needle in a haystack, those suspicious transactions that do not fit the customer profile can be investigated by the use of computer systems and by developing its algorithms (Budik & Schlossberger, 2015). Therefore, the risk management framework is required to be extended among banks as the risks of money laundering are not mitigated by using the same set of tools as with the mitigation of credit and market risks.

2.2 Asymmetric Information

The existence of banks is mainly derived from their core function as financial intermediators between depositors and borrowers, and as the need for such intermediation arises banks are also required to deal with informational asymmetries when completing financial transactions. A financial transaction always includes at least two parties, and due to the inability for two parties to hold the same amount of information on the transaction and on the opposing party, there exist problems that banks aim to solve within the financial intermediation process. As stated by Casu et al. (2006) there are at least three problems related to information in transactions; "not everyone has the same information, everyone has less than perfect information, and some parties to a transaction have inside information which is not made available to both sides of the transaction" (p.9). It can be argued that banks are incapable of holding all the relevant information of a transaction, but simultaneously the existence of asymmetric information provides a justification for financial intermediation as the banks can solve these problems more efficiently. Asymmetric information is traditionally discussed in the financial literature as a part of the credit intermediation process, where borrowers and lenders carry different information sets on each other. In such a context, borrowers may have incentives to provide only favourable information to the lender about an upcoming project, and on the opposite side the lender may have diffi-

culties to determine the true characteristics of the borrower as acquiring and verifying that information may be costly or even impossible (Leland & Pyle, 1977). These similar incentives to provide favourable information from customer's side are not only relevant in the credit intermediation process, but they are also relevant in the assessment of customer behaviour in the anti-money laundering context. Due to the existence of asymmetric information in all transactions, financial institutions are required to design their financial arrangements and risk management processes in a way that limit opportunistic behaviour from their customers (Casu et al., 2006). In order to discuss more thoroughly about the problems posed by asymmetric information, the discussion should be shifted to problems related to a transaction before and after it is completed.

A problem or set of problems that may arise prior to a transaction is completed, and which are associated with asymmetric information, are generally referred to as adverse selection problems. As defined by Darrough & Stoughton (1986), adverse selection can be referred to as hidden information, and its "problems arise when the agent has more information than the principal" (p. 501). Adverse selection is characteristically a concern in the search or verification stage of a transaction (ex-ante), in which one party is inclined to use its informational advantage in an attempt to manipulate the other party to complete a transaction, meanwhile steering the decision away from what would be mutually expected under perfect information conditions (Casu et al., 2006). The adverse selection problem applies to money laundering context, as the potential money launderer, as an agent, has clear incentives to exaggerate all the positive factors about its business in order to make financial institution, a principal, to accept illicit funds and transfer them forwards. In the research conducted by Akerlof (1970), the adverse selection problem was demonstrated in the context of used-car market, where the seller of a used-car had the informational advantage over the potential buyer and had the beneficial position to exaggerate that car's quality. The sellers in other words had the knowledge whether their car was a bad car, or a lemon as entitled in the research, and it would require a test drive and closer examination from the buyer to acquire the same information (Akerlof, 1970). Due to the fact that the buyer cannot tell the difference between a good or a bad car, market prices are same for all types of cars, which may push away honest sellers from the market due to the low price in the market associated with risks for buying a lemon (Akerlof, 1970). In general, the ability for one economic agent to exploit its informational advantage over the other party can distort the market price, increase the transaction costs and increase the number of dishonest actors in the market. In response to adverse selection problem it is a central function for financial institutions to try to understand the incentives of the other party, and to mitigate the ex-ante risks of a transaction. In this research we are focusing on signals – red flags – warning of potential money laundering and illicit behavior before and after a transaction is completed.

The asymmetric information problem related to a transaction after it has been completed is referred to as moral hazard (ex-post) problem, which is relevant for

credit issuance and also in the anti-money laundering process for banks. By the definition, the moral hazard refers to hidden action which "arises when the action undertaken by the agent is unobservable and has a differential value to the agent as compared to the principal" (Darrough et al., 1986, p. 501). In the money laundering context, such moral hazard problem arises for instance when a customer as an agent first attempts and then succeeds to open an account with the purpose of moving illicit funds via financial system, in which the bank as a principal has no understanding of the agent's true incentives. It can be argued that the opportunity for one party to use superior information for its own advantage, while risking the interests of the other party, are central in identifying moral hazard behaviour (Casu et al., 2006). In addition to the money laundering example, the moral hazard problem is more closely researched in the context of credit intermediation in the financial literature as the issuance of a loan provides incentives for the loan-applying agent to exploit its position. As a standard example, an agent seeking financing for a project may exaggerate its profits or minimize probability for its failure, while providing difficulty for a lender to verify the actual situation, and if the loan is eventually granted, there may exist incentives for the borrower to change its behaviour towards more riskier activities, while causing a moral hazard problem for the bank (Matthews & Thompson, 2005). In order to control against the risks exposed by moral hazard, especially as the focus is in money laundering issues, financial institutions are required to implement controlling activities both ex-ante and ex-post of transactions to mitigate agent's incentives for pursuing personal interests over the principal's interests. In terms of opening an account or issuing a loan, the moral hazard problem is associated with monitoring and enforcement activities of a bank after the transaction has been generated, which in response requires banks to get involved with monitoring activities (Casu et al., 2006). In connection with this research, the red flag indicators are intended to reveal the asymmetric information problems encountered by banks, and for the mitigation of red flags there are control measures, monitoring activities as one of them, that are intended to prevent these problems.

The justification for financial institutions to monitor their customers' activities is derived from the existence of asymmetric information problems, and due to the fact that potential change in the customer behaviour may expose a bank to new risks. In the context of financial intermediation theories, the role of delegated monitoring has been assigned to banks as recommended by Schumpeter (1939), when "the banker must not only know what the transaction is which he is asked to finance and how it is likely to turn out but he must also know the customer, his business and even his private habits, and get, by frequently talking things over with him, a clear picture of the situation" (p.116). This ability to acquire information on the customers partly explains the demand for indirect finance in form of bank loans, and while compared to direct forms of finance may provide cost advantages in the monitoring of a financed project. In traditional sense of indirect finance, banks aim to resolve the similar incentive problems posed by both depositor-intermediator and also individual borrower and lender relation-

ships, and as a result the ability of diversification through financial intermediators enables the reduction in incentive problems and makes it more feasible for borrowers to entrust monitoring activities of borrowers to banks (Diamond, 1984). The possibility of diversification of depositor's funds through banks provides a reason for outsourcing the monitoring activities, although the requirement for banks to monitor its borrowers is obtained from several factors. When a financial contract is assigned between a bank and its customer, monitoring ensures that gaps in asymmetric information are not exploited for personal interests, and also that the behaviour of another party is consistent based on the discussions and the information provided (Casu et al., 2006). Furthermore, the true value of a contract cannot be determined in its initial stage and due to the frequent nature of long-term financial contracts, monitoring of ex-post behaviour of a counterparty is required, as the initial conditions are rarely maintained, in order to determine the eventual value of the contract (Casu et al., 2006). A similar argument can be applied in the context of anti-money laundering as there are unique characteristics to banking needs and their duration for each customer, while customer's actual behaviour may be in imbalance with the information held by the bank. The list of red flags provided in this research represent the currently acknowledged risk indicators for potentially suspicious behaviour, and although the listing is not exhaustive as there are new risks constantly rising, the potential threat of customers exploiting financial system according to their personal interests has to be eliminated by appropriate control measures.

3 SOUND MANAGEMENT OF MONEY LAUNDERING RISKS

3.1 Risk Assessment

It has been commonly acknowledged that the effective management of money laundering risks in banks is constructed around the risk-based approach (RBA) and how it is applied to banking operations. According to the RBA definition in the FATF guidance (2014) "financial institutions are expected to identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively" (p.6). The definition of RBA sets the foundation of how banks should establish their risk management process, and due to the fact that banks have varying business models, also the risks related to money laundering are specific to each institution. The identification of relevant risks and the development of appropriate controls should lead the way of how "banks allocate their compliance resources, organise their internal controls and internal structures, and implement policies and procedures to deter and detect ML/TF" (FATF, 2014, p.17). In the context of TBML risks, it should be emphasized there are certain banking segments, including retail, corporate and correspondent banking, that contain the highest amount of

risks related to TBML. In the process of developing sound risk management to TBML risks, the banks are expected to apply RBA to the specific products and services provided by their institution, which should be taken into consideration in their comprehensive risk assessment.

Risk assessment is an essential part for evaluating money laundering risks, and it functions as a result from applying the RBA. In Finland, the obliged entities under the Act on Preventing Money Laundering and Terrorist Financing are required to include in their risk management process identification and assessment of money laundering risks. Financial institutions are included as obliged entities, and therefore all the operators in the banking sector are entitled to conduct the risk assessment. Based on a holistic approach to banking operations, "a bank should consider all the relevant inherent and residual risk factors at the country, sectoral, bank and business relationship level, among others, in order to determine its risk profile and the appropriate level of mitigation to be applied" (Basel Committee on Banking Supervision, 2017, p.4). The banks that are most vulnerable to TBML risks have a tendency to operate in several jurisdictions, which results in more careful evaluation of potential risks that has to be matched with appropriate controls. In the risk assessment, "a bank should develop a thorough understanding of the inherent ML/TF risks present in its customer base, products, delivery channels and services offered (including products under development or to be launched) and the jurisdictions within which it or its customers do business" (Basel Committee on Banking Supervision, 2017, p.4). In the context of TBML risks, the previous categorization of red flag indicators to five groups aims to cover the relevant risks related to TBML, and it can function as a basis for drawing the risk assessment.

The red flag indicators were divided into five categories based on the relevant risks specifically related to TBML, and in addition to the red flags banks should assess how vulnerable their provisions of financial services are to these risks. Since open account payments are the main facilitators of illicit money that are being washed by TBML methods, all the banks offering payment services are required to identify and assess TBML risks in their risk assessment. The high volume of transactions, inclusion of cash-intensive businesses and wider offering of services within retail banking sector provides a clear threat to potential TBML abuses, and the risk assessment related to such activities should be conducted with discretion (FATF, 2014). Furthermore, the offering of transactional and credit services in the form of trade finance facilities poses clear TBML vulnerabilities for the corporate banking sector. In addition to the retail and corporate banking, also the banking activities within correspondent banking are faced with higher TBML risks. The nature of such services includes transactions in high values, restricted amount of information in payment transactions, several jurisdictions that might not comply with AML recommendations and provision of trade finance services (FATF, 2014). Based on the listing of potential red flags, it can be stated that most of the risk indicators are related to retail, corporate or correspondent banking activities, which further emphasizes the need to evaluate

money laundering risks as identified within internal processes and also as observed from external sources.

The end results from the risk assessment process is that banks fully understand the money laundering risks encountered by their institution, and in order to implement any mitigating measures to combat these risks, they should be fully aware of their risk profile. There are several information sources that are expected to be used including "information obtained from relevant internal and external sources, such as heads of business, relationship managers, national risk assessments, lists issued by inter-governmental international organisations and national governments, AML/CFT mutual evaluation and follow-up reports by FATF or associated assessment bodies as well as typologies" (FATF, 2014, p.18). Both internal and external information should be constantly assessed, and controls implemented since money launderers are also continually modifying their operations and banks can quickly be faced by new money laundering threats. The basis for effective risk management policies and procedures is that banks fully understand the relevant risks, and that this information should then be applied to implementation of accurate controls for customer due diligence, monitoring and customer acceptance processes (Basel Committee on Banking Supervision, 2017). In addition to the concepts of fully understanding TBML risks and applying RBA, another essential dimension for sound risk management is the customer due diligence process.

3.2 Customer Due Diligence

In the fight against money laundering through financial system, it has become an inevitable task for every bank to complete the Customer Due Diligence (CDD) process for each customer, and it should be conducted having bank's risk characteristics in mind as described in the risk assessment. The underlying idea for designing the CDD process is that banks understand their customers, know deeply enough characteristics of the actual customer business and behavior and for what purposes they need banking services (FATF, 2014). In the context of CDD, Basel Committee on Banking Supervision (2012) has stated in its Core Principles, that banks should "have adequate policies and processes, including strict customer due diligence rules to promote high ethical and professional standards in the financial sector and prevent the bank from being used, intentionally or unintentionally, for criminal activities" (p.13). This statement emphasizes the importance of CDD as a prevention mechanism for potential money laundering, and on a global scale the FATF standards are intended to set the common rules for different jurisdictions. In the light of FATF recommendations, a bank should carry out CDD measures when a customer, referred to as an entering party for a business relationship or issuing an occasional financial transaction with a bank, interacts with this bank, which triggers the need to identify and verify the identity of the customer and its beneficial owner (FATF, 2012). For successful comple-

tion of CDD measures, it is important that in addition to the customer, also beneficial owners or any other persons conducting transactions on behalf of the customer are included in the CDD process.

The concept of RBA is highly relevant in the CDD process, and when all customers are required to go through the CDD process also the application of CDD measures should be estimated based on existing risks. In general, all the information required from customer for the completion of CDD and to what extent this information has to be verified should be commensurate to the level of risk caused by the customer relationship (FATF, 2014). According to the idea of RBA, it is evident that not all customers carry the same level of money laundering risks which is the reason why different business relationships should be faced with different levels of due diligence measures. After a bank determines to what extent it is required to obtain information from a customer, also the level of verification measures should be estimated accordingly. In the CDD process, the verification should be completed by "using reliable, independent source documents, data or information", and especially in the case of documents "a bank should be aware that the best documents for the verification of identity are those most difficult to obtain illicitly or to counterfeit" (Basel Committee on Banking Supervision, 2017, p.8). Based on the red flags of TBML, there are several potential risks involved with false documentation for identity, invoices and trade documents, which should elevate the level of awareness when conducting CDD process. The level of required CDD measures can be varied from simplified due diligence process to enhanced due diligence (EDD) process, and the latter process in particular might be applied in possible TBML cases. The EDD process might be relevant for customers facing TBML risks since they carry higher risks related to complex corporate structures, opaque shipment structures and to jurisdictions that have serious AML deficiencies, and the possible risks might require more strict application of due diligence measures (Basel Committee on Banking Supervision, 2017). The CDD process is an essential part of controlling money laundering risks, as based on the obtained information, the customer risk profile can be estimated, and based on the expected customer behaviour the probability of tracing suspicious activities can be increased.

In the process of identifying and verifying customer information, it is important to notify that the level of required information is associated with the risk profile of a customer. When business relationship or customer's occasional transaction is assessed, banks normally collect information on the purpose of customer relationship, size of the underlying transaction and regularity of the relationship in order to understand the behaviour of each customer (Basel Committee on Banking Supervision, 2017). The type of information required from customer should not be restricted to any of the previously mentioned information, and instead banks are expected to apply RBA to determine the sufficient level of customer information. Therefore, the key components for assessing risk profiles are "the level of risk associated with the customer's business model and activities as well

as the financial products or services requested by the customer" (Basel Committee on Banking Supervision, 2017, p.8). Before establishing business relationship or occasional transaction, banks should be aware of what is expected to be normal behaviour for each customer, and what are the underlying reasons for using particular financial products and services. The risk profiling measures are expected to change depending on the banking segment, and for example in the retail banking where customer base is wide, risk profiles can be applied either in individual level or in customer groups containing similar risk characteristics such as income levels or types of transactions (FATF, 2014). The objectives for risk profiling are diverse, as it is expected to be a medium for identifying normal and then suspicious customer behaviour, it defines whether EDD measures should be applied, and also any collected information should be reflected on updating bank's risk assessment (Basel Committee on Banking Supervision, 2017). After the completion of risk profiling, from the perspective of anti-money laundering it is important to determine the reasons for maintaining any business relationship, and therefore the focus should be shifted towards ongoing monitoring.

3.3 Ongoing Monitoring & Suspicious Transaction Reporting

The identification of potential TBML red flags requires banks to carry out strict ongoing monitoring for customer behaviour and their transactions so that the bank is not exploited for criminal activities. According to the definition by the FATF (2014), "ongoing monitoring means the scrutiny of transactions to determine whether those transactions are consistent with the bank's knowledge of the customer and the nature and purpose of the banking product and business relationship" (p.21). Ongoing monitoring is a continued effort after the risk assessment and the CDD process, and its main purpose is to evaluate transactions against the normal and suspicious behaviour of a certain customer. Due to the high amount of transactions, "bank can only effectively manage its risks if it has an understanding of the normal and reasonable banking activity of its customers that enables the bank to identify attempted and unusual transactions which fall outside the regular pattern of the banking activity" (Basel Committee on Banking Supervision, 2017, p.10). Without obtaining accurate customer information, the ongoing monitoring does not provide sufficient results and banks become more vulnerable for being abused. For the basis of developing monitoring efforts banks should apply the RBA to determine the level of monitoring efforts for each business relationship. This implies that higher risk customers, based on the risk assessment and CDD efforts, should be included in enhanced monitoring process, and the monitoring frequency should be commensurate with the level of risks (Basel Committee on Banking Supervision, 2017). As the goal is to capture potential red flags of suspicious behaviour, banks are required to conduct relevant scenarios within their monitoring process to detect such behaviour.

