Lebanese American University

Trade-Based Money Laundering: Trends, Developments and Challenges in Banking Institutions

By

Mahmoud Fakih

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Business Law

Adnan Kassar school of Business
May 2022

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

THESIS APPROVAL FORM

Student Name: Mahmoud Fakih I.D. #: 202000006

Thesis Title: Trade-Based Money Laundering: Trends, Developments and Challenges

Program: LLM

Department:

School: Adnan Kassar School of Business

The undersigned certify that they have examined the final electronic copy of this thesis and approved it in Partial Fulfillment of the requirements for the degree of:

LLM in the major of Business Law

Thesis Advisor's Name: William Melki

Signature: [redacted] Date: / /
Day Month Year

Committee Member's Name: [redacted]

Signature: [redacted] Date: 5 / 9 /2022
Day Month Year

Committee Member's Name: Abbas Tarhini

Signature: [redacted] Date: / /
Day Month Year

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

THESIS COPYRIGHT RELEASE FORM

LEBANESE AMERICAN UNIVERSITY NON-EXCLUSIVE DISTRIBUTION LICENSE

Name: Mahmoud Fakih

Signature: [redacted]

Date: 19 / 05 / 2022
Day Month Year

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

PLAGIARISM POLICY COMPLIANCE STATEMENT

I certify that:

1. I have read and understood LAU's Plagiarism Policy.
2. I understand that failure to comply with this Policy can lead to academic and disciplinary actions against me.
3. This work is substantially my own, and to the extent that any part of this work is not my own I have indicated that by acknowledging its sources.

Name: Mahmoud Fakih

Signature: [redacted]

Date: 19 / 05 / 2022
Day Month Year

ACKNOWLEDGMENT

This project would not have been possible without the support of many people.

Many thanks to my advisor Me. William Melki, who read my numerous revisions and helped make some sense of the confusion. Also, thanks to my committee members, Dr. Abdul Nasser Kassar, Dr. Abbas Tarhini and to the LAU's Director of Legal Studies, Dr. Khodr Fakih for supporting me throughout the LLM program.

Trade-Based Money Laundering: Trends, Developments and Challenges in Banking Institutions

Mahmoud Fakih

ABSTRACT

Being a Certified Anti-Money Laundering Specialist since 2016, and an expert in combatting money laundering and terrorist financing for a period exceeding 9 years, where I worked in three Alfa banks in Lebanon (BLOM, Bankmed, and Creditbank); and considering my current position as Head of Legal Compliance at Creditbank sal, I prepared this thesis on the trends and developments of Trade-based Money Laundering (TBML) and the related risks and challenges faced by the banking sector.

As one of the basic methods in the money laundering and terrorist financing framework, this study aims to identify and explore the methods used in TBML. We will highlight on how criminals are using TBML to conceal the features of their crime within routine transactions that result from commercial activities and international trade in its various aspects and forms. TBML happens in countless ways where the criminals have access to the financial institutions, particularly, the banking sector, and are able to hide the source of their funds and make it appear as legitimate.

On the other hand, we will focus on the difficulties faced by the banking sector in combating this type of money laundering and the gaps that the criminals exploit to launder their proceeds through international trade. We will also shed the light on the international legislations and laws, global recommendations, exchange of information between countries, and policies and procedures adopted by the banks, in order to limit the expansion of TBML.

The main objective of this study is to give a comprehensive idea about the concept of TBML and spreading the knowledge and increasing cultural awareness regarding the risks that this crime could pose, and to find modern and effective ways to fight it.

In my research, I relied on live interviews with specialists in combating money laundering and terrorist financing, and on several real cases that took place in the banking sector.

KEYWORDS: TBML – AML/CFT – Sanctions – Monitoring – Screening – Correspondent Banks – KYC – Customer Due Diligence – Data mining – Training – FIU – Investigations – FinTech.

TABLE OF CONTENTS

Chapter **Page**

List Of Abbreviations

ML – Money Laundering

FT – Financing of Terrorism

AML – Anti-Money Laundering

CFT – Counter Financing of Terrorism

NSCR – Netherlands Institute for the Study of Crime and Law Enforcement

FATF – Financial Action Task Force

SAR – Suspicious Activity Report

IMF – International Monetary Fund

BMPE – Black Market Peso Exchange

FTZ – Free Trade Zone

CTR – Cash Transaction Reports

DEA – Drug Enforcement Administration

ISIS – Islamic State of Iraq and Syria

OCG – Organized Crime Group

ABF – Australian Border Force

LCB – Lebanese Canadian Bank

ICC – International Chamber of Commerce

UCP – Uniform Customs and Practices

KYC – Know Your Customer

RBA – Risk Based Approach

PEP – Politically Exposed Person

CDD– Customer Due Diligence

EDD – Enhance Due Diligence

LC – Letter of Credit

MAS – Notice on the Sale of Investment Products

IMO – International Maritime Organization

TTU – Trade Transparency Unit

FIU – Financial Intelligence Unit

UNSCR – U.N. Security Council Resolution

IVTS – Informal Value Transfer System

CHAPTER ONE

INTRODUCTION

1.1 Overview

Despite being created very recently, "money laundering" and "anti-money laundering (AML) have become well-known legal words and legal research areas around the world since the 1980s. Money laundering has evolved into a multinational crime that poses a threat to each state and the international community.

Money laundering (ML) has accumulated a significant amount of value throughout time. Just in Europe, ML of drug trafficking revenues generates legal cash ranging from US$ 71,5 billion if the criminal sector launders money in South Eastern Europe to US$ 108.72 billion if the cleaning process is carried out in Eastern Europe. ML is intimately linked to the relevant upstream offenses, despite the fact that it is a stand-alone felony. Such heinous crimes generate a large quantity of unlawful earnings, which must be laundered to reduce transaction costs. Indeed, the use of these illicit funds could raise the chances of a crime being discovered and, as a result, of incrimination.

Experts in organized crime and money laundering employ a range of tactics, but they all share some common qualities, such as a heavy reliance on cash. Laundering takes place in a variety of places, including casinos, petrol stations, restaurants, the real estate industry, and other legitimate enterprises.

Banking and financial intermediaries are crucial in the execution of these laundering schemes. Money laundering takes place in the financial system, which by definition includes banks. Anti-money laundering initiatives usually target the financial sector as a result.

In this paper, we define the concept of Trade-based money laundering and discuss the demand side characteristics. Then, a discussion of some TBML techniques is proposed, as well as a quantitative study of the phenomena. Finally, we make some policy recommendations.

Money laundering through trade has become one of the most common ways for criminal groups and terrorist sponsors to transfer money. Because the funds can be buried within ostensibly legitimate economic activities, stronger banking rules have made this strategy more appealing. The TBML/FT typology, on the other hand, can be exceedingly complicated, and to those unfamiliar with its subtleties, it can easily appear as real trade activity. Traditional and developing TBML/FT tactics, as well as standard compliance program processes, are examined in this study to establish the steps banking institutions might take to combat this behavior. Money laundering tactics based on trade are diverse. As a result, banking institutions can't rely on compliance investigators to spot them. Instead, compliance programs must employ a diverse strategy and make full use of all available resources. Instead, compliance programs must employ a diverse strategy and make full use of all available resources. The proposals are meant to help banking institutions detect TBML behavior through industry-specific training, data analysis, and collaboration with other organizations fighting this type of value transfer.

1.2 Scope of the Problem

Banks are the most commonly used instruments in money laundering and thus the most vulnerable. They are appealing attractive for illicit funds movement because they offer a variety of goods, such as wire transfers and checks, as well as the simplicity of moving funds over international borders. Furthermore, bank secrecy regulations restrict information banking institutions may discuss with one another and with law enforcement, making them more appealing to criminal groups and terrorist funders. Regulators, on the other hand, hold institutions accountable for any criminal behavior aided by the financial system, culminating in the issuing of Consent Orders and huge monetary fines for numerous banks and companies that fall under the banking institution umbrella. As a result, it is in the best interests of banking institutions to identify and report suspicious conduct as soon as it is noticed, and to prevent it from happening as much as feasible.

The issue here is detecting TBML-related activity among the many transactions that banking institutions process on a daily basis. Monitoring software and warning scenarios are frequently used in anti-money laundering and counter-terrorist financing (AML/CTF) compliance programs to automatically identify suspicious conduct, such as structured cash transactions or wire activity with high-risk countries. Investigative team examines the alarms provided by the monitoring program and determines whether they belong to a specific approach. The manual element of this procedure is highly subjective, and the complexity of TBML raises the possibility of it being mistaken for normal trading operations. In contrast, because TBML activity is frequently concurrent with routine trade activity, genuine commerce may be regarded as suspicious. Melvin Soudijn (a senior researcher in the Central Unit of the Netherlands National Police and a research fellow of the “Netherlands Institute for the Study of Crime and Law Enforcement (NSCR))“ discovered that the methods described for facilitating TBML activity were too narrowly focused on misrepresentation of value, quantity, or quality of goods in his review of the available literature. Soudijn goes on to say that present definitions don't take into account the trade of services, the fact that TBML doesn't have to be international, or even provide clarity on what a trade transaction is. Unfortunately, without the necessary paperwork and training to distinguish between legitimate and illegitimate financial activity within business accounts, TBML activity can be difficult to identify as being linked to illicit money movement from the perspective of banking institutions.