It has become a common standard for banking sector to maintain monitoring systems which enable banks to meet their obligation of detecting suspicious customer behaviour. The detection of unusual activities is dependent on the risk scenarios that banks are obliged to define, and in general it means what type of behaviour is expected to be unusual for each customer. To the extent of identifying such activities, "a bank should consider the customer's risk profile developed as a result of the bank's risk assessment, information collected during its CDD efforts, and other information obtained from law enforcement and other authorities in its jurisdiction" (Basel Committee on Banking Supervision, 2017, p.10). As a general flow of information, when authorities discover new TBML threats, a bank should estimate that threat according to its risk assessment process and to implement possible scenarios for corresponding group of customers that are vulnerable to the new threat. It has become evident based on the TBML red flags that in many occasions' customer behaviour might raise suspicions, whether transaction does not make any economic sense or otherwise does not match the normal customer behaviour, when CDD information and customer behaviour provide clear discrepancies. In relation to the risk assessment, information about a new threat might be received from any possible resource, and it is important to identify customers, accounts, transaction patterns and products under the threat, and followed by applying relevant monitoring controls (Basel Committee on Banking Supervision, 2017). The ongoing monitoring is not mandated to be electronically operated, but due to the high volume of transactions especially in retail banking, it might be the only possible solution to accurately identify suspicious activity (FATF, 2014). It should also be clarified that not all transactions determined suspicious under risk scenarios are signs of illicit activity, and if after further investigation a transaction is considered illegitimate, it should be reported to investigative authorities.

There is a common requirement within the banking sector that transactions, that are eventually determined as suspicious activity by banks, has to be reported to the relevant authorities and to be processed for possible criminal investigation. As stated in the FATF (2012) recommendation, "if a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit" (p.17). In order to successfully apply this recommendation into bank practices, it requires banks to efficiently arrange the policies and procedures for collection of customer information, and to develop effective monitoring systems. According to the Basel Committee on Banking Supervision (2017), "ongoing monitoring and review of accounts and transactions will enable banks to identify suspicious activity, eliminate false positives and report promptly genuine suspicious transactions" (p.11). Based on the estimated risk scenarios, the monitoring systems are also expected to raise false positives which are possible illicit activities, but in banks' further investigation determined as normal transactions. There is a requirement for banks to create policies and procedures to clearly inform employees how suspicious transactions are analysed, on what terms these transactions are reported to

the authorities and how promptly the report should be processed to the authorities (Basel Committee on Banking Supervision, 2017). In the context of TBML, banks are required to be aware of the potential red flags before these possible risks can be implemented into monitoring systems, before any further investigation for suspicious activity can be processed forwards.

3.4 The Three Lines of Defence

In the process of applying effective risk measures to combat against money laundering, one of the major components is the successful implementation of governance arrangements. In relation to the governance structure, an introduction should also be made to the concepts of risk appetite, and furthermore on risk appetite framework within a banking organization. According to the Basel Committee on Banking Supervision (2015), risk appetite is defined as "the aggregate level and types of risk a bank is willing to assume, decided in advance and within its risk capacity, to achieve its strategic objectives and business plan" (p.1). Furthermore, the perceived risk appetite should be transformed to actual risk appetite statement that is "the written articulation of the aggregate level and types of risk that a bank will accept, or avoid, in order to achieve its business objectives", and as it should include quantitative measures, it should also include qualitative statements in relation to prevention of money laundering (Basel Committee on Banking Supervision, 2015). The assessment for risk appetite statement should function as a basis for constructing a holistic risk appetite framework, which includes "a risk appetite statement, risk limits and an outline of the roles and responsibilities of those overseeing the implementation and monitoring of the risk appetite framework" (Basel Committee on Banking Supervision, 2015, p.2). Due to the scale of banks and their operations that are the most vulnerable to TBML risks, it is important to communicate to all in-house units and their employees in all jurisdictions the defined risk appetite in order to effectively identify and control their risks. There is nothing standard in the way money laundering is conducted, and instead it can be seen as a huge all the time evolving variety of individual specific operations. Nevertheless, a good practice for tackling money laundering is to follow general recommendations confirmed by the Basel Committee in the Bank for International Settlements of how governance structure should be arranged, which can be applied to different types of banks.

The mitigation of money laundering risks within the governance structure has been acknowledged to be constructed around the three lines of defence, where the first line is represented by the business units. In a banking organization, these units are generally close to customers, and due to fact that risks exposed by the customers are evaluated and managed within the unit, they are responsible for the ongoing monitoring as stated according to the risk appetite and other policies determined by the organization (Basel Committee on Banking Supervision, 2015). In the context of TBML risks, the business units carry the highest probability to detect suspicious behaviour before an illicit transaction might be completed. A necessary condition for this is that all banking officers should have the

knowledge of potential red flags of TBML. For this purpose, all the policies and procedures should be in written form, effectively communicated to the staff, and it should be ensured that the staff is sufficiently trained. As there are varying staff functions and experiences, the training should be "tailored to an employee's specific responsibility or function to ensure that the employee has sufficient knowledge and information to effectively implement the bank's AML policies and procedures" (Basel Committee on Banking Supervision, 2017, p.5). Based on the same reason of why the bank risk assessment has to be constantly changed, also the employee training should be adjusted based on the exposed risks involved in a business segment and in a particular position. In addition to the awareness on red flags and internal policies, employees within the business unit should receive procedures for detecting suspicious transactions and for escalating potential illicit transactions to other units or to investigating authorities (Basel Committee on Banking Supervision, 2017). Although business units are responsible for their operations and on the risks related to them, in the context of sound risk management there should also be an independent line of defence to ensure their obligations are fulfilled.

The second line of defence functions as an oversight unit, and as an independent and objective assessor of money laundering procedures, it aims to ensure that AML obligations are sufficiently filled. Traditionally, the unit is comprised of "the chief officer in charge of AML/CFT, the compliance function, but also human resources or technology" (Basel Committee on Banking Supervision, 2017, p.4). The responsibility of compliance with relevant laws and regulations is centralized for the chief AML/CFT risk officer, who is in charge that all the duties are completed in an ongoing basis. These obligations include "sample testing of compliance and review of exception reports to alert senior management or the board of directors if it is believed management is failing to address AML/CFT procedures in a responsible manner" (Basel Committee on Banking Supervision, 2017, p. 5). In addition to acting as a point of contact to the management, the chief officer is also responsible for the communication with internal and external authorities, which also constitutes the responsibility of reporting suspicious transactions (Basel Committee on Banking Supervision, 2017). In the process of internal escalation of suspicious transactions, banks may apply the three lines of defence model to transmit information about suspicious transactions in order to ensure accurate level of reporting to the authorities. In terms of general flow of information, it has been recommended that the detection and investigation of suspicious transactions should be completed within the first line of defence, then escalated to the second line of defence for relevant money laundering risk officer, and if suspicions are confirmed the transaction should be reported to the authorities (The Wolfsberg Group, 2017). An emphasis should be placed on the independence of both the business and the compliance units, and the role of the chief officer is to ensure that there are procedures to solve potential conflicts. Therefore, it becomes important that the chief officer does not hold any responsibilities in any other lines of defence due to the fact that money laundering risks have to be assessed in an objective and unbiased manner to accurately measure the level of

threat (Basel Committee on Banking Supervision, 2017). The completion of the three lines of defence also includes one additional unit that similarly to the second line has to maintain objectivity meanwhile it should focus more on the effectiveness of bank policies and procedures.

The third line of defence, frequently entitled as the internal audit unit, is mainly in charge of measuring the effectiveness of the risk management policies and also sharing recommendations for further improvements. The purpose of the third line is to "provide independent, objective assurance, as well as consulting activities designed to add value and improve a company's operations", and additionally "help the company to accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes" (The Wolfsberg Group, 2017, p. 22). The task for internal audit is to take a holistic approach towards risk management policies and procedures, and to conduct periodic assessments whether bank has sufficient awareness of its risks and controls. The holistic approach is described in the requirements of the Basel Committee as there should be audits for "the adequacy of the bank's AML/CFT policies and procedures in addressing identified risks, the effectiveness of bank staff in implementing the bank's policies and procedures, the effectiveness of compliance oversight and quality control including parameters of criteria for automatic alerts, and the effectiveness of the bank's training of relevant personnel" (Basel Committee on Banking Supervision, 2017, p.5). In the TBML context, these requirements for audit function emphasize the need for bank officers to understand the risks and related policies for risk prevention, and the audit function should be responsible for testing their effectiveness. As the mechanisms to launder illicit money change, the audit function should also aim to keep up with the constant change, otherwise all the relevant risks might not be matched with appropriate controls. Whether a bank applies internal or possibly external auditors, it should ensure that the audit function is organized based on the risk profile of a bank, and additionally to assure that the frequency of periodic audits is commensurate with the level of risks (Basel Committee on Banking Supervision, 2017). Besides the previously mentioned auditing duties, it should also be noted that the third line of defence should conduct assessments on the criteria for escalating and reporting suspicious transactions, and to ensure that the employee guidance for escalation process is up to date.

3.5 Correspondent Banking

An important element for sound management of TBML is the evaluation of risks related to correspondent banking relationships, and especially on the cross-border nature of banking transactions. The purpose for correspondent banking relationship is for a correspondent institution to provide banking services to a respondent institution's customers, and these services may include for instance third-party payments, trade-finance and cash clearing services (FATF, 2016). In

general, a correspondent institution does not interact with a respondent institution's customer, and the responsibility to conduct CDD for the customer initiating the transaction is placed on the respondent institution. The requirement for the correspondent institution is to conduct due diligence measures for the respondent institution, and due to the provision of higher risk banking services and the limited amount of information available, the correspondent banking relationships may carry higher level of money laundering risks (Basel Committee on Banking Supervision, 2017). Before entering into a correspondent relationship, the correspondent institution is responsible for applying money laundering risk assessment for the respondent institution, where the application of RBA is highly relevant when considering all the risk factors. During the correspondent banking relationship as guided by the FATF (2016), "the correspondent institution will monitor the respondent institution's transactions with a view to detecting any changes in the respondent institution's risk profile or implementation of risk mitigation measures, any unusual activity or transaction on the part of the respondent, or any potential deviations from the agreed terms of the arrangements governing the correspondent relationship" (p.4). Therefore, it becomes evident for the correspondent institution to take a holistic approach for assessing the risks exposed by the respondent institution, and even when there are varying levels of risks carried by respondent institutions, there exist some risk indicators that should be evaluated in the risk assessment process of all correspondent banks.

Banks that consider providing correspondent banking services should ensure their risk assessment of a respondent institution includes risks related to the respondent bank's services, its unique characteristics as an institution and also the environment where it operates. Some of the risk indicators that should be evaluated in relation to the nature of services include the purpose of using correspondent services by the respondent, how these services are used for instance if nested correspondence or third-party payments are permitted, or if payable-through-account services are used by third parties (Basel Committee on Banking Supervision, 2017). To clarify these relationships, nested correspondence refers to the respondent bank's use of correspondent relationship to provide transaction services to other banks that do not have a relationship with the correspondent bank, and the payable-through account refers to the direct use of correspondent account by a third-party (Basel Committee on Banking Supervision, 2017). These are considered as potential risk indicators since the correspondent bank might not have access to customer due diligence information, as its responsibility is mainly to conduct due diligence on the respondent institution. If the risk assessment of a respondent institution is not sufficient and a weak channel is found by criminals, the money laundering risks may be realized, and the correspondent institution may be exposed to transferring illicit money.

In addition to the services provided to the respondent, also the unique characteristics and risks related to respondent's operations should be included in the risk assessment. These potential risk indicators include the respondent's main business operations, the type of markets and customers served, the evaluation of

bank's management in relation to potential money laundering risks, the respondent's policies and procedures for money laundering prevention and whether the bank has been compliant with the law or been faced by any shortcomings in its anti-money laundering obligations (Basel Committee on Banking Supervision, 2017). Moreover, the comprehensive risk assessment should include the evaluation of respondent's operating environment, where either the respondent bank or its other affiliates are operating. These factors include the jurisdiction where the respondent is located, where potential affiliates or third parties are located and how effective these jurisdictions are with AML laws and regulations (Basel Committee on Banking Supervision, 2017).

These previously mentioned risk indicators should not be considered as an exhaustive listing of risks, and instead the RBA should be applied to determine the level of information required in order to establish a correspondent banking relationship. In the process of understanding the respondent's business, a correspondent should identify the level of risks and then estimate the measures taken by the respondent for mitigating those risks and based on the eventual residual risk it should decide whether the residual risk can be managed (FATF, 2016). The risk assessment can be stated as being an essential element for establishing new correspondent banking relationships, and as a new relationship is commenced the focus should be shifted towards the ongoing monitoring.

In a similar way banks are conducting due diligence on their customers, also correspondent banks are required to conduct due diligence and ongoing monitoring on their customers as in the form of respondent banks. The ongoing monitoring is particularly important for controlling TBML risks since the correspondent banking relationships are exposed for mediating cross-border transfers, which are considered as high-risk transactions. As an obligation for correspondent banks, they "should establish appropriate policies, procedures and systems to detect financial activity that is not consistent with the purpose of the services provided to respondent banks or any financial activity that is contrary to commitments that may have been concluded between the correspondent bank and the respondent bank" (Basel Committee on Banking Supervision, 2017, p. 28). In a similar manner as banks are applying monitoring to their customers, also the correspondent relationship should contain transaction monitoring to determine normal transaction patterns, which are used to identify suspicious activity. As a requirement for respondent banks, it should be ensured that all the payments being transmitted to the correspondent bank include accurate message information about the originator and the beneficiary in order to enable transaction monitoring from correspondent side (Basel Committee on Banking Supervision, 2017). Based on the CDD information of respondent bank, there should be scenarios developed for expected customer behaviour and the ongoing monitoring should be targeted to detect any discrepancies that exist between expected and actual transaction patterns. In occasions when the ongoing monitoring detects a potential suspicious transaction, the correspondent bank should have processes in place to confirm the underlying reason for the transaction, while the process

might include requesting additional information from the respondent (FATF, 2016). In relation to the extent of CDD, it should be noted there is no requirement for correspondent to conduct due diligence on the respondent's customer, and instead the focus should be on the risk assessment of respondent institution and on the updated due diligence information (FATF, 2016). The identification of risks followed by the management of risks in form of ongoing monitoring are essential elements for controlling TBML, and these elements should be incorporated to all banking organisations providing correspondent banking services.

3.6 Trade Finance Providers

In close relation to the correspondent banking, the trade finance providers either in retail or corporate banking are carrying an increased amount of TBML risks, and for the purpose of understanding TBML, its risks and controls should be discussed in trade finance context. In the light of financing international trade, the involvement of financial institutions in the trade process is diversified either into bank-intermediated or non-bank-intermediated trade. When buyer and seller agree on a contract without any need for financing, a role of bank is to transmit the underlying payment, and while having no access to contract terms the potential illicit behaviour might not be detected (BAFT, 2017). This form of financing international trade is entitled as non-bank-intermediated trade, and the reduced ability of identifying illicit behaviour is relevant both to the retail and the corporate banking segments that facilitate payments. The broad definition of open account trade is used with non-bank-intermediated trade, and also when banks provide financing in non-documentary basis (such as factoring or trade loan facilities), which both have the commonality of not having access to underlying trade documents (BAFT, 2017). In turn, the provision of financing in form of documentary credit, such as letters of credit or guarantees, provides a pathway for banks to facilitate payments and also to get access to trade documents (BAFT, 2017). The main difference in relation to money laundering prevention between open account and documentary transactions exist in the ability of identifying potential red flags as the documentary transactions provide opportunities to raise suspicions for example related to price, quantity and quality information of reported goods. Nonetheless, documentary credits still provide challenges as stated according to the UCP 600 rules outlined by the International Chamber of Commerce, that "banks deal with documents and not with goods, services or performances to which the documents may relate", as it provides limitations for effective prevention of TBML (BAFT, 2017, p.2). As long as the mandate for banks does not reach to the actual inspection of traded goods or services, the emphasis for trade finance providers is to conduct strict customer due diligence measures.

The identification of suspicious transactions sets a requirement for trade finance providers to create a due diligence process that functions as an effective control measure, and it should aim towards full understanding of the trade finance customer. According to the Trade Finance Principles established by the Wolfsberg

Group, ICC and the BAFT (2017), "CDD for trade account customers, both borrowing and non-borrowing, requires the financial institution to have an understanding of the business model, the principal counterparties, the countries where the counterparties are located and the goods or services that are exchanged, as well as the expected annual transaction volumes" (p.16). The application of RBA should define the risk level associated with each of the risk factors, which are not restricted to ones mentioned earlier, and based on the unique characteristics of each customer there should be an evaluation of proper risk controls. According to banks' RBA, enhanced due diligence (EDD) process may be required for customers posing higher risks, for example in cases where several red flag indicators are identified (The Wolfsberg Group, 2017). When banks encounter suspicious transactions, they should also estimate whether to conduct further checks on the transaction or to require more information about the trading parties. These checks on transaction may include, especially in the context of EDD, the use of International Maritime Bureau's container tracking service in order to ensure that underlying shipment is legitimate, or the checks on trading parties may include gathering more information on the ownership or background of the transacting parties (Joint Committee of the European Supervisory Authorities, 2017). The role of banks is to estimate these control measures that are commensurate to the customer's risk profile and the ongoing monitoring should also be organized according to the risk profile. Due to the fact that documentary trade strongly relies on paper documents, it is a challenge for banks to create automated transaction monitoring for this purpose, and the emphasis should be shifted on the professional judgement of trade processing staff to identify any suspicious information according to the listing of red flags (Joint Committee of the European Supervisory Authorities, 2017).

4 METHODOLOGY

4.1 Research Approach

Research approaches are traditionally categorized into quantitative and qualitative methods, although applying one of them do not cancel out the other method. These methods are frequently applied together in same research and in analysis of the same research data, and furthermore these methods can be considered as each other's continuum and not as each other's opposites (Alasuutari, 2011). In general sense, the quantitative analysis methods apply numeric data in order to argue about their systematic and statistical connections, whereas the qualitative analysis methods frequently aim to explain the construction of researched phenomenon by looking at the data as a whole (Alasuutari, 2011). In the light of this research, only qualitative research methods are applied in order to explain the best practices within financial institutions to control the phenomenon called TBML. As stated according to Ghauri & Gronhaugh (2005), "qualitative research

is particularly relevant when prior insights about a phenomenon under scrutiny are modest, implying that qualitative research tends to be exploratory and flexible because of unstructured problems" (p. 202). This aspect of qualitative research is highly relevant to the TBML phenomenon, as the international trends in money laundering are currently shifting towards more sophisticated methods, and as the difficulty of gathering accurate data on illicit money flows has been commonly acknowledged. Due to the fact that there is restricted amount of research conducted in this particular money laundering method, the aim for this research is to raise awareness of the whole phenomenon amongst the financial industry, which is increasingly being influenced as a business sector.

The foundation for this research was to provide holistic understanding of the phenomenon called TBML, to explain the problems associated with it, and to discover currently used controls within financial industry to fight against the phenomenon. In its typical nature, the qualitative research aims to discover "how things work in particular situations" with the goal for the researcher to improve the way of how things work (Stake, 2010, p. 13). Due to the varying characteristics of money laundering risks, represented in this research as red flags, also the response from a financial institution is expected to be unique based on the underlying risk scenario, which furthermore emphasizes the importance to study how things work in different situations. As the phenomenon is relatively new in the field of anti-financial crime, the responses from different financial institutions regarding best practices in controlling TBML are expected to give new information regarding how banks can fight against this money laundering mechanism.

4.2 Data Gathering

The data on best practices of controlling TBML under current knowledge of banks were requested by constructing a questionnaire, which included five different steps that banks were expected to complete. The questionnaire was electronically delivered to eight internationally operating banks, that are both offering international payment solutions and trade finance products. Out of the eight banks, eventually three of them were able to reply on the questionnaire. The foundational element of this questionnaire was the collection of 49 potential red flag indicators from varying anti-money laundering resources, and as they represented how TBML can potentially be detected, the participants were asked to provide control measures to fight against these potential red flags. In order to create clarity on the large number of red flags, there were five different categories created based on where the potential risks may arise and each of the red flags were assigned to these categories accordingly. The initial task for respondents was to identify all the red flags listed in the questionnaire, and to list additional red flags which might be relevant in detecting TBML based on their observations.

Secondly, the respondents were asked to rank red flags under each category based on the expected risk-level to their financial institution. The ranking of red flags within each category was expected to represent what type of risks are relevant to be controlled for each financial institution according to their own risk assessment. Even though there are varying banking operations and the risk-based approach is unique to every institution, the ranking of red flags could create a holistic view of the perception of banking sector on what type of risks are generally expected to pose higher threat of TBML. The rank of one was determined to represent highest amount of risk, and due to the large number of red flags within some of the categories the ranking could be extended to the maximum of five.

Thirdly, the respondents were asked to assign which banking products are exposed to each of the red flags, where the banking products were divided into three categories based on the expected level of exposure to TBML. As a first category there were payments, in general wire transfers, that include money transmission between trading parties associated with the trade transaction. As a second category there were open account trade payments, that include provision of credit to support the trade transaction, such as factoring or pre-shipment finance. As a last category there were documentary trade transactions including payments, which can be interpreted as lending the financial institution's name to the transaction in forms such as a letter of credit or guarantee.

After assigning red flags to corresponding products, the respondents were asked to move on to the most relevant part of the questionnaire for this research, where the respondents were expected to describe the best practices of controlling each risk. The purpose was to gain as much information as possible on controls, which these banking organizations have observed to successfully mitigate the risks related to TBML. Due to the extensive listing of red flags, it was expected that there would be some overlapping on controls, as some of the red flags may be controlled with similar procedures. In addition to delivering the questionnaire, the respondents received two example responses of red flags and their matching controls, which were intended to set the research standard for acquiring as practical information as possible on these control measures.

Lastly, the respondents were expected to assign each red flag indicator to the appropriate line of defence responsible on controls and escalation process according to the financial institution's risk-based approach. The aim for this last task was to identify which unit can possibly detect suspicious activity based on these red flags, and which unit can escalate a particular transaction to further investigation.

4.3 Analysis

The analysis part of this research is dedicated for creating connections amongst the research responses, and for providing clearer perception on the phenomenon

of TBML. In a qualitative research, this part can be entitled as resolving the puzzle, where an insightful interpretation on the studied phenomenon is derived with the use of produced leads and available cues (Alasuutari, 2011). For this particular purpose, not only the informant responses are carefully analysed but also the non-written leads and cues related to the TBML phenomenon are discussed in this section. As the informants have responded to the questionnaire separately, this section aims to combine the best-known practices of how to fight against TBML and to make connections to the theoretical framework. Nonetheless, the detailed discussion on each red flag and its corresponding controls are discussed under the appropriate red flag categories. Due to the research objective is chosen to introduce appropriate controls to fight against TBML amongst the globally operating financial institutions, the analysis part is naturally extended to discussion in global scale. In order to resolve the puzzle of TBML, the analysis section further creates connections to the essential risk management components that are required to be in place for controlling against this phenomenon.

5 RESULTS AND ANALYSIS

5.1 Red Flags and Controls

5.1.1 Customer & Business Structure

The red flag indicators within the underlying category are mainly related to a financial institution's responsibility for conducting customer due diligence (CDD) measures on both new and already existing customers. According to the recommendation of FATF (2012), "understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship" is one of the essential CDD measures (p.12). In addition to understanding the purpose of customer relationship, "conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds" becomes an inevitable measure to control money laundering risks (FATF, 2012, p.12). From TBML perspective, the similar principles are applied to new and existing customer relationships as the potential red flag indicators should be evaluated against the customer information collected under the CDD process.

After a financial institution has understood the business model of its customer, the evaluation of red flags should be conducted in respect to the business structure, and it should be aware of what is expected to be a normal and consistent transaction from its customer. Due to the global outreach of TBML methods, the red flags related to customer and business structure frequently include something suspicious related to the shipment of goods. It should be alerting if "the

shipment is inconsistent with the exporter's normal business", as for instance an exporting company of consumer electronics is suddenly exporting paper products (Cassara, 2016). A discrepancy of conducting business in a completely different field is further complemented with the size of shipments, as the sudden increase or decrease in the scale of shipments can also be perceived as a red flag (FATF, 2006). As a control for both red flags, Company B states that "trade finance only handles transactions with clients and banks that are fully onboarded", and when a transaction is compared to the client's line of business and normal trading patterns known to the bank, if any additional information is needed the account manager is contacted and the decision of completing the transaction is based on that clarification. Similar responses were given by Companies A and C, which emphasized the importance of efficient KYC procedure, understanding the core business of their customer, checking additional documents such as invoices and to compare documents against the customer's line of business.

Both of these prior red flags are related to knowing a financial institution's own client, but a red flag might also be raised based on the shipping location or the end-customer. A financial institution could become aware that a customer is shipping goods to another country that has no industry or no demand related to those goods, which should be a trigger for further investigation (Cassara, 2016). One such an example could be shipping of advanced electronics equipment to a country that has no electronic industry or no capability of benefiting from the equipment. Company C states that as a part of effective KYC procedure, a "thorough understanding of the supply chain of the customer and it's end user" functions as a control, which is extended to knowing your customer's customer. In the context of trade finance, Company A mentions that buyer's bank as an issuer of a trade finance product has the responsibility to know its customers, but in some cases the business line of customer's customer is verified by using open sources. Company B further clarifies that the bank does not always hold the information on its customer's customer, but the buyer's line of business and existence can be verified from an external source such as Bureau Van Dijk Trade Finance portal. If such verification raises suspicions, the bank will contact their client asking for additional information in order to confirm whether to complete the transaction or not.

5.1.2 Transaction, Goods & Payment

5.1.2.1 Transaction & Payment

A red flag indicating whether a transaction is trustworthy is when "the method of payment appears inconsistent with the risk characteristics of the transaction", for example in a case where the payment to a new supplier in a high-risk country

is settled by using an advance payment (FATF, 2006). A financial institution is required to evaluate each transaction based on their risk-based approach, and the above-mentioned case is merely one example when the risk characteristics are not aligned with the chosen payment structure. Company A notifies that "it is typical for the new business relationship to use advance payments", "however special attention should be payed to percentage of advance payment" as the 100% advance payment is observed to be unusual. Company B indicates a fact that its "customers use different payment methods and risk mitigating instruments based on their individual risk policies", but if the transaction includes any inconsistencies with the normal business practices, the account manager is contacted according to banks' standard operating procedure (SOP), and in the lack of business rationale the transaction is escalated to internal investigators.

Additionally, suspicions could be raised when "the transaction and payment appear to have unnecessary and complex layers involving multiple accounts and multiple jurisdictions that combine to obscure the true nature of the transaction" (Cassara, 2016). When comparing trade finance and open account payment facilities, it could be stated that identifying complexities, followed by raising suspicions, are more probable from trade finance documents as open account payments rarely provide any underlying documentation from a trade. Company A states that "transaction monitoring process includes scenarios", which are constructed of risk characteristics for possibly obscuring transaction's true nature, and "based on possible scenarios these transactions are escalated into further investigation".

With the requirement of additional documentation, trade finance products might also face higher risks due to forged documents, and one red flag could be raised when "the transaction involves the use of repeatedly amended or frequently extended letters of credit" (FATF, 2006). It would not be interpreted as normal customer behaviour to constantly change the terms of a trade finance transaction, and a financial institution is expected to treat such transactions with closer scrutiny. Company B states that "the business reasons for frequent amendments are clarified with the client in accordance to our SOP's", and if the transaction is determined to lack business rationale, it will be escalated. Company A points out that amendments are considered as normal practice in many business cases, and as money launderers are usually inclined to retrieve their monies as soon as possible, the amendments are not typical for money laundering purposes.

For the purpose of hiding the true origin of a transaction, there are incentives for criminals to add further complexity in order to avoid detection by including other parties or intermediates into the transaction. One of the red flags for a financial institution could be a case, where "international wire transfers are received as payment for goods into bank accounts where the exporter is not located" (Cassara, 2016). In order to elaborate on this red flag, a bank should be aware on its customer's trading partner, to gather information on the exporting location and to seek further clarity whether a wire transfer to another country, besides the

exporting location, has an understandable reason. In practice, Company B has observed that this method is quite often used by Russian customers, "where the receiver of the goods is different from the payer", and "often also the payer is a holding company in a bank secrecy or tax-haven jurisdiction like British Virgin Islands. It is added by Company B that the control for this red flag is on the transaction monitoring team, and the transaction analysis as part of ODD is a relevant control mechanism. The respondents provided similar control measures for a red flag, where the payment for goods is either received from multiple sources or from multiple accounts (Cassara, 2016). The involvement of multiple sources and accounts provide a significant money laundering threat since it offers a credible cover for illicitly acquired gains to be layered back into economy, unless there are no adequate controls to verify whether the payment is from the actual customer.

Similarly, this can be extended to red flags related to alternative payment methods where "transactions that involve payments for goods through checks, drafts, or money orders are not drawn on the account of the entity that purchased the items" (Cassara, 2016). Furthermore, when "the transaction involves the receipt of cash (or other payments) from third party entities that have no apparent connection with the transaction", should be noted as a red flag (FATF, 2006). Company C emphasizes conducting effective KYC procedure, including KYC of customer's customer or counter party, and in order identify whether a transaction is received from unknown party, the responsibility is with the implementation of cash scenario and transaction monitoring to detect suspicious transactions. In summary, the involvement of additional parties or non-consistent payment methods in a trade transaction should not be condemned illicit straight away, and instead the potential discovery of these red flags should lead into further investigation.

In addition to previously mentioned red flags, there are some additional transaction and payment risk factors that should go through a careful evaluation if they are encountered by a financial institution. One of these risks include the use of cash, if "unusual deposits of cash, cash deposits in round numbers, or structured deposits under the reporting threshold into a bank account are used to fund the trade transaction (Cassara, 2016). The use of cash is already a potential risk mainly due to its anonymity and ease of transportation, but also the way how criminals are using cash might provide indicators of potential money laundering. A practical observation is offered by Company B, that has seen "Russian freight-forwarders import items to Finland and then the freight-forwarders customers travel over the border to Finland and pick up the goods, often paying with cash and high-value bank notes like the 500€ bill". Company B identifies control mechanism for the use of cash in form of "transaction monitoring scenarios, limits at deposit ATMs and transaction analysis during ODD", also indicating that cash transactions are easy to be caught.

One of the most prominent red flags that should be included in bank's risk assessment process is when "significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value (FATF, 2006). The fact that trading partners are jointly able to negotiate the price of a commodity provides an attractive channel for mispricing and a channel to launder illicit money. Due to the difficulty of gathering documentation under open account payments, it provides more opportunities for money launderers to exploit the banking system, especially if compared to trade finance payments when banks can collect information about the underlying trade terms. The respondents further confirmed that there are difficulties to detect the market value for goods, and as stated by Company B "we have seen that the suspicious customers often use items like industrial components, t-shirts and golf-balls, the value of which is very difficult to determine from the outside". Especially pricing anomalies of tailor-made goods are difficult to detect, and as further information may be requested through the account manager, the key controls for mitigating these risks according to Company B are "knowing client's trading patterns, normal line of business and having experienced personnel". Company A stated that "we do not have the resources to assess the fair market value", but "knowledge of common values is known to the bank".

In addition to valuation difficulties, a bank should pay attention in cases where parties related to each other are included, for example in familial relationships, which are identified as more vulnerable to favourable pricing techniques between cooperating parties (Cassara, 2016). As a control, Company B determines the business rationale in cooperation with the account manager based on the information provided by the client, and also the transaction monitoring includes payments with familiar relationships as red flag alerts. Additionally, even though checks are decreasing in importance as a payment method, based on known money laundering schemes from the past, one potential risk is raised when "sequentially numbered checks drawn on domestic bank accounts are negotiated through foreign money service businesses" (Cassara, 2016). Money service businesses are referred to as regulated money transfer operations outside of the formal banking system, and these operators are recognized as risky for potential money laundering operations (FATF, 2006).

5.1.2.2 Goods

The red flags for potential TBML schemes related to shipping of goods include the falsification of documents, carousel transactions, inconsistent trading routes and use of confirmed high-risk goods for money laundering purposes. To commence with the falsification of documents, one of the most attractive covers for illicit money flows are phantom shipments, where actual goods are not shipped and trading partners have falsified all documentation (The Wolfsberg Group, 2017). For phantom shipments to succeed, there is a need for collusion between

trading parties as the shipping and customs documents are required to appear legitimate and to be affirmed by both parties. When financial institutions do not have access to whether goods are actually shipped or not, they might be engaged in offering trade financing for potential phantom shipments without being aware of the exploitation of their systems (FATF, 2006). In case of payments, Company B requires bills of lading or other documentation if there are any suspicions raised around the customer, but it was admitted that this technique may be difficult to detect. As an important control, Company B uses the external service of International Maritime Bureau (IMB) to verify the information accuracy related to bill of lading before a transaction is completed. It was added by Company A that "occasionally random checks are made whether the ship has actually visited the port", and additionally confirmed the use of IMB to authenticate bills of lading.