The strengthening of rules on wire and check transfer activities, as well as on the actual movement of funds, according to the FATF (2006), appears to have shifted money laundering activity away from these means and toward the international commerce system (p. 2). The growing use of casino, real estate, cryptocurrency, and front business transactions to launder money seems to back up this theory. Furthermore, former Treasury Department Special Agent Cassara has called trade-based money laundering "*perhaps the largest and most pervasive money laundering methodology*" (Trading with the Enemy, 2016, p. 7). Despite this, depository institutions reported only 1,120 Suspicious Activity Reports (SARs) for TBML in 2017, compared to 733,899 SARs filed for money laundering and terrorist financing (FinCEN, 2018b). Either the activity isn't passing via the banking system, or it isn't being identified as TBML-related. Several of the other suspicious activity descriptions are for transaction types that could suggest the presence of TBML activity, implying either a reluctance on the part of depository institutions to identify activity as TBML or a lack of awareness about its signs.

1.3 Objective/Purpose

Previous debates on combating TBML have centered on information sharing from trade regulation organizations and situational crime prevention, both of which take place outside of the banking institution setting. The goal of this mixed-methods study is to see what steps banking institution compliance procedures can take to lessen the possibility of misidentifying behaviour that could be suggestive of TBML. Traditional and emerging TBML methods will be reviewed in order to better comprehend the methodology's complexity and to discover currently available instruments for detecting illicit trade activities. Identification of signs that can be noticed at the banking institution level will be possible with a greater understanding of how criminal trade activity is used by organizations and terrorist financiers to move funds. The research for this paper will also into potential methods for better detecting TBML activities within banking institutions. These potential solutions will include everything from a review of the coverage strategy and its ability to automate the detection of suspicious activity to ways to improve the ability of anti-money laundering (AML) compliance staff to correctly recognize and report TBML-related activity during an investigation. In reference to the huge volume of operations and transactions treated by banking institutions on a daily basis, it is critical that the indicators of this methodology be recognized, not only to reduce the risk of facilitating illicit transactions on an organizational level, but also to improve the escalation of TBML activity to law enforcement via SAR filings.

CHAPTER TWO

DEFINITIONS

2.1 What is Money Laundering?

There are several ways to define money laundering, but the majority of countries and international organizations that give great attention to this subject agree with the definition given by the Vienna Convention on the concept of money laundering being a transfer or converter of property derived from crimes and suspicious commercial operations and activities (drugs, human trafficking, murders...), with full knowledge that these activities are illegal in order to conceal their origin with the aim of making them appear as legitimate revenues from a legal and clean business, or with the aim of helping the perpetrators and participants in these crimes and suspicious acts to evade the legal consequences and risks resulted from these types of crimes.

Initially, the Vienna Convention considered that not all crimes could be classified as of money laundering crimes indicative.

On the other hand, the “Financial Action Task Force on money laundering (FATF)”, in its international standards, defined money laundering using the same technical, principles and legal definition adopted and clarified by the Vienna Convention, with an additional criteria added to the crimes classified as money laundering act by including all serious crimes.

2.2 Stages of Money Laundering

2.2.1 Placement

It is the most dangerous stage of the three money laundering stages. The launderer will try to hide his crime or transfer its illegal proceeds/income/revenues to a safe place and sector such as the financial system, by depositing these funds directly in several sectors for trading, such as casinos, banking institutions, shops, and others in order to escape any investigations from the authorities.

At this stage, the money launderer usually opens many numbers of bank accounts with several different names. The purpose of these accounts is to divide the large amounts of cash resulting from the crime and deposit them in these accounts in small amounts in an attempt to remove suspicions.

Or, he will deposit funds in foreign banking institutions by shipping funds across borders or by purchasing goods and services with a high market value with the intention of reselling and receiving payment by bank transfers and checks.

2.2.2 Layering

At this stage, the money launderer aims to conceal the illegal source of funds and to hide its origin by transferring the funds between accounts that were opened in various banking institutions during the first stage in a complex manner that would be difficult to track and audit. Money launderers at this stage rely on the development of the financial system, especially banks, that allows them to execute several quick wire transfers in a matter of seconds between scattered accounts in various banks around the world.

Example of transactions used for layering:

- Transfer from account to another;
- Transferring/converting cash into gold;
- Reselling goods purchased in a high value;

- Using shell banks registered in external areas.

2.2.3 Integration

In the last stage, money launderers legitimize their money, thus it becomes difficult to differentiate between legitimate and illegal money.

By this stage, the purpose of money laundering has been achieved and the money laundering process/scheme has been successfully completed, and money launderers reach their money and begin to move it and integrate it into the financial system as being clean, and in legitimate commercial and investment activities such as real estate and others.

2.3 Terrorism Financing

Terrorist gangs frequently obtain finances through criminal behavior, even if their ultimate purpose is not always financial gain. The primary goal of a terrorist organization is to force a populace or government into carrying out or refraining from carrying out a specific act or conduct. Terrorist groups require banking backing to achieve their goals, and they frequently operate in relative anonymity, employing unique finance systems such as cash couriers, transfer, Hawala, generate assets through coherent networks and the internet to store.

It's worth noting that a number of international treaties have failed to agree on a universal definition of terrorism. It's perplexingly difficult to describe terrorism globally without considering the nature of the crime or the tactic employed. As a result, definitions differ and are based on specific frameworks determined by the competent agency (Sorel, 2003). In "Article 2 of the UN International Convention for the Suppression of Terrorist Financing," which was approved in 1999, terrorism finance is described as follows:

> *"Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act." (UN, 1999).*

Terrorism financing, according to the IMF, is the process through which individuals or organizations collect funds with the goal of using those funds to carry out terrorist attacks. This procedure is detailed in the "International Convention for the Suppression of Terrorist Financing and its Annexes (IMF, 2003)". Terrorism finance, according to the World Bank's (2009) definition, is *"any type of financial assistance for terrorism, or those who conspire, participate, and promote the execution of terrorist activities"*.

2.4Trade-based Money Laundering (TBML)

"The Financial Action Task Force (FATF)", an intergovernmental organization that sets standards for anti-money laundering, counter-terrorist financing, and other financial crime prevention, in their report issued in 2006, has defined 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 illegal origin or finance their activities"*.

As per FATF, the primary purpose of TBML is to exploit international trade transactions in order to transfer illegal revenues and gains from them and to give legitimacy on their source. Thus, the differences arising from ordinary money laundering methods are based on the process of exchanging goods and services by transferring them between countries through the contracts signed between the parties. In this context, there are several illegal activities that criminals engage in when committing this type of crime, such as submitting false invoices, tampering or forging it (a significant difference between the market value of goods and services from those that are dealt with), or trying to exploit loopholes related to controls on goods and fraud upon them and other tax and customs violations.

In 2015, two reports related to money laundering were issued by the "U.S. Department of the Treasury". One of these reports is the *National Money Laundering Risk Assessment* that stated and described TBML as one of the most dangerous, challenging and complicated scheme of money laundering concept, because it is difficult to monitor and investigate. Annually, TBML scheme is capable to launder billions of dollars. An advisory on TBML issued on February 2010 by the "Treasury Department's Financial Crimes Enforcement Network (FinCEN)" showed approximately 17,000 Suspicious Activity Reports (SARs) as TBML potential activity, which include transactions with a total amount of $276 billion between years 2004 and 2009.

CHAPTER THREE

TRADE-BASED MONEY LAUNDERING BACKGROUND

3.1 Common TBML Techniques

The first step of a TBML mechanism begins when two parties enter into a fraudulent contract by placing special conditions on that contract that creates fraud such as billing. This invoice is the main element in the cooperation between the seller and the buyer for the exchange of goods and services. Thus, the two parties, the importer and the exporter, are able quite easily to commit fraud jointly with each other, and to manipulate the invoice and its derivatives in proportion to their personal interests to reach the goal and transfer the dirty money through it.

According to FATF, there are several activities executed for committing fraudulent invoice in TBML techniques. These activities are determined as follow:

3.1.1 Over- and under-invoicing of goods and services:

This method of TBML is one of the most common and oldest techniques in the world. It requires complicity between merchants in the process of importing and exporting goods and services, and it cannot succeed or reach its goal in the absence of cooperation between them, because it is based on increasing or decreasing the value of invoices until the settlement of accounts between them in the stage following shipment of goods by the exporter and receipt by the importer, whether it actually or hypothetical happened.

The mechanism of increasing invoices is done in agreement between the buyer or importer and the exporter or the seller, raising the value of goods and services more than their market value approved in the global markets and trade. Thus, upon payment, the buyer transfers the invoiced value to the seller, which exceeds the value of the real goods and services in the market. This difference in value serves as a legitimate cover for the illicit source of funds. As for the process of reducing invoices, the exporter or the seller reduces the value of the goods and services below their global market value, in agreement with the buyer or the importer. The latter pays the reduced value to the seller, then resells them at their market value and settles the account with the seller regarding the reduction.

Therefore, it is clear from this mechanism that it is difficult for the supervisory authorities and banking institutions to monitor and detect them due to the collusion between the commercial parties in this process, especially since these parties take advantage of the weakness of the supervisory controls related to money laundering in many countries, and collude with foreign companies or establish subsidiaries to send wrong bills and transfer of illegal funds against them.

3.1.2 Multiple invoicing of goods and services:

In order to create more complexity in the commercial process, merchants or money launderers aim through this technique to present several invoices in the form of payments related to the same shipment. Thus, several parties participate in this mechanism to justify this. In comparing with the above-mentioned method, here it is not necessary to reduce or increase the value of goods and services or the invoice and is not related to the prices of goods and services traded globally, but the goal is to transfer illegal funds from multiple parties involved in this mechanism and trying to provide legitimate reasons to justify it.