The falsification of documents also raises a red flag, when "there are multiple invoices for suspect goods", and "a frequently repeated suspect pattern of numerous invoices involves the same or similar items and where the actual physical shipment is never physically verified" (Cassara, 2016). Multiple invoicing has the potential of justifying several payments related to same shipment of goods as the method appears legitimate and it offers added complexity to detect falsified payments among the legitimate payments. From a bank's perspective this method presents challenges due to the lack of access to invoices and to shipment verifications, and by the possible involvement of several financial institutions, the whole operation becomes even more difficult to detect. Company B comments on multiple invoicing that this mechanism "might be caught during transaction analysis phase of ODD" when transmitting payments, and even though there may exist no tools to verify multiple invoicing, the trade finance process requires the original transport document such as bill of lading to verify that the actual shipment has taken place. As a similar control than in phantom shipments, if any suspicions are raised the IMB service may be used to verify accuracy of documentation.

One additional red flag that can be identified by banks dealing with trade transactions is when "transaction involves shipment of goods inconsistent with normal geographic trade patterns of the jurisdiction", which as an example could be a sudden importing or exporting of goods by bank's customer with a jurisdiction that is not known of trading such goods (Cassara, 2016). This red flag requires not less than acquiring additional information on global trading patterns and comparing these patterns with acquired customer due diligence information. The challenge of being completely aware of all the global trading patterns was introduced by Company B, and it was stated that knowing the client line of business and normal trading patterns are key controls to detect discrepancies in trading patterns. Additionally, the implementation of inconsistent trading patterns as a red flag in transaction monitoring and ODD is a relevant control when transmitting payments.

There exist some additional ways for criminals to launder their funds, which are associated with the increasing international trade and these loopholes exist due to the common duty agreements. This mechanism to launder money is referred to as carousel transactions or value-added (VAT) tax fraud, which has been observed as a way to raise funds for criminal organizations and also to launder funds gained by criminal activities (FATF, 2007). In the mechanism's simplest form, goods are purchased free from VAT from another member state according to the common duty agreement (for example within EU), then goods are sold onward including VAT, and lastly the purchaser goes missing meanwhile defaulting on VAT payment to the government (FATF, 2007). When the same shipment of goods is used to leave and enter the common duty area, the mechanism becomes more complex with the purpose of increasing the VAT liabilities. The red flag for financial institution is when these forms of carousel transactions are involved, and "the repeated or circular importation and exportation of the same high-value commodity" is able to be identified (Cassara, 2016). As stated in the research by the FATF (2007), "the main typology is that all transactions within a chain will use the same banking institution" to move illicit money, which creates a requirement for banks to be aware of the phenomenon in order to perform effective investigations (p.2). It was pointed out by Company B that these types of carousel transactions "can be discovered during the transaction analysis phase of ODD where the customer will be asked to give rationale for such behaviour". An effective control against carousel transactions is to ensure banks do not handle transactions with clients that are not confirmed through the KYC process, and in case of any suspicious activity the business rationale may be verified by requiring additional information from the customer.

Financial institutions should also be aware of the risks related to certain types of goods that are identified as being used for money laundering purposes, and in that sense considered as high-risk goods. One of the red flags is when a trade transaction includes "goods that are commonly associated with TBML schemes", for example "scrap gold, precious metal and stones, trade in tobacco, consumer electronics and automobiles" (Cassara, 2016). Company C describes that involvement of such goods immediately leads into enhanced due diligence for the customer trading with these goods. In general, it is common for TBML schemes to involve high-value and low-volume goods, which effectively enables the value transfer across different jurisdictions. Similarly, the characteristics of these goods frequently involve the difficulty of present valuation as there's no database or accurate market information on certain types of goods (Cassara, 2016). As a control mechanism for both of these prior red flags, Company B states that involvement of such goods always leads into further investigation, where "customer can also be asked to sign declaration (risk-based approach) confirming the compliance of export control regulation" and based on information gained from account manager and customer, it is determined whether the transaction is confirmed. TBML can also occur with the use of barter trade, where two or more set of goods are only exchanged by the trading parties, and the value is transferred to other

party without including a payment. Certain types of goods are identified as commonly being exchanged for bartering schemes, such as gasoline or tires, which should also be a red flag for a financial institution (Cassara, 2016). The difficulty of detecting such schemes was identified by Company B, and even though the company is not involved in bartering schemes, a red flag is raised, and further investigation is conducted based on internal compliance screening process.

One risk category for goods being traded is when "goods do not comply with applicable import or export regulation or involve dual-use and high-risk goods" (Khanna, 2019, p.9). As a risk indicator for banks, it can be possible that importer or exporter of certain goods does not withhold license or other form of certification to conduct trade, which should be in the awareness of a bank. As mentioned also dual-use goods, which are referred to as goods that can be used for both civil and military purposes for example software and technology, are recognized as being vulnerable for money-laundering schemes (Financial Conduct Authority, 2013). Even though there are several goods that are known to be used for money laundering purposes, it should be stated that the involvement of such goods does not automatically indicate that trade is illicit. It becomes a responsibility for banks to wholly understand customer's business activities involving such goods and based on their evaluation it should be determined whether there is a rationale of trading with such goods (BAFT, 2015). In relation to payments, Company B describes that "controls exist around the target country and asking the customer for documentation, but if done cleverly enough this would be very difficult to detect from the bank". When Company B faces transactions that include high risk areas or involve obvious dual-use goods, they have "dialog with the client on the export control regulations", they "will ask the client to sign declaration confirming that they adhere to OFAC sanctions and EU sanctions and export control regulations", and also verifies from the customer whether an export license can also be asked. Similar procedure is followed by Company C as they require additional confirmation if high-risk countries, high-risk goods or transactions that are subject to sanctions are involved. Company C also requires clients to assess whether dual-use goods or goods used for military purposes are involved, to confirm to the bank if there exists any connection to oil or gas industry and furthermore to specify what geographical areas are involved and for what reason. Additionally, the previous listing of high-risk goods is not exhaustive and there might be several reasons why certain goods can include TBML risks.

5.1.3 Shipment Structure

The red flags that can be identified from a shipment structure are related to possible suspicions raised on the involvement of high-risk jurisdictions, inconsistent shipping routes and other unusual shipment arrangements. There is a possibility that some of the high-risk jurisdictions are involved along the shipping route, and the red flag should be raised when "the commodity is being shipped to or from or through areas of high-risk for money laundering" (Cassara, 2016). The high-risk jurisdictions are in connection with weak anti-money laundering and

counter-terrorist financing measures, and it has been stated that criminals are able to evade comparative controls due to the existence of high-risk areas (FATF, 2019). In order to make certain that there is an understandable reason for such shipments, banks should implement strict controls to investigate these types of cases. As a practical note on recent money laundering phenomenon, Company B indicates that illicit actors "tend to use more legitimate countries instead to mask the suspicious nature of the shipments", where "most often payments might be routed through EU-countries that might have weaker controls but still in the EU". One of the controls introduced by Company B is to ask customers "sign a declaration confirming the compliance of export control regulation". Company B adds that "in case of an unusual complex shipment structure, we will contact the account manager in order to verify that the transaction is within the client's business profile", and that clarification determines whether transaction is completed or not. If a high-risk country is involved in a transaction in any way, Company C states that enhanced due diligence and escalation procedure are used to control these risks. The closer examination of customer information is also executed by Company A, as "in these kinds of cases the bank pays special attention to the customer's business, the documentations, and the parties involved".

In addition to jurisdictions, also specific free trade zones (FTZ) have been considered as high-risk areas since it is characteristic for FTZs to have fewer authorities and less monitoring and examination for cargo and other trade transactions (FATF, 2010). The potential TBML risks of FTZs is also extended to the ease of company formation, lack of transparency in ownership structures, creation of added layers for transactions and lack of trade data offered for law enforcement (FATF, 2010). Due to the inadequate oversight of anti-money laundering issues, banks should pay closer attention for transactions where "shipments involve suspect free trade zones or special economic zones" (Cassara, 2016). According to Company A, involvement of free trade zones or special economic areas may impose risks in documentary collection stage, which can be controlled when "goods are consigned to the freight-forwarder in order to make sure the buyer doesn't get hold of the goods without payment". In order to verify the shipment information, Company B recommends the use of IMB and for the purpose of verifying the buyer's existence and line of business the use of Bureau Van Dijk, Trade Finance portal.

There are some red flags that are related to the shipping routes, which should raise concerns if they are inconsistent with customer's behaviour or they provide no business rationale. One red flag can be identified in a transaction where "the routing of the shipment is circuitous, not direct, is illogical, or is being transhipped through a questionable area for no apparent economic reason (Cassara, 2016). If parallel shipping structures are detected, banks should collect more information and to follow their risk assessment process to determine the legitimacy of complex shipment structures. It was stated by Company B that similar controls, as in case of free trade zones and special economic zones, can be used to detect and investigate more closely on complex shipment structures. Furthermore,

Company B pointed out "if it is possible not to take part to these kinds of transactions, we wouldn't participate", as "in order to avoid tipping off, we would participate and then make suspicious activity report".

The identification of TBML mechanisms is frequently related to paying attention to smaller details, and after evaluating all details more holistic approach can be taken to prevent TBML. One red flag associated with focusing on details is when "a shipment does not make economic sense", if for example a relatively low volume of goods is shipped by using 40-foot shipping container (FATF, 2006). According to the Company B's response, "if a shipment doesn't make economic sense or obvious irregularities spotted in the documents, we will take contact to the client and ask for clarification". Furthermore, one example from detecting suspicious information in trade documents is if "a freight-forwarding firm is listed as the commodity's final destination" (Cassara, 2016). In practice, Company B has observed this method of being frequently used when banks are transmitting payments, which emphasizes the importance of focusing on details in order to prevent TBML. In order to summarize the red flags related to shipment structure, it can be stated that all the relevant documentation might potentially expose illicit activity, and further clarification should be searched if a transaction lacks understandable reasons.

5.1.4 Documentation

The red flags under the documentation category contain indicators of suspicious activity that can be noticed from collected documents throughout the payment or trade financing process. In open account trade transactions banks are rarely involved with the transaction until there is a clean payment made between trading parties, and so there are no opportunities to review trade documents (The Wolfsberg Group, 2017). In comparison to trade financing documentation, where documents such as contracts, invoices and shipping documents are available, the investigation of false information is more convenient, even though it challenges bank officers to work in a rigorous manner. As stated by the Wolfsberg Group (2017) in their report of trade finance principles, "reviewing trade documentation is highly manual process, requiring that the commercial documents that are presented for payment are compared against each other for material differences, that they relate to the transaction described in the covering schedule" (p. 52). Since the documentation is still based on manual processes, although technology is already changing the business landscape, it becomes important to emphasize possible risks that can be identified from underlying documents.

The red flags categorized under documentation are mainly related to inaccurate representation of information, when compared to other known databases, and also fraudulent information discovered from trade documents. Some of the most powerful forms of discovering inaccurate information is the comparison of information to other resources for example to fair-market prices, and also the comparison of both shipping and payment documents. One red flag for banks is when

"significant discrepancies exist between the description, quality, and quantity of commodity on the bill of lading, invoice, and actual goods shipped" (Cassara, 2016). Company A states that in these cases "the documents are rejected by the banks", even though not effecting payments. In order to detect such discrepancies, Company B relies on their internal Red Flags Standard Operating Procedure (SOP), where the obvious discrepancies are addressed. Another red flag that can be added to the process is if there is "significant deviation between the value of the commodity as reported on the invoice and a normal arm's-length fair-market price" (Cassara, 2016). The challenge for banks to deal with these red flags is the lack of access to the actual shipment information and also to accurate market prices, which should shift the focus of transaction processing teams more towards these aspects before ultimately completing transactions. It was stated by Company A that "we do not have the resources to assess the fair market value", although common values are generally known in the bank. For both of these prior red flags, Company B indicates that the transaction monitoring teams have no capability of evaluating these discrepancies, and as the fair market value is difficult to determine especially for tailor made goods, the irregularities and actions against them are included in the SOP.

Trade documents and underlying shipments might also issue red flags if "the weight of the shipment does not match the listed contents" or if "shipment locations or description of goods are not consistent with the letter of credit" (Cassara, 2016). Some difficult types of risks for banks to identify are if "the quantity or quality of the goods is padded or inflated", or if "packaging is inconsistent with the commodity or shipping method involved" (Cassara, 2016). In order to discover these red flags, banks are required to get an access to the information provided by the exporter, and although being rare for open account transactions, it is feasible for trade finance payments. Company A responds that the bank will reject such documents, which include any such discrepancies or information inconsistencies. It was added by Company A that "the bank does not necessarily have the competence to assess the weight of the shipment", and also "the bank might not have enough experience regarding commodities or shipping methods" to detect any discrepancies. As stated by Company B, "obvious discrepancies will be addressed according to our Red Flags SOP", which will determine the measures to collect more information from both the customer and also the account manager. Additionally, it was pointed out by Company B, that in response to these red flags the "transaction monitoring teams are unable to evaluate" these mentioned red flags on open account payments, which further highlights the problem of getting criminals caught when trading in open account basis.

Another way to detect potential TBML cases is to concentrate on clear inaccuracies in trading documents or to identify patterns that appear abnormal. One such way to detect anomalies is when "invoices or bills of lading include inaccurate information about the product being shipped or information that is not commonly accepted", and an example of this case could be invoicing of granite tiles which are listed in units of square feet when the common norm is pricing by the

ton (Cassara, 2016). Similar cases might rise if "invoices contain inaccurate or incomplete product descriptions", and such cases could involve the lack of global product codes in the importation of goods, while making it difficult to estimate the true market value (Cassara, 2016). The detection of inaccurate information can also be applied to common mistakes in trade finance documents that might indicate on illicit activity. According to Khanna (2019), focus should be shifted to "common red flags for Letters of Credit fraud including incorrect use of banking terms, spelling mistakes and errors in grammar and composition (p.9). In addition to these common mistakes, there are possible risks related to information that is out of the scope of commonly accepted standards if for instance "the letter of credit contains non-standard clauses or phrases" (BAFT, 2015). The abnormal input of information should make bank officers more cautious on trade transactions, and due to the documentary nature of trade transactions, bank officers who are aware of these red flags have the highest probability of detecting illicit activity. According to Company B, in addition to obvious discrepancies also the unusual wording and its structure will be addressed in Red Flags SOP, and if the description of goods is for example too generic more explanations will be asked from the client. It was added by Company B that inaccurate information or incomplete product description are red flags in transaction monitoring, which should create an alert if any suspicions are raised in this sense when transmitting payments. Company A responds to risks related to wording structure that "special attention is being made to terminology especially guarantees", and if non-standard clauses are found the bank wouldn't participate on the transaction, which would lead into making a Suspicious Activity Report (SAR) and informing the internal fraud department.

Lastly, there are some red flags on documentation that can be considered as rather general information, but still they should be listed as potential red flags. Even though there are no definite guidelines of how to notice fake documents, when "documentation appears fraudulent" or if "counterfeit invoices are used", more thorough investigation should be conducted in these cases (Cassara, 2016). Company B states that "clearly faked bills for exported or imported goods have been seen in ODD quite often", referring that the attempts to offer fraudulent invoices is a standard practice for illicit actors. In addition to suspicions related to documentation offered by a customer, also the customer behaviour and the lack of responsiveness to bank inquiries might be an indicator of illicit activity. The red flag related to behaviour should be raised when "a party is unable or unwilling to produce appropriate documentation upon request", which should not be considered as challenging in normal business circumstances (Cassara, 2016). As a control to fraudulent and counterfeit documents, Company B states that "if document appear fraudulent it would be a full stop pending result of a further investigation hereunder verification of the bill of lading at IMB", and "despite the result such a transaction should be escalated". Coincidental approach is confirmed by the Company A, which would not participate in such transactions if these red flags are detected, that would require the bank to make a SAR and inform the fraud department.

5.1.5 Intermediaries, Deal Parties & Third Parties

The last category of red flags is linked to intermediaries, deal parties and third parties involved throughout the open account and trade financing processes. Most of the red flags include the discussion over possible misuses of corporate vehicles that enable obstructing the identity of beneficial ownership. The international standards set by the FATF (2012) define beneficial owner as "the natural person who ultimately owns or controls a customer and the natural person on whose behalf a transaction is being conducted", and "it also includes those persons who exercise ultimate effective control over a legal person or arrangement" (p. 111). The use of corporate vehicles is highly relevant mechanism for TBML purposes as the obstruction of beneficial ownership enables two different parties to hide their true identities, and also these two parties might be controlled by the same individuals. Furthermore, it has been stated by the FATF (2014) that hiding beneficial ownership enables disguise of "the identity of known or suspected criminals, the true purpose of an account or property held by a corporate vehicle, and the source or use of funds or property associated with a corporate vehicle" (p. 6). In addition to hiding beneficial ownership information, there are other established risk groups that should raise the awareness of banks if they are identified throughout the trade process.