Banking institutions or the competent supervisory authorities can often detect this type of illicit activity. Money launderers then present some arguments or excuses as an indication of the legitimacy of these payments and justify them in different ways, such as changing the previously agreed payment rules, or the occurrence of sudden factors that led to a change in agreement or the emergence of previous financial payments that were not taken into account.

3.1.3 Over- and under-shipments of goods and services:

It is a process of collusion between the parties, the exporter and the importer. It is based on reducing the number of goods when shipped or not shipping any of them at all. Therefore, the shipping process in this case is fictitious, and the mechanism for processing all customs transactions, bills of lading and the related supporting documents remain in place with the aim of disguising, removing suspicions and adding more complications to the process. The main purpose of this technique is to transfer funds across borders. This technique is a combination of the mechanism of manipulating the prices of goods and services on one hand, and the mechanism of multiple invoices on the other hand.

In this mechanism, both parties benefit from it because the decrease in the quantity of goods mentioned in the commercial invoices and the documents provided enable the seller obtaining legitimate money in exchange for a fake shipment that did not occur in the first place, and the buyer will also benefit from the transfer of illegal money to be laundered across the border through pay the value of these invoices or goods that he did not receive. In the end, the two sides settle scores between themselves. In most cases, this fake process takes place without the banking institutions knowing about it, despite the scrutiny of their papers and the documents that prove them.

3.1.4 Falsely described goods and services:

This mechanism is based on misrepresentation in the descriptions, information and quality of the characteristics of the goods and services to be shipped. This technique aims to confuse and mislead the regulatory authorities, especially the customs authorities, because they are authorized to check the quality of these goods. Like other techniques, it always takes place with the complicity and agreement between the exporter and the importer.

This technique works in two different ways and benefit both parties: In the first, expensive goods are shipped and the quality of these goods is distorted and tampered by indicating them on the bills of lading as being cheap and inexpensive. The purpose of this act is to transfer the additional value to the importer for resale at the market price. In the second, cheap goods are shipped and their quality is distorted and tampered in bills of lading and the documents necessary for them as being expensive.

In addition, sometimes goods and services whose market value is difficult to determine, especially for services that may be shipped, so that the trading process is linked and governed by bilateral price negotiations through which their market value is difficult, and money launderers adopt camouflage through this method to mislead the regulatory authorities.

3.1.5 Phantom shipments:

In this technology, no goods will be shipped and there will be no shipping process at all. Thus, the forged and submitted documents and shipping papers are a cover for the fictitious shipping process to give it the status of legitimacy. In this technique, the price or quantity of goods mentioned in the documents and commercial transaction papers is not tampered with, and this technique does not depend/rely on these elements.

The latter method is considered one of the least used by money launderers, as it poses a risk to them if the transaction raises suspicions with the supervisory authorities because it will become difficult for them to submit any new related documents to the fake shipping transaction. As a result, the transaction will end under investigation.

3.2 Black Market Peso Exchange

The Black-Market Peso Exchange (BMPE) is a good example of a more intricate TBML technique used to launder drug proceeds by Central and South American drug cartels. The origins of the Black-Market Peso Exchange can be traced back to legitimate business and Colombian government policy. In the 1960s, the Colombian government adopted a legislation prohibiting any Colombian national from holding any money other than the Colombian Peso, in response to an influx of currency made up of earnings from the coffee business, which depreciated the Colombian Peso and caused financial instability. Colombians had two options for purchasing products outside of the country: utilize a bank, which was prohibitively expensive, or use an informal means of exchange, in which private "brokers" converted Colombian Pesos to foreign currencies.

This technique of exchange is somewhat similar to currency trading on the black market in Lebanon, which appeared after the events of October 17, 2019 and the deterioration of the economic and financial situation in it.

The technique of BMPE was used by narcotics traffickers who wanted to launder large amounts of money (mostly US dollars) earned through drug trafficking. The broker usually receives the dollars from the drug cartel's network of cash controls and uses them to pay the US supplier in Black Market Peso Exchange schemes. Depending on the scheme's complexity, the broker can either pay the supplier directly or deposit the money in several bank accounts via structured deposits, then wire the funds to the suppliers. The goods are subsequently exported from the United States to companies in Central and South America, which then transfer local cash to a local money broker. After that, the money broker sends the drug cartel local currency minus commission. This technique assures that no cash is transferred between jurisdictions where it could be discovered and intercepted by law enforcement agencies.

3.2.1 Black Market Peso Exchange Real Case

In January 2020, the US Justice Department indicted six Colombian people for their roles in one of an international money laundering scheme employing TBML and unregistered money transmission businesses used, in collaboration with an Indian individual.

The scheme's goal was to launder drug-trafficking money, principally through a Black-Market Peso Exchange-style method that kept currency in the United States from being physically transferred.

The conspiracy revolved around Colombian nationals reportedly acting as money brokers, receiving illegal gains from couriers around the United States as well as receiving incoming international wire transfers. To avoid raising suspicion, the physical currency was introduced into the US financial system before being transferred to the Indian national's business bank account, which was handled by an accused complicit merchant. The retailer sold consumer gadgets to buyers all across the world, including Colombian importers.

The merchant shipped roughly the same amount of consumer goods to Colombian importers, who agreed to pay for the goods by delivering pesos to Colombian money brokers, who then passed the money on to the drug trafficking organization. This eliminated the need for drug traffickers to try any cross-border currency movement, lowering their chance of detection.

The case study also emphasizes complicit exporters and importers' persistent dependence on peso exchange channels and the abuse of lawful commercial connections to move comparable value from the United States to Colombia.

3.3 COVID-19 and TBML

The coronavirus pandemic has provided white collar criminals with a slew of new opportunities, particularly in international trading. Criminals may try to invest their illicit funds in struggling enterprises or persuade them to launder money on their behalf, taking advantage of the more distressed business climate. COVID-19 has resulted in higher demand for specific goods and services, such as pharmaceuticals, textiles, and personal protective equipment (PPE), as well as supply chain disruption on a worldwide scale. The pandemic has increased the risk of fraud and or money laundering for trade nationally and internationally, according to the UK's National Risk Assessment 2020. The disruption of supply chains means "a pivot to new and potentially unfamiliar clients, increasing the risk of fraud and or money laundering for trade nationally and internationally."

The epidemic has also aggravated some of the prevalent TBML trends:

- **Counterfeit goods**: We've noticed an increase in counterfeit or rebranded commodities like personal protective equipment, as well as an increase in phantom shippings, where no equipment is shipped at all, or when the same cargo is subject to multiple invoicing. Several law enforcement organizations and regulators, including Interpol, Europol, UNODC, and FinCEN, have issued alerts about probable counterfeiting of COVID-19.
- **Reduced monitoring**: Remote working and social distancing have hindered parties' ability to undertake trade finance checks because TBML screening is still heavily reliant on human inspection and forensic knowledge of physical documents involved.
- **Corruption:** Some commodities have had their prices fraudulently increased under the guise of being in high demand. Due to the increasing demand for PPE and pharmaceutical products, supply chain middlemen have had greater opportunities to overcharge, as buyers and end users are sometimes uninformed of the true cost price and are pressured to buy due to a pressing necessity.

3.4Free Trade Zones and TBML

FTZs, also known as free ports, are regions "where commodities may be landed, handled, manufactured or reconfigured, and re-exported without the interference of customs authorities." Customs taxes/duties are imposed only when items/goods are delivered to customers within the country where the zone is located. Throughout 3,000 FZs exist around the world now, and they certainly provide a significant opportunity to stimulate economic growth and investment. For example, Prime Minister Boris Johnson of the United Kingdom has declared plans to establish up to ten free ports in the country following Brexit.

FTZs, on the other hand, constitute a significant financial crime risk, prompting the European Union to call them a "new emerging hazard" and discourage their development, as well as the FATF to declare them places of heightened TBML risk in its 2020 report.

The duty status and special tariffs connected with FTZs have frequently been linked to insufficient AML and CFT precautions, lax procedures for inspecting products held, a lack of cooperation with customs authorities, and a lack of transparency standards.

Massive free trade zones are used by drug traffickers who want to avoid detection by transporting large amounts of goods. FATF, for example, gives a case study depicting a worldwide drug trafficking cell with clear links to drug cartels in South America and Islamic extremist organizations in the Middle East in its "Money Laundering Vulnerabilities of Free Trade Zones" report. The network apparently had a central ML operation and was able to channel drug proceeds through a number of enterprises in Panama's “Colon Free Zone (CFZ)”.

Lack of transparency requirements made it impossible to follow shipments to, from, and between enterprises in different zones in this case, as well as many others involving FTZs. Despite the fact that cash transaction reports (CTRs) and suspicious transaction reports (STRs) were required, "the practice of filing was not enforced, and clients paying in cash for goods in the zone were not subject to any customer due diligence procedures," according to the report. Due to a lack of adequate surveillance and screening, the criminal network at hand was able to develop, with tentacles eventually reaching the United States, Asia, and Europe.

For example, Dubai’s multiple free trade zones promote illicit financial and commercial activity, particularly TBML, thanks to the emirate’s loose regulatory atmosphere.

The emirate's ambivalence about uncontrolled financial activities and illegal trade has a long and profound history. Dubai's civil legal frameworks, unlike other sharia-based legal systems, lack adequate anti–money laundering regulation and control, reflecting the long history of UAE’s as a freewheeling regional commercial center. As a result, Dubai has become one of the most favorable locations for TBML.

3.5 New Payments Methods and New Challenges

Terrorist financiers and criminal groups respond to restrictions and controls by devising new and imaginative ways to wash money. They also find ways to get around current controls by employing systems that allow them to conceal their identities and the scope of their operations. This section discusses several new TBML approaches as well as the additional problems encountered by anyone who would try to stop it. It should be noted, however, that several of the approaches discussed are so new that there is little scholarly information accessible on them.