In order to evaluate whether a transaction attempts to hide the true identities of transacting parties, there are some red flags that provide assistance for the evaluation. One signal for a financial institution might be when "the transaction involves the use of front or shell companies" in any stage of the transaction (FATF, 2006). According to the definition by FATF (2018), a front company is a "fully functioning company with characteristics of a legitimate business, serving to disguise and obscure illicit financial activity" and a shell company is an "incorporated company with no independent operations, significant assets, ongoing business activities, or employees" (p. 5). Both of these legal persons enable disguising beneficial ownership information, which is the reason why further investigation is required if such legal structures are found throughout the trade process. Company B informs that "if a transaction appears to involve front or shell company, the transaction will be considered suspicious", and "the business rationale will be determined in cooperation with the client". Company A states they wouldn't do any business with shell or front companies. Company C follows a procedure where "transaction monitoring and cash scenario identifies new counterparties and recognises if the payment to the client's account comes from an unknown sender", which further triggers to ask for more clarification from the client.

In addition to front or shell companies, one red flag is when "companies are operating out of foreign countries where it is very difficult to determine the true ownership or controlling persons of the company or where the type of business is not fully apparent" (Cassara, 2016). Even though front and sell companies are frequently associated with such structures, depending on the jurisdiction there

might be some other structures or arrangements that increase the risks for potential TBML. Company B has observed countries such as Cyprus, the British Virgin Islands and Marshall Islands to be used by Russians. There have been cases where for example Cypriot lawyer is listed as a beneficial owner, and when taken a closer examination it has been observed that the same lawyer is serving on the board or listed as an owner of hundreds of different companies. When controlling risks related to payments, Company B focuses on "the ODD process by verifying the identity of beneficial owners, including source of wealth". In relation to trade finance, Company B investigates the beneficial ownership information for certain high-risk countries and transactions, where "parties' existence and line of business are verified through the external portal of Bureau Van Dijk". Company C informs they will immediately commence the escalation procedure, when a high-risk country, industry or nationality is involved in the transaction. Lastly, it was pointed out by Company A that "our customers carry out their own KYC, and when necessary, we ask more detailed information about processes".

One red flag related to unusual ownership information is when "the parties involved are not transparent and use Delaware -like shell corporations with lack of beneficial ownership information" (Cassara, 2016). The difficulty of obtaining ownership information is emphasized in the U.S. National Money Laundering Risk Assessment in 2018 that states "bad actors consistently use shell companies to disguise criminal proceeds and U.S. law enforcement agencies have had no systematic way to obtain information on the beneficial owners of legal entities" (U.S. Department of the Treasury, 2018, p. 28). Under some state laws there might be an opportunity to incorporate a company by providing minimum amount of information about the beneficial owners, which enables the use of such legal structures for illicit purposes. The respondents of this research questionnaire explained that mitigation of these red flags is similar as mentioned in the use of front or shell companies in a transaction.

In addition to finding accurate ownership information, there are some other red flags that increase the risk-level of trade transactions. A financial institution should be on alert if "the transaction involves a third party that has no apparent connection to the buyer or seller", which eventually relates to prudent customer due diligence process (Cassara, 2016). Company B confirms "if a third party with no relation to the buyer or the seller appears in a transaction" it will be considered as suspicious. Company B has observed that frequently "the payer is different from the receiver of the goods", and as a control the bank relies on "transaction analysis in the ODD process". Company A provides a control, where the third party is checked against the sanctions lists, and "when necessary, we would investigate the role of the third party".

Another risk category is the use of certain corporate structures that are known of being commonly used for money laundering mechanisms. A financial institution might discover such mechanisms if "numerous sole-proprietorship businesses or

private limited companies are involved in the transaction or established by proxies or where false addresses are involved" (Cassara, 2016). The reason why these corporate structures are estimated as risky for money laundering is because of their vulnerability of hiding true ownership, the ease of being established and the possibility of being more conveniently used in complex legal structures (FATF, 2018). Company B provides insight that this mechanism has not been seen quite often, and the application of ODD functions as the most effective control.

The risks are not restricted to certain corporate structures as there are also risks related to particular industries or types of businesses. Based on known money laundering cases, if "money services businesses or money exchange bureaus located in third countries are used as intermediaries for the transfer of goods or money" there are higher risks for money laundering (Cassara, 2016). Company B has seen the use of these types of businesses quite often "especially with certain minority groups in the Middle-East and Africa". As a control, Company B names "transaction analysis (ODD) and transaction monitoring". Additionally, if "upon inspection or verification, the manufacturing entity has no physical address, no or limited production capability, limited or no inventory at its business premises, and so on" a financial institution should take closer scrutiny on processing such transactions (Cassara, 2016). Company B also notes that this red flag "has been seen quite often and is very difficult to assess, especially in countries where there is less public information". One control proposed by Company B is the completion of google searches, for example street view, web address and media articles throughout the ODD process. Company C refers that one control is conducting "unannounced visits to the companies involved to prove that the company actually exist and has the production capability", although quite impossible to complete for foreign companies. If it has been determined that some companies do not have a physical address or business premises, Company A states that "according to our KYC Policy we wouldn't accept this kind of customers".

5.2 Analysis

The scope of this research is narrowed down to the phenomenon of TBML, and how it can be controlled, based on the latest available information among the banking industry. As stated in the theoretical part of this research, the liberalization of financial markets has been shifting more responsibilities from public sector towards the private sector, and in the light of this research it has influenced how the banks are required to response on money laundering issues. This setting can also be seen in the light of Agency-Principal Theory, where a bank is effectively operating as an agent to the regulator as a principal, but if strict rules and regulations do not exist, the bank will not be as compliant in its AML tasks (Naheem, 2016). This growing responsibility on banks is also extended for setting internal standards on what is expected as normal customer behaviour and what type of actions are undertaken within banks, when abnormal customer behaviour

is detected. Nonetheless, the lack of case studies in the AML field remains as one of the main deficiencies for strengthening governance frameworks within banks, but at least there are some results from actual cases. In one case study conducted by Naheem (2016) related to HSBC bank in the US the main issues in AML controls "were lack of resources to deal effectively with the suspicious alerts that had been filed, high turnover of staff in AML, especially the director, and lack of priority given to addressing any of the issues raised by the OCC (financial regulator)" (p. 232). These types of cases becoming public have further escalated the process of creating stricter rules and regulations for the financial sector in order to mitigate harmful exploitation of bank's role as an agent.

Due to the opening of financial markets and liberation of capital movements across borders, also the issues related to money laundering have elevated to global scale. In order to evaluate possible countermeasures for TBML "particularly the recommendations set out by FATF and the approach taken by the US Government, it is evident that the emphasis is on information gathering and the analysis of data to identify possible TBML activities, with a secondary focus on sharing this information with relevant agencies and authorities" (Sullivan & Smith, 2011). Due to the global outreach and complexity of TBML mechanisms, it becomes difficult to detect suspicious activities without the analysis of trade data and without sharing information across different authorities. As stated by the FATF (2008), "financial and trade data analysis is a useful tool for identifying trade anomalies, which may lead to the investigation and prosecution of TBML/FT cases", which could be followed by developing training programmes for investigative authorities to use trade data and to conduct relevant analysis (p.3). Therefore, stronger response from international organizations, such as the FATF, has been essential to mitigate these globally expanding risks and by the introduction of international standards and especially the risk-based approach, these problems associated with money laundering are aimed to be mitigated. Although freeing up capital movements across borders as well as growing trend of international trade are perceived as highly successful practices for the world economy, it has also laid the foundation for TBML mechanisms to thrive.

In the scope of this research, those financial institutions that have international customer base in their corporate banking business are expected to be the most vulnerable institutions for this threat, and the possible ways of controlling TBML have been targeted for these institutions. By conducting comprehensive research on current knowledge related to TBML, "a series of red flag indicators can be identified, which can then guide the development of localised check lists for different units in the bank" (Naheem, 2018). The research objective has been to raise awareness of TBML, especially when cash-based transactions have become under closer scrutiny and when criminals are expected to move towards more sophisticated methods. This urge to learn more about TBML is further emphasized by the statement of Sullivan & Smith (2011) as "TBML often involves a complex series of transactions and operations to ensure that the value of what is being traded

is concealed or obfuscated; thus, a clearer understanding of TBML and its associated typologies is helpful for those who seek to combat the crime". These red flags and controls introduced in this research are targeted for those who are combating this crime, and the research results can be used for example to draw banks' risk assessment, customer risk profiling and for the purpose of ongoing transaction monitoring.

Due to the existence of illicit actors in the financial world, and their attempts to clean the origins of their ill-gotten funds, our financial institutions as financial intermediators and as the main transmitters of payments are obliged to fight against financial crime. These efforts to combat financial crime are increasingly an on-going project for banks, as there is a tendency for illicit actors to constantly adjust their operations according to current circumstances. This is also referred as crime displacement, and its connection to banking "could be perceived as a combined response to AML regulation and compliance, implying that there is a link between regulatory responses and criminal laundering activity and techniques" (Naheem, 2018). As discussed earlier in this research, money laundering is able to occur when two different parties completing a transaction, whether asking to complete an account payment or providing trade finance products, do not hold the same amount of information on each other. These asymmetric information problems were described as adverse selection and moral hazard problems, briefly defined as hidden information and hidden action, which are essentially the main problems that banks are required to solve when completing customer due diligence. From the perspective of potential money launderer, the intention is to use criminal's informational advantage for completing an illicit transaction, which is aimed to remain unnoticed in the bank. As the rules and regulations are constantly becoming stricter and criminals are searching for ways to gain legitimacy to their actions, there will be increasing demand for sophisticated TBML mechanisms to hide illicit gains (Naheem, 2018). In order to question their legitimacy and to detect informational advantages, the research included several red flags of potential TBML behaviour divided into five main categories, which should be included in the evaluation process of normal customer behaviour.

Based on the collected answers in this research, the foundation for fighting against money laundering is truly knowing the customer, in which contribution from all lines of defence is required to make a holistic evaluation of the customer's business and underlying intentions for customer relationship. In order to combat TBML the emphasis is not only put on training of bank employees but also on the training of different authorities such as trade and investigative authorities as well as banking supervisors with the focus on red flag indicators, typologies and case studies related to TBML (FATF, 2008). In the banking context it was emphasized in the research responses that due to the global scale of TBML banks should have qualified personnel, who are aware of the customer's normal trading patterns in order to be compliant with the CDD requirements. This is mainly the responsibility for the front office staff, which for example in the client

meetings and in discussions about future business plans might be able to detect that customer transaction is not in the scope of normal commercial activity, and therefore should be notified as a red flag (Naheem, 2018). In order to reveal informational advantages and possible opportunistic behaviour from the customer, the research responses highlighted the importance of verifying customer information from reliable external sources. As an example, when bank wants to ensure there are no risks related to phantom shipments, the bill of lading is required to be submitted and its originality is verified from the register of International Maritime Bureau. Additionally, the verification of customer information was mentioned as one of the main controls for both banks' customer and also for verifying information on customer's customer.

There have been several money laundering scandals from the recent past that have become public, and as in the cases of ABLV Bank Latvia and Danske Bank covered in this research, the ignorance of potential money laundering red flags has a severe effect on the share valuation, and might even lead into closure of banks. One of the red flags introduced in these cases was the involvement of complex business structures, that were designed to hide the true beneficial owners of transactions flowing through these banks. In this research, there were several red flags that included complex or opaque business structures, and even though there exists actual business rationale for using such structures, these mechanisms provide attractive facilities for opportunistic behaviour. This can also have an influence on the normal market environment, and as explained in the bad-lemon example by Akerlof (1970), the existence of bad actors in the market may cause a distortion from fair market prices. In the money laundering context if there are banks with low awareness of red flags combined with weak controls, the illicit actors in the market are able to get their monies back to the normal economy, meanwhile generating profits for these banks with weak controls. In this setting, it can be observed that there are similar incentives for criminals and banks to tolerate this type of behaviour, unless there wouldn't be other incentives for banks to operate. One such incentive to mitigate money laundering is derived from the role shift from public authorities to private sector, where banks are increasingly faced with reputational risks if they do not comply with international standards on risk-based approach, the rule for CDD and accurate risk assessments. Through the above mentioned cases of ABLV Bank Latvian and Danske Bank in addition to several other public cases it can be concluded that "the combined costs to the bank of fines, as well as reputational loss and increased resources needing to be focused on AML compliance, means that AML compliance has become a very resource-intensive and costly business" (Naheem, 2018). As failure of complying with AML rules has led to resigning of bank CEO's and other management, caused severe drops in share prices, created damage on bank reputation and influenced negatively on many banking operations, there are increasingly strong incentives for bank management to remain strictly compliant with AML rules and legislations.

The introduction of risk-based approach has become an essential element for AML and CFT supervision in the global scale, which is also reflected in the responses in this research. As highlighted by the FATF (2008) "applying an intelligence, risk-based and target-based approach which makes consistent use of TBML/FT red flag indicators" can be implemented within financial institutions without preventing the flow of legitimate transactions (p.7). There are clear indicators that banks are now accustomed for analysing AML risks for each customer separately and based on those unique risk characteristics related to single customer determines the intensity of risk controls. According to the research responses, if banks identify at least one TBML red flag, whether in transaction monitoring or during due diligence process, it requires closer scrutiny from bank investigators in order to exclude the possible exploitation of TBML mechanisms. In this case if no suspicions are detected, the risk scoring of a customer may remain unchanged and the next inspection of customer due diligence information may be conducted according to normal intervals. On the other hand, if there are more than one red flag identified throughout the process the risks for potential TBML are increased, which according to risk-based approach requires commensurate controls to these risks. As stated in the research responses, in these occasions the customer is frequently profiled as high-risk customer while requiring enhanced due diligence measures in the bank's internal process. In practical application of risk-based approach, this leads into paying closer attention to the information provided by the customer, commencing stricter investigation of information both from internal and external resources and also setting tighter schedule for the next ongoing due diligence checks.

In order to answer for the question who should be responsible on detecting TBML red flags, the respondents clearly indicated that business units and transaction monitoring teams within the first line of defence have the best opportunity to detect any suspicious behaviour. Based on the fact that business units tend to have the best information available related to a customer, both spoken and written information, accompanied with the use of computer systems to detect any anomalies on customer behaviour, especially the employees within the first line of defence should be trained and knowledgeable on TBML mechanisms. In summary, the framework proposed by the risk-based approach requires that all customers are included in the Know Your Customer process but based on the holistic evaluation of risks related to each customer, there should be a closer scrutiny for the customers that provide elevated amount of risks.

6 CONCLUSIONS

In this master's thesis the focus was on increasing awareness of potential TBML methods from an anti-money laundering perspective, and how banks can detect and mitigate risks related to TBML. This task was conducted by collecting potential risk indicators, entitled as red flags, from available publications related to AML, by forming a questionnaire for internationally operating banks and by requesting them to provide their current best practices of controlling against these red flags. This master's thesis originated from the FATF statement that international trade of goods and services is one of the main three methods of how criminals hide their illicit gains, and as internationally operating banks are the main channels for transmitting payments and processing trade transactions there was an increasing demand to learn more how banks can prevent this type of crime. The following estimations, introduced earlier in this research, further emphasized the significance of why money laundering needs to be mitigated as the amount of money laundering is estimated to be approximately 2-5% of the world GDP and the share of illicit flows from total trade in developing countries has been around 20% to 30%. An essential fact related to exploitation of international trade system was introduced by Baker (2005) as he stated "anything that can be priced can be mispriced", which raised both the importance of this problem but also the difficulties for banks to detect TBML (p.25). Due to most of the trade transactions are completed on open account basis and only fifth of total transactions are completed with trade finance products, banks rarely have access to underlying reasons for trade transactions and they are required to detect any suspicious activity from large amount of bank transfer data. This research was directed for banks to learn more about these problems related to TBML and the listing of red flags and their controls was targeted to assist banks in improving their internal risk management processes.

Prevention of money laundering in the banking context is eventually solving problems related to asymmetrical information, where two parties are not holding same information on each other and criminals are capable of exploiting that position with their opportunistic behaviour. This research included discussions over problems related to conducting transactions (ex-ante and ex-post), where red flags were designed to reduce adverse selection problems and monitoring activities and other controls were designed to reduce moral hazard problems. It was confirmed in the research process that potential suspicious behaviour of a customer may arise from wide range of things, which was also seen in the listing of close to 50 red flags under five different categories. As earlier research by Budik & Schlossberger (2015) suggests the growing amount of risk indicators and finding suspicious behaviour may feel like finding a needle in a haystack, more transactions can be investigated by the use of computer systems and constantly developing its algorithms. The research responses clearly identified some of the core elements that are required to be in place in order to combat against TBML, and one of the key points was developing computer systems.

The concept of risk-based approach has created a strong foothold for approaching money laundering risks and setting of controls commensurate to the level of risks has become the core for building efficient AML programs. Based on the research responses, the crime displacement and that way all new forms of financial crime are required to be in bank's horizon, and as there are new emerging trends also there has to be adjustments to transaction monitoring scenarios. Closely attached to emerge of new trends is certainly the need to share information not only between national authorities, such as regulator or financial intelligence units, but also to share more information with the private sector. As discussed by Bergström et al. (2011) banks have better access to client information, which ensures efficient revelation of criminal activities if banks are correctly incentivized and if they are also receiving first-hand information of new money laundering trends. One of the elements for risk-based approach is also to determine what is normal customer behaviour, and bank's systems should be designed to react whenever there are transactions falling out of the ordinary behaviour as emphasized by Bergström et al. (2011). The research responses also underlined the need not only to rely on computer systems, but also to constantly educate bank staff to understand potential money laundering mechanisms. This includes the co-operation between different staff within first line of defence, which was determined of having best information of customer behaviour, to share information of suspicious behaviour based on transaction monitoring data and from actual client interactions.