Illicit money have been layered and integrated using casino gambling and real estate transactions. The Royal Canadian Mounted Police discovered a TBML operation in British Columbia, Canada, in 2015, in which Chinese citizens were recruited to gamble with money obtained through narcotics trafficking and use the earnings to buy luxury houses. Money was transmitted to Mexico and Peru for narcotics purchases, accompanied by fraudulent trade invoices for Chinese items, by the money transfer business behind the activities (Cooper, 2017a). Some transactions were linked to Iranian companies suspected of being involved in terrorist financing, according to an investigation (Cooper, 2017b). Another recently discovered technique involves transferring value through Amazon's self-publishing book business. Phony books are made and listed at exorbitant costs in order to discourage regular people from buying them. The buyer then buys the bogus book at the inflated list price, and Amazon pays the publisher 60% of the list price (Pressman, 2018).

The use of digital money transfer services, cryptocurrencies, prepaid cards, and virtual currencies as vehicles to move value in internet-based world contexts is referred to as New Payment Methods. The capacity to transact on a worldwide scale, along with the anonymity provided by encryption and remote transfer, makes these transactions appealing, as does the difficulties in ascertaining jurisdictional authority for any unlawful conduct. According to the FAFT (2010), anonymity can be achieved by employing products that do not need client identity or by evading limitations on tailored products by using stolen identification or straw-men (individuals who agree to deal on behalf of others). New payment mechanisms have become more generally accepted in recent years, and in some countries, they now offer a viable alternative to traditional financial systems (pp. 7-9).

Digital money transfer services: The internet has made payment easier by allowing consumers to make payments and send money using their phones (Litan & Baily, 2009, pp. 10-11). As a result of this phenomena, prepaid online payment systems such as PayPal, Stripe, Square, and Venmo have risen in popularity, allowing customers to make transfers and purchases using monies placed into their accounts (FATF, 2010b, p. 17). The opacity of funding sources and counterparties to the transaction is the risk associated with these goods (FATF, 2010b, pp. 22-23). While electronic records are generated automatically, there may be complications with the payment firm and the banking institution sharing information. There are other international money transfer services, such as Skrill, and business-to-business payment systems, such as Payoneer, that may be of interest to people wishing to launder money through international trade (McCrossan, 2015, pp. 4-5). As probable future trends for this type of payment, McCrossan (2015) mentions the ability to load digital money transfer services with cash deposits, convert cash payments to digital currency, and international payments with pooled funds (p. 6).

Cryptocurrencies: According to the DEA (Drug Enforcement Administration), the use of Bitcoin, the most widely used cryptocurrency, as a payment mechanism has risen as respectable businesses throughout the world have begun to accept it. It has been noticed in schemes where Chinese items are sent to Mexico and South America for TBML activities. Previously, payment was made via wire or bulk cash smuggling. However, there has been a trend to Bitcoin payment, which Chinese producers prefer because it allows them to bypass Chinese capital controls. Buying Bitcoin from a licensed MSB is less scrutinized than sending money from the United States to China. Bitcoin can also be purchased from unregulated brokers in other countries who combine its use for TBML with capital flight schemes (2017, p. 130).

Although it was claimed in 2017 that Bitcoin was used to support terrorist acts in Indonesia, Goldman, Maruyama, Rosenberg, et al. (2017) discovered that terrorist use of cryptocurrencies is mostly tied to online fund raising (pp. 10-12). Many terrorist groups have not adopted cryptocurrencies since transferring funds from cryptocurrency to cash is often difficult. Some terrorist organizations, on the other hand, have a large geographical footprint and multiple points of transfer between the initial source of cash and the eventual benefactor, making the use of cryptocurrencies more feasible (Goldman, Maruyama, Rosenberg, Saravalle, & Solomon-Strauss, 2017, p. 27).

Prepaid cards: Prepaid access cards, which can be open loop like prepaid credit cards or closed loop like retail gift cards, are an increasing method of money laundering, according to Simser (2013). They're not used to buy things on credit; instead, they're intended to store money that has been paid in advance (pp. 44-45). Bank Secrecy Act reporting requirements are waived for open loop cards with a value of $1,000 or less and closed loop cards with a value of $2,000 or less (FinCEN, 2011). Suspicious conduct involving prepaid cards is frequently linked to fraud or cross-border money transfers (Simser, 2013, p. 45). They can also be used for money laundering, according to Assistant US Attorney Courtney Linn (2008), who claims that closedloop gift cards pose the biggest concern. The risk comes from the purchase's secrecy, which can be funded by shady methods like cash and money orders, as well as the fact that anyone can use a gift card regardless of who bought it (p. 150).

Gift cards have been used to fund terrorism before, like in the case of a Washington transit police officer arrested in January 2017 for attempting to offer material support to ISIS through Google Play gift cards (Goldman, et al., 2017, p. 19). In December 2017, a couple was accused for laundering $70,000 over the course of three days by purchasing gift cards at several Walmart outlets in five states. To further sabotage the audit trail, they used the gift cards to buy more gift cards (WCVB, 2017). The transition to TBML activity is accomplished by purchasing stuff with gift cards, which is subsequently transported overseas or sold for profit and forwarded to a third party (Choo, 2008, p. 4). Gift cards can also be acquired and then transferred straight to another person, who can then convert them at a loss via a gift card resale service that deposits monies into a traditional bank or digital account (Friedman, 2017).

3.6TBML Real Cases

3.6.1 Vehicles used in a trade-based money laundering scheme

The earnings of drug trafficking and tax fraud were laundered through a network of companies set up by Italian nationals living in Spain, according to a joint investigation by Spanish and Italian police. There were ties between the scam and Mafia activity. After purchasing expensive vehicles in Germany using illegal funds, the OCG (Organized Crime Group) created value-added tax chains by registering and using legal organizations and creating a phony paper trail for sales and acquisitions. They then used the trading process to both conceal and create further illicit proceeds from their original unlawful activity. This aspect of the ML plan progressed to the point that the OCG was able to persuade a legal supplier in Italy to deliver huge numbers of automobiles on a yearly basis, so legitimizing their laundering activities. In addition to exploiting these high-end automobiles, the OCG employed import/export corporations under their control to purchase additional luxury things, such as watches, as well as lower-value items like shoes and textiles. The watches were bought in Spain and Switzerland before being sold to drug dealers in Morocco and the Netherlands, while the clothes was bought in Hong Kong and China before being shipped to Colombia and Morocco. Intervention operations in 2017 discovered assets worth EUR 8 million in numerous European countries, and follow-up action in 2018 discovered more assets, including 11 properties, 6 automobiles, 32 bank accounts, and shares in two companies, all of which were confiscated.

3.6.2 Lebanese Canadian Bank

The “U.S Department of the Treasury” recognized the “Lebanese Canadian Bank (LCB)” as a key ML concern in February 2011, noting that Hezbollah "received financial support" through these drug and ML activities including TBML, according to US government sources. "*Move[d] illegal drugs from South America to Europe and the Middle East via West Africa and launder[ed] hundreds of millions of dollars monthly through accounts held at LCB, as well as through trade-based money laundering involving consumer goods throughout the world, including through used car dealerships in the United States*," Treasury said.

In one operation, LCB authorized wire transfers to American banks in order to purchase cars (used) in the US. Used cars were allegedly acquired in the US and delivered to West Africa and abroad, with the money allegedly being repatriated to Lebanon via mass cash deposits at collaborating exchange companies. Asian-supplied consumer items were delivered to Latin America in another operation tied to the same Hezbollah-affiliated narcotics trafficking network, and through a BMPE-styled scam the proceeds were laundered. The cash allegedly went through LCB's U.S. correspondent accounts to pay for the consumer products.

In September 2011, the Banque du Liban, Lebanon's central bank and monetary authority, cancelled the license of LCB, and bank's assets and liabilities were ceded to the “Lebanese Societé Generale de Banque au Liban (SGBL)”. Financial sanctions and law enforcement investigations have been imposed on some of the persons and businesses linked to this illegal network in the United States.

3.6.3 Tobacco Products in illicit trade

Stormy Paul was the leader of a money laundering and illicit cigarette smuggling enterprise under investigation. This large-scale operation imported illicit cigarettes into the US and then used cash deposits to avoid paying millions of dollars in Washington State taxes. The cigarettes were imported into a Hawaii FTZ before being rerouted to Washington, rather than the intended destination of a Native American reservation in Idaho. Paul then laundered the earnings from the illegally obtained smokes in Washington. The investigation resulted 16 warrants were issued in Washington and Hawaii, resulting in the seizure of 1,451,697 million counterfeit cigarettes packs, one car, and more than $600,000. The state of Washington will lose $2,068,668 in income due to the confiscation of the smokes. Paul and his friends were subsequently charged with cigarette smuggling and trafficking, money laundering, and financial transaction structuring.

3.6.4 Illegal Fishing

In Cape Town, South Africa, Arnold Benjis is the "Managing Director and Chairman of Hout Bay Fishing Industries (PTY) Ltd. ("HBFI")". Arnold Benjis, his son, and their co-conspirators engaged in a complex conspiracy from 1987 through 2001 to unlawfully collect significant numbers of South and West Coast rock lobster and export them to the United States. Arnold Benjis and his associates lied to South African authorities on the amount of fish they harvested and bribed fisheries inspectors in South African to enable them carry out their unlawful harvesting scheme. They also submitted falsified export documents to South African officials to disguise their overharvesting. Arnold Benjis and his son were sentenced to 46 and 30 months in jail, respectively, in April 2004. Arnold Benjis and his son forfeited $5.9 million to the authorities as part of their penalties. In South Africa, Arnold Benjis was also prosecuted. His repayment to the South African government was originally set at $62 million, but it was eventually lowered to $22.5 million.

3.6.5 High-end electronics used in a trade-based money laundering scheme

The Australian Border Force (ABF) began investigating a TBML referral from an overseas partner in 2017 regarding the exploitation of small portable electronics trade.

ABF professionals were able to create a complete criminal network assessment of connected entities using a variety of analytical approaches, which were reinforced by financial and criminal intelligence. The ABF discovered that more than AUD 500 million [EUR 303.6 million] had flowed through Australian bank accounts since 2014 after piecing together a large network of ML facilitators.

The sale of pharmaceuticals in North America created revenue. The illegal proceeds were sent to bank accounts in Southeast Asia before being routed through a number of Australian bank accounts in Australian banking institutions. The money was sent to offshore accounts or used to buy small, high-end electronic items to sell to businesses in Southeast Asia and the Middle East. The illegal value being transferred offshore was magnified by the undervaluation of exported devices.

In this situation, the ABF was able to better identify and assess suspected cases of TBML by combining automated and manual trade data discrepancy analysis methodologies. Export declarations from nation A should match import declarations from country B. (because the consignment, in theory, is the same thing). When they didn't match in this case, ABF officials had reason to assume the disparities were a sign of trade mis-invoicing and, as a result, possible TBML. The OCG was linked to the transactions after more investigation and consultation with partner authorities.

3.6.6 Euskadi Ta Askatasuna (ETA).

The ETA is a terrorist organization based in Spain that was discovered laundering funds through a network of shell and front firms in the computer and electronic equipment industry in 2008. Individuals associated with the organization set up businesses in Spain and Costa Rica's Coyol Free Zone, which were subsequently utilized for illegal trading. Businesses in Spain sold goods, but the number of sales was insufficient to support the massive amount of cash deposits and wire transfers they received. The Costa Rican firms allegedly smuggled parts from Spanish firms for the assembly and selling of computers. However, the amount of money received and then returned to the senders over a six-month period was not proportional to the amount of sales activity that took place. The owner's daily bank usage and personal contacts with bank workers led to the explanation that the inbound money were for capital expansion and the outgoing transfers were for payment of imports, which was accepted by the bank's FTZ branch. Costa Rica established bank regulations requiring personnel at FTZ branches to be rotated every three months, as well as legislation criminalizing terrorist financing, as a result of this case (FATF, 2010a, p. 24).

CHAPTER FOUR

TBML Banks P&P

4.1 Banking Services and TBML

In international trade, banks' key responsibility is providing risk mitigation, financing and payment resolution for cross-border transactions. However; They are progressively being asked to assist in detecting and preventing financial crime. Banks understand their duty as citizens in safeguarding the financial system's integrity; nonetheless, there are fallacy about bank-intermediated commerce and the ability of the banks to detect illegal behavior.

To better comprehend the concept of TBML in the bank's context, it is necessary firstly distinguish between trades that are bank intermediated and those that are not. The seller and the buyer agree contracting conditions regardless whether financing is required or not. Financing, in some cases, may not be necessary. In some circumstances, the two parties offered financing (e.g., 30/60-day terms of sale), in which within a set period of time is made when the buyer pays the seller after the invoice is received. The only one bank's responsibility is to process the money and complete the transaction. Because this trade transaction was not bank-intermediated, the bank has little knowledge of or visibility into it, and hence has limited ability to detect illegal trade activity.

When commerce is facilitated by banks, these institutions may provide finance and/or risk mitigation products and services. Documentary (e.g., collections, letters of credit and guarantees) and non-documentary (e.g., receivables/payables financing, trade loans) financing are two common types of financing. Non-documentary, non-bank intermediated transactions are referred like open account commerce. According to Wolfsburg, nearly 80% of worldwide commerce was settled utilizing open account settlement in 2017.

Banks follow universally accepted norms for documentary trade, such as the “Uniform Customs and Practices (UCP) of the International Chamber of Commerce (ICC)”, and other similar rules for specific transaction types. "Banks deal with paperwork, not with goods, services, or performance to which the documents may relate, according to UCP 600 Article 5”. Because financing can be quite deal-specific, there are restrictions for certain, but not all, transaction types in bank-intermediated open account trade. Documentation requirements are outlined in policies of the lending institution and its deal structure.

For the roughly 20% of documented trade, a fraction of bank-intermediated trade non-documentary, and 0% of non-bank intermediated trade, banks obtain underlying paperwork. Both the quantity of opportunities to intercept unlawful flows and the practicality of recognizing "the bad needle" are limited.

4.2 TBML Risk Assessment

The definition and use of TBML is most typically employed in banking sector when assessing the risk of the overall business proposition of a client. While this is a part of a conventional "Know Your Customer" strategy, there are some additional elements of TBML. The first step is to figure out where the materials are coming from (currency, commodities, or services), and then to see if they're feasible for the business proposition in question. The bank can't tell if the items or money came from unlawful earnings, but it can tell if the proposal can be carried out with cash or products/goods illegally obtained, or if another type of business is functioning to supply illegal cash in the background.

In this sense, a more and more realistic description of TBML for the banking institutions may be "*The use of the financial services to facilitate the movement of money, through the use of fraud or deception*". This clearly defines banks' role in TBML activities, as their risk assessment systems as a result of the deception process will have been compromised. The term "money" should be reintroduced into banks definition because it is this aspect of the TBML transaction that will be reflected the risk assessment in the bank.

It is widely understood that the risk-based approach (RBA) is the key to the effective management of money laundering concerns in banks. According to FATF guidance (2014, p.6) "*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*". RBA definition lays the groundwork for banks to how they should build up their risk management processes, and because banking institutions have different business models, the risks associated with ML are likewise unique to each one. As per (FATF 2014, p.17), how "*banks allocate their compliance resources, organize their internal controls and internal structures, and implement policies and procedures to deter and detect ML/TF*" should be guided by identifying relevant risks and the establishment of appropriate controls. In terms of TBML risks, it's worth noting that specific banking categories, such as retail, corporate, and correspondent banking, have the highest concentration risks of TBML. Banking institutions are expected to apply RBA to the specific goods/products and services provided by them in building solid risk management for TBML risks, which should be taken into account in their entire risk assessment.

Risk assessment is an important aspect of money laundering hazards evaluation, and it is accomplished through the use of the RBA. In Finland, the "Act on Preventing Money Laundering and Terrorist Financing" requires obliged companies to include detection and assessment of money laundering risks in their risk management process. Because banking institutions are considered compelled enterprises, all banking sector operators are permitted to undertake risk assessments. As per Basel Committee on Banking Supervision 2017, p.4 "*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*". The previous categorization of red flag signs into five areas, in the context of TBML hazards, tries to encompass the relevant concerns associated to TBML.

The red flag signs are grouped into five categories especially related to TBML and based on the relevant risks, and banks should analyze how exposed their financial services offering is to these risks in addition to the red flags. Because open account payments are the primary conduits for illegal funds to be washed through TBML methods, TBML risks must be identified and assessed by all banks that provide payment services as part of their risk assessment. As per FATF, 2014, The huge volume of transactions, the cash-intensive implying of enterprises, and the big range of services offered by retail banking provide an obvious threat to potential TBML abuses, and risk assessments for such operations must be undertaken with caution. Moreover, transactional and credit services provisions in trade financing facilities exposes the corporate banking sector to significant TBML risks. TBML risks are larger not just in retail and corporate banking, but also in correspondent banking. According to "FATF, 2014", transactions of high value, limited amount of information in payment transactions, various jurisdictions that may not comply with AML standards, and supply of trade finance services are all examples of such services. According to the list of potential red flags, the majority of risk indicators are related to retail, correspondent banking or activity corporate, emphasizing the importance of evaluating money laundering threats identified through internal processes as well as external sources.

The end result of the risk assessment process is that banking institutions have a clear understanding of the money laundering dangers that they face, and they should be fully aware of their risk profile in order to take any necessary countermeasures. According to FATF report (2014), several sources of information 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*". Because money launderers are constantly changing their activities and banking institutions can be confronted with any money laundering threats, internal and external information must be constantly analyzed and controls established. Effective policies and procedures of risk management are based on banking institutions' complete understanding of relevant risks, which should then be used to develop precise controls for client due diligence, monitoring, as well as acceptance processes (Basel Committee). In addition to clearly comprehending TBML risks and implementing RBA, the customer due diligence process is an important aspect of sound risk management.

4.3 Policies and Procedures

According to the bank's risk assessment, a bank must design and implement clear customer P & P for identifying types of customers who pose a high risk of ML and FT. When assessing risk, a bank should consider a customer's history and background, usinf of products, occupation, source of funds, country residency, purpose and nature from opening the account, linked accounts, line of business, and other indicators in determining the level of risk and the necessary measures to apply.

All consumers should be expected to conduct basic due diligence, as well as proportional due diligence when the level of risk associated with the client fluctuates. If the statute allows it, simplified measures may be allowed in circumstances where the danger has been proven to be minimized. Basic account-opening procedures, for example, may be perfect for someone who intends to maintain a small account balance and use it for routine retail banking operations. It's vital that the client acceptance policy isn't so strict that it inhibits the general population, particularly those who are financially or socially disadvantaged, from using banking services. The FATF Financial Inclusion Guidance is useful for designing AML/CFT systems that are not excessively demanding for those who are financially and socially disadvantaged.