This master's thesis listed some of the main elements for sound management of money laundering risks, which are essential for organizing internal risk management process while knowing the customer is the central idea. It was evident based on the research responses that only thorough understanding of customer and its business enables banks to detect any suspicious behaviour. This includes e.g. understanding customer's business, knowing normal types to conduct transactions, being familiar with normal trading routes, acquiring more information on customer's customer and verifying information from internal and external sources. Although account managers and other first line staff who are in close interactions with customer have the best information on specific customers, increasing amount of financial data still makes it nearly an impossible challenge to detect suspicious transactions without any effective transaction monitoring systems. As it has been argued by Cassara (2016) "today it is also possible to code or engineer TBML red-flag indicators into traditional AML/CFT software", in which "analytics can provide alerts when there is a likelihood of specific TBML methodologies such as hawala, trade pricing anomalies, the likelihood of trade fraud, and so on" (p.184). This increasing amount of sophistication related to TBML methods makes it more difficult to detect any distortions in price, quality and quantity of goods in underlying trade transaction, which adds more pressure on developing better analysis of trade data and to utilize digital solutions in transaction monitoring.

The purpose for this research was to focus on TBML from banking perspective and to raise awareness for bank employees for detecting this type of behaviour, but there are additional steps that are recommended to be taken to further mitigate these risks. Although banks are playing a major role due to their role in international payments and trade transactions, but the obligation to report suspicious behaviour may be extended to other sectors as well. As suggested by Cassara (2016) all updated FATF recommendations should also be targeted for "transporting or arranging the transport of goods such as brokers, freight forwarders, and carriers", and to also "include manufacturers and companies involved in global trade" (p. 181). This would especially aim to solve the problem where banks rarely have all the available information about a trade transaction in hand, and those companies that are working on trade transactions in practice could identify and report potential illicit behaviour. Although targeting of these measures to other sectors would be a costly project, the requirement for these companies to conduct CDD and to file suspicious activity reports would eventually raise awareness of TBML methods and this could mitigate crime displacement efforts (Cassara, 2016). One additional field, where more research could be targeted to reveal TBML, is in analysis of international trade data and how different countries could share that information whether bilaterally or multilaterally. One of the main efforts in this area has been the establishment of Trade Transparency Units (TTU), which aim to bring together customs authorities and law enforcement agencies in international scale. In practice TTUs have used publicly available and open source data to identify whether trade transactions are completed with distorted trade terms, and by such analysis "TTUs analytic, investigative, and enforcement efforts have identified and disrupted the activities of transnational criminal organizations involved in fraudulent trade schemes" (Cassara, 2016). Analysis of such data and sharing that information for banks could provide significant assistance e.g. for evaluating trade finance documents, developing transaction monitoring scenarios and learning about evolving TBML trends.

As stated earlier in this master's thesis, there are common limitations that influence academic research of AML issues which were also confronted in this research. The first problem is related to lack of data for the actual amount of money laundered globally. As the purpose of money laundering is to hide illicit gains and transfer them back to normal economy, there are significant difficulties for collecting accurate data which enforces authorities to rely on rough estimates on the size of this issue. Therefore, the approach taken for this research was to utilize qualitative methods to determine how banks can improve their processes as there exists limited amount of data to conduct quantitative analysis. One further limitation of this research was related to the sensitivity of TBML, which especially influenced the willingness of banks to share their best practices. As there have been several public cases where banks have been exploited by TBML methods, some of the respondents may have considered not to share information on their internal processes and their approach on tackling TBML. Due to the topicality of TBML, the research was designed not to reveal any possible vulnerabilities that

banks may have in their controls and instead it was designed in the spirit of sharing best-known practices, which could be implemented in other banks as well to combat TBML.

7 REFERENCES

Akerlof, G.A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics, 84*(3), pp. 488-500. Retrieved from http://www.jstor.org/stable/1879431

Alasuutari, P. & Alasuutari, P. (2011). *Laadullinen tutkimus 2.0* (4. uud. p.). Tampere: Vastapaino.

Asia/Pacific Group on Money Laundering. (2012). APG typology report on trade based money laundering. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/reports/Trade_Based_ML_APGReport.pdf

BAFT. (2015). Guidance for Identifying Potentially Suspicious Activity in Letters of Credit and Documentary Collections. Retrieved from http://www.baft.org/Handlers/

BAFT. (2017). Combating Trade Based Money Laundering: Rethinking the Approach. Retrieved from https://baft.org/docs/default-source/marketing-documents/baft17_tmbl_paper.pdf

Baker, R.W. (2005). *Capitalism's achilles heel: Dirty money and how to renew the free-market system.* Hoboken, New Jersey: Wiley & Sons.

Basel Committee on Banking Supervision. (2000, September 27). Principles for the Management of Credit Risk. Retrieved from https://www.bis.org/publ/bcbs75.htm

Basel Committee on Banking Supervision. (2012, September 14). Core Principles for Effective Banking Supervision. Retrieved from https://www.bis.org/publ/bcbs230.htm

Basel Committee on Banking Supervision. (2015, July 8). Corporate Governance Principles for Banks. Retrieved from https://www.bis.org/bcbs/publ/d328.htm

Basel Committee on Banking Supervision. (2017, December 7). Basel III: Finalising post-crisis reforms. Retrieved from http://www.bis.org/bcbs/publ/d424.htm

Bergström, M., Helgesson, K.S., & Mörth, U. (2011). A new role for for-profit actors? The case of anti-money laundering and risk management. *Journal of Common Market Studies*, 49(5), pp. 1043-1064. doi:10.1111/j.1468-5965.2010.02167.x

Bessis, J. (2009). *Risk management of banking (3rd Edition).* Chichester, United Kingdom: Wiley & Sons.

Bovens, M. (2006). Analysing and Assessing Public Accountability: A Conceptual Framework. *European Governance Papers*, Eurogov. Retrieved from http://www.connex-network.org/eurogov/

Budik, J. & Schlossberger, O. (2015). Processes and Technologies for Identifying Illegal Financial Operations. *International Journal of Economics and Business Administration,* III(Issue 2), pp. 22-31. doi:10.35808/ijeba/68

Casu, B., Girardone, C., & Molyneux, P. (2006). *Introduction to banking*. Harlow, England: Pearson Education.

Cassara, J. A. (2016). *Trade-Based Money Laundering: The Next Frontier in International Money Laundering Enforcement.* Hoboken, New Jersey: Wiley.

Cumming, C.M., & Hirtle, B.J. (2001). The challenges of risk management in diversified financial companies. *Economic Policy Review – Federal Reserve Bank of New York, 7(*1), 1-17. Retrieved from http://search.ebscohost.com.ezproxy.jyu.fi/login.aspx?direct=true&db=afh&AN=4324152&site=ehost-live

Darrough, M.N., & Stoughton, N.M. (1984). Moral Hazard and Adverse Selection: The Question of Financial Structure. *The Journal of Finance, 41*(2), pp. 501-513. Retrieved from http://www.jstor.org/stable/2328450

Diamond, D.W. (1984). Financial Intermediation and Delegated Monitoring. *The Review of Economic Studies, 51*(3), pp. 393-414. Retrieved from http://www.jstor.org/stable/2297430

European Banking Authority. (2018). Market Risk. Retrieved from https://eba.europa.eu/regulation-and-policy/market-risk

FATF. (2006). Trade-based money laundering. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/Trade%20Based%20Money%20Laundering.pdf

FATF. (2007). Laundering the proceeds of VAT carousel fraud report. Retrieved from http://www.fatf-gafi.org/publications/methodsandtrends/documents/launderingtheproceedsofvatcarouselfraudreport.html

FATF. (2008). Best practices on trade based money laundering. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/recommendations/BPP%20Trade%20Based%20Money%20Laundering%202012%20COVER.pdf

FATF. (2010). Money laundering vulnerabilities of free trade zones. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/reports/ML%20vulnerabilities%20of%20Free%20Trade%20Zones.pdf

FATF. (2012). International standards on combating money laundering and the financing of terrorism proliferation: the FATF recommendations. Retrieved from http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

FATF. (2014). Guidance for a risk-based approach: The banking sector. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf

FATF. (2014). Guidance on transparency and beneficial ownership. Retrieved from https://www.fatf-gafi.org/fr/themes/recommandationsgafi/documents/transparency-and-beneficial-ownership.html?hf=10&b=0&s=desc(fatf_releasedate)

FATF. (2016). FATF Guidance: Correspondent banking services. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Correspondent-Banking-Services.pdf

FATF. (2018). Concealment of beneficial ownership. Retrieved from https://www.fatf-gafi.org/publications/methodsandtrends/documents/concealment-beneficial-ownership.html

FATF. (2019, February 12). What is money laundering? Retrieved from https://www.fatf-gafi.org/faq/moneylaundering/

Financial Conduct Authority. (2013). Banks' control of financial crime risks in trade finance. Retrieved from https://www.fca.org.uk/publication/thematic-reviews/tr-13-03.pdf

Freixas, X., & Rochet, J.C. (2008). *Microeconomics of banking*. Cambridge, the United States: The MIT Press.

Ghauri, P. and Gronhaugh, K. (2005). *Research Methods in Business Studies: A Practical Guide*. Prentice Hall.

Global Financial Integrity. (2019, February 2). Illicit financial flows to and from 148 developing countries: 2006-2015. Retrieved from https://www.gfintegrity.org/wp-content/uploads/2019/01/GFI-2019-IFF-Update-Report-1.29.18.pdf

International Chamber of Commerce. (2018). Global trade: Securing future growth. Retrieved from https://iccwbo.org/publication/global-survey-2018-securing-future-growth/

Jensen, M. & Meckling, W. 1976. Theory of the firm: managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3, 305-360.

Joint Committee of the European Supervisory Authorities (2017, June 26). Final Guidelines on Risk Factors. Retrieved from https://eba.europa.eu/esas-publish-aml-cft-guidelines

Khanna, M (2019). *Trade Based Money Laundering – Capturing the New Frontier through Analytics* [White Paper]. Retrieved from https://www.acams.org/aml-white-paper-trade-based-money-laundering-analytics/

Leland, H.E. & Pyle, D.H. (1977). Informational asymmetries, financial structure, and financial intermediation. *The Journal of Finance, 32*(2), pp. 371-387.

Matthews, K. & Thompson, J. (2005). *The Economics of Banking*. Hoboken, New Jersey: Wiley & Sons.

Matussek, K., Comfort, N. & Arons, S. (2018, November 29). *Deutsche Bank raided in laundering probe going into 2018.* Retrieved from https://www.bloomberg.com/news/articles/2018-11-29/deutsche-bank-headquarters-searched-in-money-laundering-probe

Naheem, M. A. (2016). Risk of money laundering in the US: HSBC case study. *Journal of Money Laundering Control, 19*(3), pp. 225-237. doi:10.1108/JMLC-01-2015-0003

Naheem, M. A. (2017). Trade based money laundering: A primer for banking staff. *Int J Discl Gov, 14(*2), pp. 95-117. doi:10.1057/jdg.2015.21.

Naheem, M. A. (2018). Is tackling Trade Based Money Laundering (TBML) through stricter reporting regulation the most effective response? *Journal of Money Laundering Control, 21*(3), pp. 345-357. doi:10.1108/JMLC-08-2015-0034

Neale, D. (2019, January 9). *Taking stock of 2018's money laundering scandals: When is enough enough? (Part 2).* Retrieved from https://gfintegrity.org/taking-stock-of-2018-part-2/

Schumpeter, J. A. (1939). *Business cycles: A theoretical, historical and statistical analysis of the capitalist process.* Vol. 1 (3rd impr.). New York: McGraw-Hill.

Soudijn, M.R.J. 2014. A critical approach to trade-based money laundering. Journal of Money Laundering Control, Vol. 17 Issue: 2, pp.230-242.

Stake, R. E. (2010). *Qualitative research: Studying how things work*. New York: Guilford Press.

Sullivan, C. & Smith, E. (2011). Trade-based money laundering: Risks and regulatory responses. *Research and Public Policy, 115*, p. i.

The Wolfsberg Group. (2017). Trade finance principles. Retrieved from http://www.baft.org/docs/default-source/policy-department-documents/final-clean-trade-finance-principles-final.pdf?sfvrsn=2

U.S. Department of the Treasury. (2018). National Money Laundering Risk Assessment 2018. Retrieved from https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf

United Nations Office on Drugs and Crime. (2011). Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes. Retrieved from https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf

World Trade Organization. (2016). World trade statistical review 2016. Retrieved from https://www.wto.org/english/res_e/statis_e/wts2016_e/wts2016_e.pdf

World Trade Organization. (2018). World trade statistical review 2018. Retrieved from https://www.wto.org/english/res_e/statis_e/wts2018_e/wts2018_e.pdf

APPENDIX 1 RESEARCH QUESTIONNAIRES

Company A

Questionnaire: Red Flags and Controls

Red Flags in Customer & Business Structure	Controls	Line of Defense Responsible of Escalation
The shipment is inconsistent with the importer or exporter's normal business (e.g., an exporter of consumer electronics shipping paper supplies)	Efficient KYC Process. Checking the documents e.g. invoices and available documents. Compairing the information to the customer's line of business.	Trade Finance (1. LoD)
The size of the shipment appears inconsistent with the scale of the importer or exporter's regular business activities	Efficient KYC Process. Checking the documents e.g. invoices and available documents. Compairing the information to the customer's line of business e.g. turnover	Trade Finance (1. LoD)
A shipment of goods destined for an end-user has no need for the product (e.g., electronics manufacturing equipment sent to a destination that does not have an electronics industry)	N/A. It is the responsibility for the issuing bank to know its customers. On the other hand the isuuing banks are usually our correspondent banks. In some cases we investigate from the open sources if the customer has that line of business.	

Red Flags in Transaction, Goods & Payment	Controls	Line of Defense Responsible of Escalation
The method of payment is inconsistent with the normal business practice of the parties involved or inconsistent with the characteristics of the transaction	The bank has to know its customers and understand the structure of the deal. One of the red flags can be that the terminology differs from the standard practise. The structure appears to be too complicated compared to underlying transaction.	Trade Finance, Finance (1. LoD)
The method of payment appears inconsistent with the risk characteristics of the transaction (e.g., the use of an advance payment for a shipment from a new supplier in a high-risk country)	The bank has to know its customers and understand the structure of the deal. It is typical for the new business relationship to use advance payments. However special attention should be payed to percentage of advance payment (100% very unusual). The structure appears to be too complicated compared to underlying transaction.	Trade Finance (1. LoD)
Transaction involves shipment of goods inconsistent with normal geographic trade patterns of the jurisdiction (trade in goods other than goods which are normally exported/imported)	The bank has to know its customers and understand the structure of the deal.	Trade Finance, Cash Management (1. LoD)
International wire transfers are received as payment for goods into bank accounts where the exporter is not located	The bank has to know its customers.	Cash Management (1.LoD)

Payment is made from multiple sources and/or multiple accounts	Transaction monitoring process includes scenarios where payment is incoming from multiple sources and/or accounts and based on possible scenarios these transactions are escalated into further investigation.	AML Team (1 LoD), AML Compliance (2 LoD)
The transaction and payment appear to have unnecessary and complex layers involving multiple accounts and multiple jurisdictions that combine to obscure the true nature of the transaction	Transaction monitoring process includes scenarios where payment appear to have unnecessary and complex layers involving multiple accounts and multiple jurisdictions that combine to obscure the true nature of the transaction and based on possible scenarios these transactions are escalated into further investigation.	AML Team (1 LoD), AML Compliance (2 LoD)
The transaction involves the use of repeatedly amended or frequently extended letters of credit	The bank has to know its customers and understand the structure of the deal. This is normal practise in many cases. Not typical in ML, since they usually want to get the money back asap.	Trade Finance (1. LoD)
Transactions that involve payments for goods through checks, drafts, or money orders are not drawn on the account of the entity that purchased the items	The bank has to know its customers.	Cash Management (1.LoD)
The transaction involves the receipt of cash (or other payments) from third party entities that have not apparent connection with the transaction	The bank has to know its customers.	Cash Management (1.LoD)
Unusual deposits of cash, cash deposits in round numbers, or structured deposits under the reporting threshold into a bank account are used to fund the trade transaction	Transaction monitoring process includes scenarios where unusual deposits of cash, cash deposits in round numbers, or structured deposits under the reporting threshold into a bank account are used to fund the trade transaction and based on possible scenarios these transactions are escalated into further investigation.	AML Team (1 LoD), AML Compliance (2 LoD)
Sequentially numbered checks drawn on domestic bank accounts are negotiated through foreign money services businesses.	N/A	
Significant discrepancies appear between the value of of the commodity reported on the invoice and the commodity's fair market value	We do not have the resources to assess the fair market value. However knowledge of common values are known to the bank.	Trade Finance (1. LoD)
Related-party transactions are involved (e.g., familial relationships).	The bank has to know its customers.	1 LoD
Carousel tranasctions are involved - the repeated or circular importation and exportation of the same high-value commodity	The bank has to know its customers.	
Phantom shipment - no goods are actually shipped but payment is made	The bank has to know its customers. Occationally random checks are made whether the ship has actually visited the port. It is possible to send B/L to be authenticated by The ICC International Maritime Bureau (IMB).	Trade Finance (1. LoD)
There are multiple invoices for suspect goods. A frequently repeated suspect pattern of numerous invoices involves the same or similar items and where the actual physical shipment is never physically verified	N/A	Trade Finance (1. LoD)