Where risks are higher, banking institutions should take extra efforts to mitigate and manage them. Individuals who aim to maintain a large account balance and make frequent cross-border wire transfers, as well as those who are politically exposed, may need to conduct more due diligence (PEP). Foreign PEPs, in particular, necessitate this level of scrutiny. Decisions to get into or pursue business relationships with higher-risk consumers should be subjected to more stringent due diligence procedures, such as senior management approval to enter into or continue such relationships. When a new business connection is approved or when an existing one is canceled, the bank's client acceptance policy should indicate.

The group AML/CFT officer's responsibilities include continuing monitoring of AML/CFT regulations at the group level, national, as well as international level. As a result, the group AML/CFT must be satisfied (including regular on site visits) that the AML/CFT standards are being followed across the board. If necessary, he or she should be able to issue orders or take action on behalf of the entire group.

Three Line of Defense:

The Chief Compliance Officer (CCO) and the CRO are the second line of defense for general compliance and AML/CFT controls, in addition to the senior officer that often have AML/CFT operational responsibility. It must be also mentioned that the CCO could also be on the top of AML/CFT officers at some banking institutions.

The front office is the first line for discovering customer-facing business units, assessing, and controlling risks within the business areas they are in charge in risk management. They must be aware of and follow the policies and procedures, as well as they must be given adequate resources in this regard.

Control functions are to ensure that rules and procedures are implemented are respected “for example, risk management, compliance, human resources, and legal” which are the second line. The risk management function assists and oversees business-line management in implementing effective risk management procedures, as well as reporting exceptions and the progress of first-line implementation.

The internal audit function is usually considered the third line of defense. The function of the internal audit is in charge of evaluating the efficacy of internal control design and implementation, as well as compliance with applicable laws and regulations. The internal audit evaluates the functioning of the second line of defense to ensure that are working properly both. Internal audit independently offers and issue a written assessment of control testing and related regulatory/legal compliance on a regular basis.

The “front office client facing business units” are still in charge of identifying, controlling, assessing and managing risks in their respective business sectors when it comes to AML/CFT risk management. (Due of the ever-changing AML/CFT expectations and regulations, it's typical that the second line to provide the first line the necessary technical support and to do the AML/CFT risk assessment). Today environment, the second line (AML/CFT), led by appointing an AML officer, to perform some duties of the first line function, as well as monitoring and screening. The unit must be aware of the policies, rules and procedures, and follow up them, as well as be given adequate resources form implementation. The third line (AML/CFT) has comparable roles and obligations as the institutional third line of defense, but it is in charge also of this risk-based and highly technical area are of the compliance.

4.4 Customer Due Diligence

The ability of a bank to prevent money laundering is heavily influenced by the “Know Your Customer and Customer Due Diligence” processes. Because of the acknowledged problems of TBML prevention, such as deal complexity, party relationships, and data availability, the most important and likely most influential element of any prevention attempt is proper due diligence and comprehensive deal underwriting of a trade-related financial instrument. When greater risk situations are identified, banks are expected to increase deal underwriting efforts to meet with new TBML regulatory standards.

Banks are expected to use a risk-based approach in the onboarding process and customer retention by following best exercises/practices for CDD reviews for trade account customers, and have a full understanding business model, counterparties, countries where the various entities operate from, goods or services that are exchanged, and the expected annual transaction volumes and money flows.

Where the countries, goods, or consumers involved are regarded to pose a higher risk, or where high-risk financial products are sold, “Enhanced Due Diligence (EDD)” is to be required, depending on the bank's procedures and projected risk. Also, once earlier reviews have revealed that the commodities sold are of high risk or have a dual use character, banks are obligated to perform a full EDD process.

In any scenario where transactions or other trigger events reveal new information about the nature of a relationship or the veracity of the data supplied, a loop-back mechanism, as in any suitable KYC/CDD procedure, is expected to initiate a re-evaluation process.

When a trigger event happens, the bank must do a comprehensive KYC/CDD re-evaluation of the customer to ensure that their Customer Risk Profile is correct and up to date. The outcomes of such a review process might range from merely confirming that the information on file is correct and that no changes are required, to a negative finding that leads to a change in the Customer (or linked party) Risk Profile and escalation to a higher level for further consideration. Following that, account/s may be subjected to controls, transaction prohibitions, or, in extreme cases, the relationship may be terminated.

4.5 Enhanced Due Diligence

Customers and trade finance transactions represent different levels of financial crime risk depending on their businesses, geographical areas, and risk profiles. Banks must have a thorough due diligence procedure in place to ensure higher-risk customers and transactions are subjected to more thorough due diligence and transaction monitoring.

Several parties are involved in a typical trade finance transaction. The parties involved include the buyer and seller, as well as their intermediaries, agents and lenders. In principle, banking institutions must treat an ordering party in a trade finance transaction as if they were a customer and take necessary due diligence measures based on risk.

The tests of due diligence that banks should perform are determined by the involvement of the banking institutions in the trade finance transaction. Because the bank's risk differs from transaction stage to another, there would be a commensurate difference in the type and scope of due diligence measures necessary. The ordering party of a bank is determined by the role of banking institutions in the transaction; for example, the L/C issuing bank's ordering party for “import documentary Letters of Credit (L/Cs)” is the L/C applicant; for export L/Cs, the L/C advising/confirming banking institutions instructing party is the L/C issuing bank or the first advising bank. In a trade finance transaction, banks should develop rules to designate the ordering party and the scope of due diligence processes to be performed.

For Trade Finance Transactions, more information must be obtained.

Banking institutions are expected to obtain additional information to assess the risk specific of the financial crime to a trade finance transaction, in addition to the requirements due diligence of customer outlined in the “MAS Notices” to banking institutions on Prevention of “Money Laundering and Countering the Financing of Terrorism (hereinafter referred to as "the Notice)”.

In taking into consideration the participation of the banking institution in the transaction, banking institutions must gather additional information on other important parties (listed in paragraph 2.10) to a trade financing transaction. Banking institutions should define clear protocols for all related parties, including “beneficiaries of L/Cs and documentary collections, agents, and third parties specified, regarding the additional information required under various scenarios”.

The additional data obtained, type and timing, are determined by the participation of banking institutions in the transaction and must follow a risk-based strategy. This also applies to situations in which banking institutions extend credit lines to its customers or supports open account trades “(e.g., invoice financing, pre-shipment financing, inventory financing)”. The following are some examples of supplementary information:

a) Customers' trading partners or counterparties (such as shippers, buyers, sellers, notifying parties, consignees, shipping agents, and so on);
b) The nature of the traded goods;
c) The country of origin of goods and products (including whether the commodities come from a country listed as sanction);
d) Trade cycle;
e) The vessel's flag, history, and name (to see if it's connected to any of the countries listed as sanction);
f) Any vessel planned to be utilized must have a name and a specific (unique) identification number (e.g., an “International Maritime Organisation (IMO) number) (e.g., to better identify if it is ultimately owned by a sanctioned party)”.

g) Trace the beneficial owner, commercial operator, and registered owner of the vessel involved in the transaction, with an emphasis on the country of residence of the former shipowners;

h) The proposed trade routes, including the port of loading, ports-of-call, and ports-of-discharge, as well as if the commodities are produced in or exported to sanctioned countries; and

i) When the contract price differs significantly from the market price, market prices of goods like commodities are evaluated to decide if more information is needed to lessen the risk of financial crime.

To authenticate the specifics of a trade financing transaction, banks should verify information collected from independent or public sources “e.g., against business documents, transport documents, and on a risk-sensitive basis”. This must also apply to situations in which banking institutions give credit lines to their customers' open account trades “e.g., invoice financing, pre-shipment financing, inventory financing” or otherwise aid them.

The following are some instances of trade finance transactions, as well as the supplementary information that banks should gather either during customer onboarding or during the transaction:

a) Import L/Cs (Outward):

- The L/C issuing banking institution must inquire about the nations with which the L/C applicant trades, as well as the trading routes used, the goods traded, and the types and nature of persons with which the applicant does business. If possible, the L/C issuing banking institution must also inquire about the role and location of other parties “such as shipping agencies, inspection companies, and warehouses that the applicant utilizes in the business”.

b) Export L/Cs (Inward):

- If the advising/confirming bank has an ongoing relationship with the L/C issuing bank, the bank may be able to rely on previously completed due diligence processes.
- If the advising/confirming bank does not have an ongoing relationship with the L/C issuing bank, it should ensure that any L/C received from the L/C issuing bank is authenticated and that the relevant persons are submitted to the bank's sanctions screening process.
- If the L/C is issued by an L/C issuing bank in a nation with a high risk of financial crime, or if the nature of the transaction has a high risk of financial crime, the advising/confirming bank should take extra precautions.

c) Bonds/Guarantees:

- Banks are reminded to follow the Notice requirements while dealing with the instructing party/applicant as a bank customer. The beneficiary should also be subjected to the bank's sanctions screening process.
- Banks should also have a rigorous risk assessment methodology in place to detect higher-risk transactions (for example, by identifying higher-risk contracting parties, jurisdictions, categories of goods, and other L/C terms). Additional verification methods and AML/sanction checks should be carried out for such higher-risk transactions (e.g. obtaining certified true copies of underlying commercial and transport documents).

For Trade Finance Transactions that provide a higher risk of financial crime, more information should be obtained:

If a bank becomes aware, at the outset or during the course of a trade financing transaction, that the transaction poses higher financial crime risks, the banking institution is required to gather additional information, to assess:

a) Structure of the transaction;
b) The ports of call, as well as the shipment's route, to verify that the transshipment sites and final destination look reasonable; the validity of the payment flows;
c) The verification of the authenticity of the bills of lading and confirmation that the cargo has happened using public sources of specialist data, documents, or information (e.g., the International Maritime Bureau); and
d) Whether or not they are dual-purpose goods.

In addition, the bank must conduct site visits and talks with the instructing party as necessary.

Invoice Financing

Banking institutions commonly provide invoice financing as part of their trade finance operations. For invoice financing schemes, banking institutions accept summaries of invoice data from selected clients instead of real invoices and shipping papers.

After providing consumers with invoice financing services, banking institutions must follow up with them to get commercial invoices and transportation documentation in order to verify the trades' authenticity. Such verification checks are usually carried out by a department separate from the front office. Banking institutions must have a system in place to do post-financing validation checks to ensure that invoice summaries reflect the facts in the actual trade papers.

Banking institutions that use sampling “sampling transactions, sampling approaches, repeat sampling, statistical sampling and result sampling” to perform validation tests should make sure their sample approach is sound. To target clients and transactions with greater risk profiles, an RBA to sampling approach should be employed, and the frequency of checks and quantity of samples picked should be proportional to the risks detected. Some lower-risk accounts should be included in the sample checks. Because mistakes in customer information, such as invoice value, names of boats, shipping companies/agents, and so on, would go undiscovered if there were no checks, financial institutions are at risk. The checks are particularly significant because the accuracy of such information is critical to the bank's AML/CFT sanctions screening. These checks prohibit customers from entering false or erroneous information in invoice summaries.

Dual-Use Goods

Goods, software, and technology that are commonly used for civilian purposes but might be utilized for military objectives or contribute to the proliferation of weapons of mass destruction are known as dual-use commodities. The interpretation of "dual-use" necessitates a level of technical understanding that not all L/C checkers possess. Furthermore, the items may be described in the documents using language that prevents such goods from being identified as "dual-use." If a bank lacks the necessary technical credentials and understanding across a wide variety of products and goods, it will be constrained in its capacity to grasp the different uses of dual-use items. Banking institutions, on the other hand, may use information from sources such as “Singapore Customs' Strategic Items Control List and the European Commission's TARIC” database to assess the possibility that particular goods are "dual-use" or in other meaning subject to movement restrictions.

It's critical that banks make sure their employees are informed of the dangers of dual-use goods and the most frequent sorts of dual-use goods, as well as how to spot red signs that suggest dual-use goods are being supplied for illegal purposes. To make sure that dual-use items in concept of trade financing transactions could be detected wherever possible, references to public sources of information and other guidance must be provided to staff, which must be formalized in the bank's P&P. As part of the bank's due diligence procedure, such transactions should be recognized and escalated.

4.6 Sanctions/Screening

Banking institutions all around the world have been following the requirement to screen consumers against a variety of lists for several years by implementing some form of name matching mechanism. The matching logic, technique, and quality of accessible data all play a role in a system's matching capabilities and accuracy.

Banking institutions utilize anti-money laundering software to detect suspicious behaviors by individuals or groups attempting to make income through unlawful means. Compliance experts use this software to adhere to legislation such as the “Bank Secrecy Act” and corporate policy addressing financial fraud. When analyzing prospective clients and suppliers, accountants and managers from various departments can profit from adopting this type of software. Banking institutions and financial organizations also utilize AML software to detect and tackle suspicious actions and fraudulent schemes to avoid any profitability and reputation harm that may be happened.

Banking institutions can deploy this type of software to avoid execute business with corruption with certain persons or groups that are suspected of stock market manipulation, financial fraud or terrorist financing.

AML software integrates data from a variety of financial transaction management systems, including as ERP systems and accounting software. Integration can also be advantageous with corporate performance management software for large firms with huge numbers of financial transactions.

A product must meet the following criteria to be considered for inclusion in the Anti-Money Laundering category:

- Use clever/smart algorithms to identify fraud and control risk;
- Compile watch lists of individuals and organizations to be on the lookout for;
- Enable users to award scores based on risk potential and previous behavior;
- Comply with AML regulations by delivering regular documentation and reports;
- Develop behavior models to identify persons or businesses that are suspect;

- Create dashboards with real-time data to track suspicious people or businesses.

There are many important and approved softwares to detect money laundering operations, the most important of which are, but not limited to are: WORLD CHECK, REFINITIV, SANCTION SCANNER, ORACLE, PLIANCE, RISK SCREEM and WORLD COMPLIACE DATA.

When screening customers and payments, banking institutions must be cautious since the matching logic must be created to screen the specific data. Screening names or payments through systems that were not designed for that purpose, such as screening payment transactions (i.e., MT103 or MT700 messages) for Sanctions or Dual Use Goods with a matching algorithm that was designed for name matching (i.e., culture-based matching), the results are likely to be insufficient, produce a high level of false positives, and, more importantly, fail to detect sanctioned entities.

Banking institutions are required to screen both direct customers (the processing bank's client) and ALL relevant entities, such as related parties (directors, signatories, guarantors, and so on), counterparties (such as suppliers, tax agents, lawyers, and so on), vessels, ports, and purchased products, among others. Payment transaction screening is also intended to be performed against customers, sanctioned nations, accounts entities, ports, and Dual Use Goods, among other things.

To ensure that transactions and operations do not breach UN or relevant international and local sanctions against identifiable individuals, legal entities, and governments, the capacity to filter multiple parties must be in place.

Banking institutions must keep documents to indicate that all relevant entities were examined and that any findings were made (or lack thereof). Banking institutions must thoroughly assess any potential matches discovered and keep track of the process for audit purposes.

A feedback mechanism is planned to be utilized to notify the KYC system and initiate a review procedure in the event of a positive match.

4.7 Correspondent Banking

The assessment of risks associated with correspondent banking relationships, particularly the cross-border character of banking transactions, is a crucial component of sound TBML management. The objective of a correspondent banking relationship is for a correspondent bank or body to provide financial services to the customers of a respondent bank or body, which may include payments by third-party, cash clearing services and trade financing, among other things “according to FATF, 2016”. In general, a correspondent bank does not communicate with a respondent bank’s customer, and the respondent institution is responsible for conducting CDD for the consumer initiating the transaction. The correspondent bank is required to execute due diligence for the respondent bank, and because correspondent banking partnerships provide higher-risk banking services and have limited information, they may pose a larger risk of money laundering “Basel Committee on Banking Supervision, 2017”. Before engaging into a relation with correspondent, the correspondent bank must conduct a risk assessment in money laundering for the respondent bank, by using RBA being particularly important when all risk variables are considered. *"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 respondent's part, or any potential deviations from the agreed terms of the arrangements governing the correspondent relationship,"* according to the FATF (2016). (p.4). As a result, it is clear that the correspondent bank must take a total approach to assess the risks that the respondent bank faces, and even though respondent institutions face varying levels of risk, there are several risk indicators that may be evaluated in all correspondent banks risk assessment process.

If a bank is considering delivering correspondent banking services, it must ensure that its risk assessment of a respondent institution includes risks associated with the respondent bank's services, its specific characteristics and the environment in which it works. The purpose from using correspondent services by the respondent, how these services are used “for example, if nested correspondence or third-party payments are permitted, or if payable-through account services are used by third parties are some of the risk indicators that should be evaluated in relation to the nature of services Basel Committee on Banking Supervision, 2017”. Nested correspondence refers to the responder bank's use of the correspondent relationship to provide transaction services to banks with no relationship and not deal with the correspondent bank, while “payable-through account PTA” refers to a third-direct party's use of the correspondent account (Basel Committee on Banking Supervision, 2017). Because the correspondent bank's primary job is to undertake due diligence on the responding institution, they are regarded possible risk indicators. The concern of money laundering may be realized, and the correspondent bank may be vulnerable to execute transfers operations for illicit money, if criminals find a weak channel due to the insufficient risk assessment of a respondent bank.

Other than services supplied to the respondent, the risk assessment must contain the specific characteristics and risks associated with the respondent's activities. “According to Basel Committee on Banking Supervision 2017, these potential risk indicators include the respondent's main business operations, the types of markets and customers served, the bank's management's assessment of potential money laundering risks, the respondent's anti-money laundering policies and procedures, and whether the bank has been in compliance with the law or has been confronted with any shortcomings in its anti-money laundering obligations”. Furthermore, the respondent's operational environment, which comprises either the respondent bank or its many affiliates, must be assessed as part of the complete risk assessment. These criteria include the respondent's, affiliates and any other subsidiaries locations, and how effective these governments' anti-money laundering laws and regulations are “Basel Committee on Banking Supervision, 2017”.

These risk indicators must not be viewed as a full list of risks; rather, to assess the amount of data necessary to create a correspondent banking relationship, the RBA must be used. A correspondent should identify the amount of risks as part of their understanding of the responder's business, assess the actions taken by the respondent to mitigate those risks, and then decide if the residual risk can be handled based on the eventual remaining risk (FATF, 2016). Risk assessment is an important component of establishing new correspondent banking ties, and once those partnerships are established, the attention should move to continuing monitoring.