The exporter request payment of proceeds to an unrelated third party	The bank has to know its customers. The reasons for payments to unrelated parties must be investigated.	Trade Finance (1. LoD)
In guarantees issued on behalf of exporter the beneficiary may request assignment of proceeds	In case the assigment of proceeds is allowed in the guarantee, the bank has to check that the third party is not sanctioned.	Trade Finance (1. LoD)
Goods that are commonly associated with TBML schemes are involved (e.g., scrap gold, precious metals and stones, trade in tobacco, consumer electronics, automobiles, etc.).	The bank has to know its customers.	Trade Finance (1. LoD)
Goods present valuation difficulties (precious stones, artwork, scrap gold, etc.).	The bank has to know its customers. We do not have the resources to assess the fair market value. However knowledge of common values are known to the bank.	
Goods involved are frequently used in bartering schemes (e.g., gasoline and tires).	N/A	
Goods do not comply with applicable import or export regulations, or involve dual-use (e.g. technology, software, chemicals etc.) and high-risk goods	The bank may require a copy of the import or export license or a certification from the importer/exporter that the required license has been obtained or that no license is required.	Trade Finance (1. LoD)

Red Flags in Shipment Structure	Controls	Line of Defense Responsible of Escalation
The commodity is being shipped to/from or through areas of "high risk" for money laundering.	The bank has to know its customers. In these kind of cases the bank pays special attention to the customer's business, the documentations, and the parties involved. The issuing or advising bank has to be our correspondent bank.	Trade Finance (1. LoD)
The routing of the shipment is circuitous, not direct, is illogical, or is being transshipped through a questionable area for no apparent economic reason	If it is possible not to take part to these kinds of transactions, we wouldn't participate. In order to avoid tipping off, we would participate and then make the SAR.	Trade Finance (1. LoD)
Shipments involve suspect free trade zones or special economic zones	In collection this might be possible. Goods are consigned to the freight-forwarder in order to make sure the buyer doesn't get hold of the goods without payment.	Trade Finance (1. LoD)
A freight-forwarding firm is listed as the commodity's final destination.		
A shipment does not make economic sense (e.g. the use of 40-foot shipping container to transport a relatively small volume of goods)	n/a. The container can be used by more than one company. The bank doesn't have the competence to assess this kind of information concerning the container or vessel.	Trade Finance (1. LoD)

Red Flags in Documentation	Controls	Line of Defense Responsible of Escalation
Significant discrepancies exist between the description, quality, and quantity of the commodity on the bill of lading, invoice, and actual goods shipped.	The documents are rejected by the banks. Payments not effected.	Trade Finance (1. LoD)
Significant deviation between the value of the commodity as reported on the invoice and a normal "arm's-length" fair-market price.	We do not have the resources to assess the fair market value. However knowledge of common values are known to the bank	Trade Finance (1. LoD)

The weight of the shipment does not match the listed contents	In case the documents are in descrepancy, we reject the documents. The bank does not necesserarly have the competence to assess the weight of the shipment.	Trade Finance (1. LoD)
Invoices or bills of lading include inaccurate information about the product being shipped or information that is not commonly accepted (e.g., an invoice listing the square feet of granite tile being imported when the accepted norm is pricing by the ton)	In case the documents are in discrepancy or the information is inconsistent, we reject the documents.	Trade Finance (1. LoD)
Invoices contain inaccurate or incomplete product descriptions; for example, an invoice for 1,000 kilograms of frozen shrimp is not sufficient to analyze its market value because there are multiple U.S. harmonized codes for frozen shrimp reflecting imports of different sizes	In case the documents are in descrepancy, we reject the documents.	Trade Finance (1. LoD)
Documentation appears fraudulent	We wouldn't participate, and we would make a SAR and inform the Fraud Department.The bank would try to assess the genuity of the B/L.	Trade Finance, Finance (1. LoD)
A party is unable or unwilling to produce appropriate documentation upon request	We wouldn't participate, and we would make a SAR and inform the Fraud Department.	1. LoD
Shipment locations or description of goods are not consistent with the letter of credit	In case the documents are in discrepancy or the information is inconsistent, we reject the documents.	Trade Finance (1. LoD)
The quantity or quality of the goods is padded or inflated	We would need more information to reply.	
Counterfeit invoices are used	We wouldn't participate, and we would make a SAR and inform the Fraud Department.	1. LoD
Packaging is inconsistent with the commodity or shipping method involved	In case the documents are in descrepancy, we reject the documents. The bank might not have enough experience regarding commodities/shipping methods	Trade Finance (1. LoD)
Common red flags for LC fraud including incorrect use of banking terms, spelling mistakes and errors in grammar and composition	Special attention is being made to terminology especially guarantees.	Trade Finance (1. LoD)
The letter of credit contains non-standard clauses or phrases	We wouldn't participate, and we would make a SAR and inform the Fraud Department.The bank would try to assess the genuity of the L/C.	Trade Finance (1. LoD)

Red Flags in Intermediaries, Deal Parties & Third Parties	**Controls**	**Line of Defense Responsible of Escalation**
Companies are operating out of foreign countries where it is very difficult to determine the true ownership or controlling persons of the company or where the type of business is not fully apparent	The bank has to know its customers. Our customers carry out their own KYC, and when necessary, we ask more detailed information about their processess. We don't offer services to such companies. The issuing or advising bank has to know its customers.	Trade Finance (1.LoD)

The transaction involves a third party that has no apparent connection to the buyer or seller	We check the third party against sactions. When necessary, we would investigate the role of the third party.	Trade Finance (1.LoD)
The transaction involves the use of front or shell companies	The bank has to know its customers. We wouldn't do business with shell or front companies.	1. LoD
The parties involved are not transparent and use "Delaware" -like shell corporations with lack of beneficial ownership information	The bank has to know its customers. Our customers carry out their own KYC, and when necessary, we ask more detailed information about their processess. We don't offer services to such companies. The issuing or advising bank has to know its customers.	1. LoD
Numerous sole-proprietorship businesses or private limited companies are involved in the transaction or established by proxies or where false addresses are involved	The bank has to know its customers. Our customers carry out their own KYC, and when necessary, we ask more detailed information about their processess. We don't offer services to such companies. The issuing or advising bank has to know its customers.	1. LoD
Money services businesses or money exchange bureaus located in third countries are used as intermediaries for the transfer of goods or money	N/A	
Upon inspection or verification, the manufacturing entity has no physical address, no or limited production capability, limited or no inventory at its business premises, and so on.	According to our KYC Policy we wouldn't accept this kind of customers without physical address and business premises.	1. LoD

Company B

Questionnaire: Red Flags and Controls

Red Flags in client & Business Structure	Controls	Line of Defense Responsible of Escalation
The shipment is inconsistent with the importer or exporter's normal business (e.g., an exporter of consumer electronics shipping paper supplies)	Trade Finance only handle transactions with clients and banks that are fully onboarded/KYC'ed. We know clients line of business and also normal trading patterns. Should additional information be required the account manager is contacted. Depending on the clarification we will decide whether or not to handle the transaction.	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
The size of the shipment appears inconsistent with the scale of the importer or exporter's regular business activities	Trade Finance only handle transactions with clients and banks that are fully onboarded/KYC'ed. We know client line of business and also normal trading patterns. If inconsistencies appears, the account manager is contacted subsequently the client. Depending on the clarification we will decide whether or not to handle the transaction.	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).

A shipment of goods destined for an end-user has no need for the product (e.g., electronics manufacturing equipment sent to a destination that does not have an electronics industry)	Trade Finance does not always know our customer's customer line of business in advance. However through the external portal of Bureau Van Dijk Trade Finance can verify the buyers line of business and exsistence. If the outcome is not satisfactory we will take contact to the client and ask for clarification. Depending on the clarification we will decide whether or not to handle the transaction.	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).

Red Flags in Transaction, Goods & Payment	Controls	Line of Defense Responsible of Escalation
The method of payment is inconsistent with the normal business practice of the parties involved or inconsistent with the characteristics of the transaction	Customers use different payment methods and risk mitigating instruments based on their individual risk policies. However we are only handling Trade Finance transactions with clients and banks that are fully on-boarded/KYC'ed. Should goods/payment methods/structure of transactions be inconsistent with the normal business practice, then the client and account manager are contacted in accordance with our SOP for Red Flags. Depending on the explanations we will decide whether or not to handle the transaction. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
The method of payment appears inconsistent with the risk characteristics of the transaction (e.g., the use of an advance payment for a shipment from a new supplier in a high-risk country)	Customers use different payment methods and risk mitigating instruments based on their individual risk policies. However we are only handling Trade Finance transactions with clients and banks that are fully on-boarded/KYC'ed. Should goods/payment methods/structure of transactions be inconsistent with the normal business practice, then the client and account manager are contacted in accordance with our SOP for Red Flags. Depending on the explanations we will decide whether or not to handle the transaction. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Transaction involves shipment of goods inconsistent with normal geographic trade patterns of the jurisdiction (trade in goods other than goods which are normally exported/imported)	All the global changing trading patterns are challenging to be aware of. However we are only handling Trade Finance transactions with clients and banks that are fully on-boarded/KYC'ed. Trade Finance knows the client line of business and normal trading patterns. Should additional information be required the account manager is contacted according to our SOP's. Depending on the explanations we will decide whether or not to handle the transaction. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).

International wire transfers are received as payment for goods into bank accounts where the exporter is not located	Considered as a red flag by Transaction Monitoring in alert. Transaction anlysis in ODD is also control mechanism.	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Payment is made from multiple sources and/or multiple accounts	Considered as a red flag by Transaction Monitoring in alert. Transaction analysis in ODD is also control mechanism.	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
The transaction and payment appear to have unnecessary and complex layers involving multiple accounts and multiple jurisdictions that combine to obscure the true nature of the transaction	We are only doing traditional Trade Finance transactions. However, if a Trade Finance transaction appears unnecessary complex, the client and the account manager are contacted according to our SOP's. Depending on the explanations we will decide whether or not to handle the transaction. If there is no rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
The transaction involves the use of repeatedly amended or frequently extended letters of credit	The business reasons of the frequent amendments are clarified with the client in accordance to our SOP's. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Transactions that involve payments for goods through checks, drafts, or money orders are not drawn on the account of the entity that purchased the items	Considered as a red flag by Transaction Monitoring in alert. Transaction anlysis in ODD is also control mechanism.	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
The transaction involves the receipt of cash (or other payments) from third party entities that have not apparent connection with the transaction	Considered as a red flag by Transaction Monitoring in alert. Transaction anlysis in ODD is also control mechanism.	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Unusual deposits of cash, cash deposits in round numbers, or structured deposits under the reporting threshold into a bank account are used to fund the trade transaction	Transaction monitoring scenarios, limits at deposit ATMS and transaction analysis during ODD. Caught easily	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).

Sequentially numbered checks drawn on domestic bank accounts are negotiated through foreign money services businesses.	Checks are used rarely in Finland	
Significant discrepancies appear between the value of of the commodity reported on the invoice and the commodity's fair market value	The true market value of the goods is challenging to determine especially in tailor made goods. However obvious discrepansies will be addressed according to our Red Flags SOP. We will seek explanations from the client and contact the account manager. Depending on the explanations we will decided whether or not to handle the transaction. Knowing clients' trading patterns, normal line of business and having experienced personnel are key to mitigate this.	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Related-party transactions are involved (e.g., familial relationships).	We are only handling Trade Finance transactions with clients and banks that are fully on-boarded/KYC'ed. In case of a related-party transactions the business rationale is determined in cooperation with the account manager based the clients clarification.	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Carousel tranasctions are involved - the repeated or circular importation and exportation of the same high-value commodity	We are only handling Trade Finance transactions with clients and banks that are fully on-boarded/KYC'ed. In case of any unusual transactions the business rationale is determined after discussions with the client in accordance the SOP. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Phantom shipment - no goods are actually shipped but payment is made	In case of any suspicious shipments, we are using the service of external provider IMB (International Maritime Bureau) in orderto verify the accuracy of the information stated in the B/L. The IMB verification is done prior to any payment. In case of inconsistency => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
There are multiple invoices for suspect goods. A frequently repeated suspect pattern of numerous invoices involves the same or similar items and where the actual physical shipment is never physically verified	We are not sure how to interpret this. However to verify that actual shipment has taken place, the orginal transport document is needed (L/Cs). In case of any suspicious shipments, we are using the service of external provider IMB (International Maritime Bureau) in orderto verify the accuracy of the information stated in the B/L. The IMB verification is done prior to any payment. In case of inconsistency => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
The exporter request payment of proceeds to an unrelated third party	If this should happen the business rationale is determined in discussion with the client. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).

Goods that are commonly associated with TBML schemes are involved (e.g., scrap gold, precious metals and stones, trade in tobacco, consumer electronics, automobiles, etc.).	We are only handling Trade Finance transactions with clients and banks that are fully on-boarded/KYC'ed. Involvement of such goods always leads to further investigation. The client and the account manager are contacted for clarification. Customer can also be asked to sign declaration (risk based approach) confirming the compliance of export control regulation. Depending on the clarification we will decide whether or not to handle the transaction. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Goods present valuation difficulties (precious stones, artwork, scrap gold, etc.).	We are only handling Trade Finance transactions with clients and banks that are fully on-boarded/KYC'ed. Involvement of such goods always leads to further investigation. The client and the account manager are contacted for clarification. Customer can also be asked to sign declaration (risk based approach) confirming the compliance of export control regulation. Depending on the clarification we will decide whether or not to handle the transaction. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Goods involved are frequently used in bartering schemes (e.g., gasoline and tires).	We are only doing Traditional Trade Finance which is not involving barter trade. However should such a situation occur it would be a Red Flag, requiring further investigation according to our compliance screening process.	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Goods do not comply with applicable import or export regulations, or involve dual-use (e.g. technology, software, chemicals etc.) and high-risk goods	We are only handling Trade FInance transactions with clients and banks that are fully on-boarded/KYC'ed. Dual use is a part of our SOP's. If a transaction is to high risk areas and/or involves obvious dual use goods: 1. we have dialog with the client on the export control regulations 2. we will ask the client to sign a declaration confirming that they adhere to OFAC sanctions and EU sanctions and export control regulations and/or 3. To verify that we can also ask for the export license	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Red Flags in Shipment Structure	**Controls**	**Line of Defense Responsible of Escalation**

The commodity is being shipped to/from or through areas of "high risk" for money laundering.	In certain high-risk areas we need customer to sign a declaration confirming the compliance of export control regulation. In case of an unusual complex shipment structure, We will contact the account manager in order to verify that the transaction is within the clients business profile. Depending on the clarification we will decide whether or not to handle the transaction. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
The routing of the shipment is circuitous, not direct, is illogical, or is being transshipped through a questionable area for no apparent economic reason	In certain other high-risk areas we need customer to sign a declaration confirming the compliance of export control regulation. In case of an unusual complex shipment structure, we are using the service of external provider IMB (International Maritime Bureau) in order to verify the accuracy of the shipment information. Depending on the clarification we will decide whether or not to handle the transaction. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Shipments involve suspect free trade zones or special economic zones	In case of an unusual complex shipment structure, we are using the service of external provider IMB (International Maritime Bureau) in order to verify the accuracy of the shipment information. Through the external portal of Bureau Van Dijk, Trade Finance can verify the buyers line of business and exsistence. Depending on the clarification we will decide whether or not to handle the transaction. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
A freight-forwarding firm is listed as the commodity's final destination.	Should we receive such a transaction the client are contacted for clarification. Depending on the clarification we will decide whether or not to handle the transaction. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
A shipment does not make economic sense (e.g. the use of 40-foot shipping container to transport a relatively small volume of goods)	If a shipment does not make economic sence or obvious irregularities spotted in the documents we will take contact to the client and ask for clarification. Depending on the clarification we will decide whether or not to handle the transactionn. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).

Red Flags in Documentation	Controls	Line of Defense Responsible of Escalation

Significant discrepancies exist between the description, quality, and quantity of the commodity on the bill of lading, invoice, and actual goods shipped.	Obvious discrepansies will be addressed according to our Red Flags SOP. We will seek explanations from the client and contact the account manager. Depending on the explanations we will decided whether or not to handle the transaction. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Significant deviation between the value of the commodity as reported on the invoice and a normal “arm’s-length” fair-market price.	The true market value of the goods is challenging to determine especially in tailor made goods. Obvious irregularities are addressed according to our Red Flags SOP. We will seek explanations from the client and contact the account manager. Depending on the explanations we will decided whether or not to handle the transaction. Knowing clients' trading patterns, normal line of business and having experienced personnel are key to mitigate this. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
The weight of the shipment does not match the listed contents	Obvious discrepancies will be addressed according to our Red Flags SOP. We will seek explanations from the client and contact the account manager. Depending on the explanations we will decided whether or not to handle the transaction. Knowing clients' trading patterns, normal line of business and having experienced personnel are key to mitigate this. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Invoices or bills of lading include inaccurate information about the product being shipped or information that is not commonly accepted (e.g., an invoice listing the square feet of granite tile being imported when the accepted norm is pricing by the ton)	Obvious discrepansies will be addressed according to our Red Flags SOP. We will seek explanations from the client and contact the account manager. Depending on the explanations we will decided whether or not to handle the transaction. Knowing clients' trading patterns, normal line of business and having experienced personnel are key to mitigate this. If there is no rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Invoices contain inaccurate or incomplete product descriptions; for example, an invoice for 1,000 kilograms of frozen shrimp is not sufficient to analyze its market value because there are multiple U.S. harmonized codes for frozen shrimp reflecting imports of different sizes	Obvious discrepansies will be addressed according to our Red Flags SOP. If a goods desription is too generic we will seek explanations from the client. Depending on the explanations we will decided whether or not to handle the transaction. Knowing clients' trading patterns, normal line of business and having experienced personnel are key to mitigate this. If there is no rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Documentation appears fraudulent	If documents appear fraudulent it would be a full stop pending result of a further investigation hereunder verfication of the B/L at IMB. Despite the result such a transaction should be escalated	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).

A party is unable or unwilling to produce appropriate documentation upon request	If satisfactory clarification, explanation or documentation is not provided upon request we are not allowed to proceed with the transaction according to our SOP => Escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Shipment locations or description of goods are not consistent with the letter of credit	Obvious discrepansies will be addressed according to our Red Flags SOP. We will seek explanations from the client and contact the account manager. Depending on the explanations we will decided whether or not to handle the transaction. Knowing clients' trading patterns, normal line of business and having experienced personnel are key to mitigate this. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
The quantity or quality of the goods is padded or inflated	We are only handling Trade Finance transactions with clients and banks that are fully on-boarded/KYC'ed. If documents appear fraudulent it would be a full stop pending result of a further investigation. Despite the result such a transaction should be escalated	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Counterfeit invoices are used	If documents appear fraudulent it would be a full stop pending result of a further investigation hereunder verfication of the B/L at IMB. Despite the result such a transaction should be escalated	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Packaging is inconsistent with the commodity or shipping method involved	Obvious inconsistences will be addressed according to our Red Flags SOP. We will seek explanations from the client and contact the account manager. Depending on the explanations we will decided whether or not to handle the transaction. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Common red flags for LC fraud including incorrect use of banking terms, spelling mistakes and errors in grammar and composition	Unusual wording/structure will be addressed according to our Red Flags SOP. We will seek explanations from the client and contact the account manager. Depending on the explanations we will decided whether or not to handle the transaction. If there is no rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
The letter of credit contains non-standard clauses or phrases	Unusual wording/structure will be addressed according to our Red Flags SOP. We will seek explanations from the client and contact the account manager. Depending on the explanations we will decided whether or not to handle the transaction. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).

Red Flags in Intermediaries, Deal Parties & Third Parties	**Controls**	**Line of Defense Responsible of Escalation**

Companies are operating out of foreign countries where it is very difficult to determine the true ownership or controlling persons of the company or where the type of business is not fully apparent	We are only handling Trade FInance transactions with clients and banks that have been fully on-boarded/KYC'ed. All involved parties are screened against EU, UN & OFAC sanction lists. In certain other high-risk areas we need customer to sign a declaration confirming the compliance of export control regulation. In certain high risk countries/transactions beneficial ownerships is investigated and parties exsistence and line of business are verified through the external portal of Bureau Van Dijk. If required information is not obtainable then we not handle the transaction => escalation.	Group Financial Crime in sanction matters and SARO in suspected money laundering (Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR))
The transaction involves a third party that has no apparent connection to the buyer or seller.	If a third parties with no relation to the buyer or the seller appears in a transaction will be consider suspicious. The business rational will be determined in cooperation with the client. Depending on the explanations we will decide whether or not to handle the transaction. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
The transaction involves the use of front or shell companies	If a transaction appears to involve a Front or Shell company. the transaction will be consider suspicious. The business rational will be determined in cooperation with the client. Depending on the explanations we will decide whether or not to handle the transaction. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
The parties involved are not transparent and use "Delaware" -like shell corporations with lack of beneficial ownership information	If the involved parties appear suspcious in structure and the required information is not obtainable. The business rational will be determined in cooperation with the client. Depending on the explanations we will decide whether or not to handle the transaction. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Numerous sole-proprietorship businesses or private limited companies are involved in the transaction or established by proxies or where false addresses are involved	We are only handling Trade FInance transactions with clients and banks that have been fully on-boarded/KYC'ed. All involved parties are screened against EU, UN & OFAC sanction lists. In certain high risk countries/transactions beneficial ownerships is investigated and parties exsistence and line of business are verified through the external portal of Bureau Van Dijk. If required information is not obtainable then we will not handle the transaction => escalation.	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).

Money services businesses or money exchange bureaus located in third countries are used as intermediaries for the transfer of goods or money	Transaction analysis (ODD) and transaction monitoring	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).
Upon inspection or verification, the manufacturing entity has no physical address, no or limited production capability, limited or no inventory at its business premises, and so on.	We are only handling Trade FInance transactions with clients and banks that have been fully on-boarded/KYC'ed. Should it occur the business rational will be determined in cooperation with the client. Depending on the explanations we will decide whether or not to handle the transaction. If there is no business rationale => escalation	Business Units and Transactions Monitoring team will escalate all suspicious findings (UAR) to SARO and SARO will escalate them to the authorities after their own analysis (SAR).

Company C

Questionnaire: Red Flags and Controls

Red Flags in Customer & Business Structure	Controls	Line of Defense Responsible of Escalation
The shipment is inconsistent with the importer or exporter's normal business (e.g., an exporter of consumer electronics shipping paper supplies)	Effective know your customer (KYC) procedure and fundamental understanding of the core business of the client.	1st line
The size of the shipment appears inconsistent with the scale of the importer or exporter's regular business activities	Effective know your customer (KYC) procedure and fundamental understanding of the core business of the client.	1st line
A shipment of goods destined for an end-user has no need for the product (e.g., electronics manufacturing equipment sent to a destination that does not have an electronics industry)	Effective know your customer (KYC) procedure and fundamental understanding of the core business of the client. Thorough understanding of the supply chain of the customer and its end-user. Know your customer's customer and also the recipients of the customer.	1st line

Red Flags in Transaction, Goods & Payment	Controls	Line of Defense Responsible of Escalation
The method of payment is inconsistent with the normal business practice of the parties involved or inconsistent with the characteristics of the transaction		
The method of payment appears inconsistent with the risk characteristics of the transaction (e.g., the use of an advance payment for a shipment from a new supplier in a high-risk country)		
Transaction involves shipment of goods inconsistent with normal geographic trade patterns of the jurisdiction (trade in goods other than goods which are normally exported/imported)		

International wire transfers are received as payment for goods into bank accounts where the exporter is not located		
Payment is made from multiple sources and/or multiple accounts		
The transaction and payment appear to have unnecessary and complex layers involving multiple accounts and multiple jurisdictions that combine to obscure the true nature of the transaction		
The transaction involves the use of repeatedly amended or frequently extended letters of credit		
Transactions that involve payments for goods through checks, drafts, or money orders are not drawn on the account of the entity that purchased the items		
The transaction involves the receipt of cash (or other payments) from third party entities that have not apparent connection with the transaction	Effective KYC procedure and due diligence of the transaction in question. KYC and KYC of customer's customer or counter party. Transaction monitoring and cash scenario identifies new counterparties and recognises if the payment to client's account comes from an unknown sender. Screening of the parties.	1st line / 2nd line (monitoring activity)
Unusual deposits of cash, cash deposits in round numbers, or structured deposits under the reporting threshold into a bank account are used to fund the trade transaction		
Sequentially numbered checks drawn on domestic bank accounts are negotiated through foreign money services businesses.		
Significant discrepancies appear between the value of of the commodity reported on the invoice and the commodity's fair market value		
Related-party transactions are involved (e.g., familial relationships).		
Carousel tranasctions are involved - the repeated or circular importation and exportation of the same high-value commodity		
Phantom shipment - no goods are actually shipped but payment is made	Effective KYC procedure and due diligence of the transaction. Controlling and assessing the documentation of the trade transaction.	1st line
There are multiple invoices for suspect goods. A frequently repeated suspect pattern of numerous invoices involves the same or similar items and where the actual physical shipment is never physically verified	Effective KYC procedure and due diligence of the transaction. Controlling and assessing the documentation of the trade transaction.	1st line
The exporter request payment of proceeds to an unrelated third party	Effective KYC procedure and due diligence of the transaction. Understanding of the ownership structure of the client and identifying all the parties to the trade, including the end user. Indicator that triggers the bank to ask more questions. Screening of the parties involved.	1st line
Goods that are commonly associated with TBML schemes are involved (e.g., scrap gold, precious metals and stones, trade in	Effective KYC procedure. If any such product is involved it immediately triggers an enhanced due diligence procedure.	1st line

tobacco, consumer electronics, automobiles, etc.).		
Goods present valuation difficulties (precious stones, artwork, scrap gold, etc.).		
Goods involved are frequently used in bartering schemes (e.g., gasoline and tires).		
Goods do not comply with applicable import or export regulations, or involve dual-use (e.g. technology, software, chemicals etc.) and high-risk goods	Effective KYC procedure. If the transaction is related to any high risk country, involves any high-risk goods or is subject to any sanctions, before each transaction the client needs to confirm the bank of certain facts related to the tansaction and goods. If the trade is subject to export lisence, then the client has to provide it whenever asked. The client also has to assess whether the goods are dual-use goods or are used for military purposes. In addition to this the client is obliged to tell the Bank whether there is any oil/gas industry connection and to spesifically what geographical area the goods will be shipped to and why.	1st line

Red Flags in Shipment Structure	Controls	Line of Defense Responsible of Escalation
The commodity is being shipped to/from or through areas of "high risk" for money laundering.	If the transaction is in any way related to any high risk country an enhanced due diligence procedure as well as escalation procedure will take place. The client is obliged to give more detailed information of the transaction, purpose of the transaction, end use etc.	1st line
The routing of the shipment is circuitous, not direct, is illogical, or is being transshipped through a questionable area for no apparent economic reason	If the transaction is in any way related to any high risk country an enhanced due diligence procedure as well as escalation procedure will take place. The client is obliged to give more detailed information of the transaction, purpose of the transaction, end use etc.	1st line
Shipments involve suspect free trade zones or special economic zones	If the transaction is in any way related to any high risk country an enhanced due diligence procedure as well as escalation procedure will take place. The client is obliged to give more detailed information of the transaction, purpose of the transaction, end use etc.	1st line
A freight-forwarding firm is listed as the commodity's final destination.		
A shipment does not make economic sense (e.g. the use of 40-foot shipping container to transport a relatively small volume of goods)	If the transaction is in any way related to any high risk country an enhanced due diligence procedure as well as escalation procedure will take place. The client is obliged to give more detailed information of the transaction, purpose of the transaction, end use etc.	1st line

Red Flags in Documentation	Controls	Line of Defense Responsible of Escalation

Significant discrepancies exist between the description, quality, and quantity of the commodity on the bill of lading, invoice, and actual goods shipped.	Effective know your customer (KYC) procedure and fundamental understanding of the core business of the client. Thorough understanding of the supply chain of the customer and its end-user. Know your customer's customer and also the end-user.The client is asked to correct the documentation accordingly and if not fulfilled the transaction needs the acceptance from the counterparty.	1st line
Significant deviation between the value of the commodity as reported on the invoice and a normal "arm's-length" fair-market price.		
The weight of the shipment does not match the listed contents		
Invoices or bills of lading include inaccurate information about the product being shipped or information that is not commonly accepted (e.g., an invoice listing the square feet of granite tile being imported when the accepted norm is pricing by the ton)		
Invoices contain inaccurate or incomplete product descriptions; for example, an invoice for 1,000 kilograms of frozen shrimp is not sufficient to analyze its market value because there are multiple U.S. harmonized codes for frozen shrimp reflecting imports of different sizes		
Documentation appears fraudulent	Effective know your customer (KYC) procedure and fundamental understanding of the core business of the client. Understanding the trade zone within which the transaction is carried out. Escalation procedure and enhanced due diligence of the transaction and customer.	1st line
A party is unable or unwilling to produce appropriate documentation upon request	Effective know your customer (KYC) procedure and fundamental understanding of the core business of the client. Understanding the trade zone within which the transaction is carried out. Escalation procedure and enhanced due diligence of the transaction and customer.	1st line
Shipment locations or description of goods are not consistent with the letter of credit		
The quantity or quality of the goods is padded or inflated		
Counterfeit invoices are used	Effective know your customer (KYC) procedure and fundamental understanding of the core business of the client. Understanding the trade zone within which the transaction is carried out. Naturally the documentation is reviewed by product specialists before accpeting those. When necessary escalation procedure and enhanced due diligence of the transaction and customer.	1st line
Packaging is inconsistent with the commodity or shipping method involved		
Common red flags for LC fraud including incorrect use of banking terms, spelling mistakes and errors in grammar and composition		

The letter of credit contains non-standard clauses or phrases	Effective know your customer (KYC) procedure and fundamental understanding of the core business of the client. Understanding the trade zone within which the transaction is carried out. Each document and its wording is reviewed when received. Furthermore it will be assessed whether the documentation is fit for its purpose or whether additional information is needed. Escalation procedure and enhanced due diligence of the transaction and customer.	1st line

Red Flags in Intermediaries, Deal Parties & Third Parties	Controls	Line of Defense Responsible of Escalation
Companies are operating out of foreign countries where it is very difficult to determine the true ownership or controlling persons of the company or where the type of business is not fully apparent	Effective KYC procedure and fundamental understanding of the core business of the client. Thorough understanding of the supply chain of the customer and its end-user. Know your customer's customer and also the end-user. Escalation procedure immediately when a high risk country/industry/nationality is involved in the transaction. Enhanced due diligence on counterparties and sanctions screening.	1st line
The transaction involves a third party that has no apparent connection to the buyer or seller	Effective KYC procedure and due diligence of the transaction in question. KYC and KYC of customer's customer or counter party. Transaction monitoring and cash scenario identifies new counterparties and recognises if the payment to client's account comes from a unknown sender. Trigger to ask more questions from the customer. Screening of the parties.	1st line/2nd line (monitoring activity)
The transaction involves the use of front or shell companies	Effective KYC procedure and due diligence of the transaction in question. KYC and KYC of customer's customer or counter party. Transaction monitoring and cash scenario identifies new counterparties and recognises if the payment to client's account comes from a unknown sender. Trigger to ask more questions from the customer. Enhanced due diligence of counterparties, and further questions from the client.	1st line
The parties involved are not transparent and use "Delaware" -like shell corporations with lack of beneficial ownership information	Effective KYC procedure and due diligence of the transaction in question. KYC and KYC of customer's customer or counter party. Transaction monitoring and cash scenario identifies new counterparties and recognises if the payment to client's account comes from a unknown sender. Trigger to ask more questions from the customer. Enhanced due diligence of counterparties, and further questions from the client.	1st lin
Numerous sole-proprietorship businesses or private limited companies are involved in the transaction or established by proxies or where false addresses are involved	Effective KYC procedure and due diligence of the transaction in question. KYC and KYC of customer's customer or counter party. Transaction monitoring and cash scenario identifies new counterparties and recognises if the payment to client's account comes from a unknown sender. Trigger to ask more questions from the customer. Enhanced due diligence of counterparties, and further questions from the client.	1st line

Money services businesses or money exchange bureaus located in third countries are used as intermediaries for the transfer of goods or money		
Upon inspection or verification, the manufacturing entity has no physical address, no or limited production capability, limited or no inventory at its business premises, and so on.	Effective KYC procedure and fundamental understanding of the core business of the client. Thorough understanding of the supply chain of the customer and its end-user. Know your customer's customer and also the end-user. Escalation procedure immediately when a high risk country/industry/nationality is involved in the transaction. Unannounced visits to the companies involved to prove that the company actually exist and has the production capability.	1st line