In the same way that banks undertake due diligence on its customers, correspondent banks, in the form of respondent banks, are expected to execute due diligence and continuing surveillance on their clients. Constant monitoring is especially important for managing TBML risks because correspondent banking links are exposed for facilitating cross-border transfers, which are considered high-risk transactions. "Correspondent banks should establish appropriate policies, procedures, and systems to detect financial activity that is inconsistent 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, according to the directive (Basel Committee on Banking Supervision, 2017, p. 28)". In the same way that banks monitor their customers, the relationship with correspondent must also include transaction monitoring to discover normal transaction patterns that can be utilized to spot suspect conduct. All payments being transferred to the correspondent bank should include precise message information about the sender and the receiver as a requirement for respondent banks "in order to enable transaction monitoring from the correspondent side (Basel Committee on Banking Supervision, 2017)". Based on the respondent bank's CDD data, scenarios for predicted customer behavior should be constructed, and continuing monitoring should be focused on detecting any inconsistencies between predictable and current transaction patterns. According to FATF, 2016, "When continued monitoring discovers a potentially suspicious transaction, the correspondent bank must have procedures in place to authenticate the transaction's underlying purpose, which may include seeking additional information from the respondent". "In terms of the scope of CDD, it must be noted that correspondents are not required to undertake due diligence on the responder's client; instead, the focus should be on the respondent institution's risk assessment and updated due diligence material (FATF, 2016)". Identification of hazards, followed by risk management in the form of ongoing monitoring, are critical components of TBML control, and these components should be implemented into all financial organizations that provide correspondent banking services.

4.8 Sharing of Information

To share information, a system of collaboration between banking institutions, regulators, law enforcement agencies, and financial intelligence organizations is required, with secrecy being a secondary issue to detecting TBML conduct. (Bank of China (Hong Kong), 2017, p. 19) banking institutions should proactively communicate any difficulties to assist reduce the behavior by boosting transparency. Awareness training on TBML/FT, such as seminars, interagency meetings, internet-based learning, and pertinent information provided directly to contacts, could also be used to share information (FATF, 2008, p. 4). According to Levitt and Bauer (2017), financial intelligence sharing produced information that helped disrupt a 2006 attempt to blow up many planes in the United Kingdom by tracking big transactions from a charity to the potential bombers. It also helped lead to the arrest in 2017 of three al-Qaeda operatives who were preparing attacks in Germany (p. 145). After the incident, financial intelligence was used in the investigations of the 2013 Boston Marathon bombing and the 2015 Charlie Hebdo and Paris attacks (Levitt & Bauer, Can Bankers Fight Terrorism?). 145-146 in Bank On It, 2017).

Information exchange through nonprofit platforms like the “Egmont Group of Financial Intelligence Units” should be part of international cooperation, as should simplified judicial aid processes to make prosecution easier (He, 2010, p. 23). Hoffmann proposes that data sharing might be conducted through information sharing agreements, liaison officers, task groups, and specialist units such as “US Immigration and Customs Enforcement's Trade Transparency Unit (TTU)”. Any legal impediments to information exchange, she claims, may be overcome by a memorandum of understanding agreement on how the data will be used (2013, p. 332).

4.9 Ongoing Monitoring

Ongoing monitoring is an important section of ML/FT risk management that is both effective and sound. A bank is able only properly manage risks if it has a thorough awareness of its customers' ordinary and acceptable banking activity, which allows it to detect attempted and uncommon transactions that deviate from the ordinary model of banking activity. The bank is possible to fall short of its duty to discover and report suspicious transactions to the proper authorities if it lacks this information. All business contacts and transactions must be monitored on an continuing basis, but the scope of the monitoring must be determined by the risk indicated in the risk assessment of the bank and CDD initiatives. Customers or transactions with a higher risk should be monitored more closely. For the purpose to discover and prevent emerging risk trends, a bank must monitor cross-sectional product/service monitoring and not only its clients and their transactions.

Every bank must have mechanisms to detect anomalous or suspicious transactions and activity patterns. A bank must use the risk profile of the customer when establishing scenarios to detect such conduct as a result of the risk assessment of the bank, information obtained from law enforcement, information obtained from CDD activities and agencies. A bank, for example, may be aware of specific plans to launder crime proceeds detected as revolving within its jurisdiction by authorities. As part of its risk assessment process, it will have assessed the probability that activity related to such “schemes or arrangements is occurring within the bank through a category of clients, a group of accounts, a transaction pattern, or product usage”. The bank must build and implement suitable monitoring tools and controls based on this knowledge in order to detect such activity. These could be achieved, for example, by creating alert script for computerized systems for monitoring or establishing limits for a specific class or type of activity.

A bank must be able to discover transactions that do not appear in order to make economic sense, entail big cash deposits, or are inconsistent with the customer's usual and expected transactions using CDD information.

Customers in which the bank has classified them as high-risk, must been subjected to heightened due diligence policies and processes. In addition to established rules and processes pertaining to account opening approvals, a bank must have explicit policies on the extent and kind of required CDD, the frequency of continuous account monitoring, and the updating of CDD information and other records.

In order to identify, analyze, and effectively monitor customer accounts, a bank must ensure that it has “appropriate integrated management information systems in place, commensurate with its size, organizational structure, or complexity, based on materiality and risks, to provide timely information to both business units (e.g.

relationship managers) and risk and compliance officers (including investigative staff)". The systems in place and the information available must enable "cross-line monitoring of such customer relationships, including transaction history, missing account opening documentation, significant changes in the customer's behavior or business profile, and unusual transactions made through a customer account".

4.10 Suspicious Transaction Reporting and Asset Freezing

Banks will be able to spot suspicious activity, remove bogus positives, and report true suspicious transactions more quickly with ongoing monitoring and assessment of accounts and transactions. The process for "spotting, investigating, and reporting" suspicious transactions to the "FIU" must be clearly stated in the policies and procedures of the bank, and all type of employees must be trained on it on a regular basis. These rules and procedures must include a clear definition of the responsibilities of the employees, and instructions for analyzing, investigating, and reporting suspicious conduct in the bank, and directions on how to file reports.

There must also be procedures in place to identify whether the statutory duties of the bank under recognized suspicious activity reporting regimes require that the transaction be reported to the appropriate "law enforcement agency, FIU, and/or supervisory authorities", if applicable. These protocols must also represent the notion of secrecy, guarantee that investigations are completed quickly, and that reports are written and presented in a timely way. When money or other property suspected of being proceeds of crime remains in an account, the chief AML/CFT officer should ensure that disclosures are made quickly.

In addition to reporting suspicious conduct in regard to an account or relationship, a bank must ensure that necessary measure is done to appropriately limit bank's risk being exploited for illegal activities. This could include a customer's or account's review of the risk classification, as well as the entire relationship. Rapid increase to the suitable decision-maker level may be required to choose how to handle the relationship, taking into account any other relevant factors including coordination with law enforcement authorities or the FIU.

Terrorist financing is similar in different ways to money laundering, but it also has some differences that banks must be aware of “funds used to finance terrorist activities can come from either criminal or legal sources, and the nature of the funding sources can vary depending on the type of terrorist organization. Furthermore, it should be highlighted that transactions related to terrorist financing might be undertaken in extremely tiny sums”.

In accordance with appropriate national legislation and UNSCRs, a bank must be able to detect and execute money freezing decisions issued by the competent government, and it must stop or refrain dealing with any identified terrorist entities or individuals.

CDD must assist a bank in detecting and identifying prospect FT transactions, as well as giving key factors for a better understanding of customers and transactions. When designing customer policies and procedures, a bank must consider the unique risks of doing business with individuals or institutions associated to terrorist organizations. A bank must monitor new customers against lists of terrorists issued by competent (national and international) authorities before entering in a commercial relationship or conducting an incidental transaction with them. Similarly, continuous monitoring must ensure that current consumers are not added to these lists.

Every bank must detect have a system to detect and identify transactions with entities/persons listed on the sanctions lists. Transactions’ monitoring and screening are not classified as risk-sensitive due diligence measures and must be performed regardless of the customer's risk profile. A bank may use an automatically screening systems for sanctions' screening, but it must confirm that the systems are appropriate for the job. Screening systems and solutions must be subject to periodic testing (at least annually) to insure that no false negatives are generated and that the system is working properly.

This typically time-consuming regulatory requirement is beginning to be transformed by new technology. This is because law enforcement organizations all around the world are developing, authorizing, and encouraging new technology to make reporting easier, including Application Programming Interfaces (APIs).

In the US, the new AML Act includes provisions for FinCEN to "create streamlined, including automated processes" for non-complex categories of SARs, among other things.

Action 30 of the Government's Economic Crime Plan, which aims to improve SARs' IT, is driving progress in the UK. The new digital service for SAR reporting and analysis is expected to be ready by March 2022. Additionally, efforts are being made to improve the quality of SARs submitted. For example, sector-specific templates are an endeavor to assist users in submitting reports and indicate any problems or omissions as they occur. This is critical since a large majority of SARs are of poor quality and include little or no meaningful information.

In Hong Kong, police are beefing up computational power to help their new anti-money laundering unit deal with an increase in STRs of about 11% last year. Officers will no longer have to manually analyze STRs thanks to the computer system overhaul, which will leverage big data technologies to assist with STR processing and save them time.

The National Crime Agency’s (NCA) new IT is attempting to better handle the volume of SARs submitted in the United Kingdom. The new technologies are expected to extract the value of SARs by detecting signs of susceptibility, trends, and networks. Furthermore, the new system should provide law enforcement with a more user-friendly site, with improved access and search capabilities.

In STR processing, there is a lot of room for digital automation. This would free up human regulators to focus on high-priority investigations by allowing automated software systems to handle all of the low-value, repetitive job of checking STRs.

Where legal, new technology and APIs are allowing more data to move between diverse business areas in financial organizations.

Compliance teams have a better knowledge of a customer's risk profile now that they have more data, allowing them to make better decisions about whether or not to pursue an investigation.

Rather than being regarded as business as usual, this strategy indicates appropriate action to all stakeholders. Industry requires - and is beginning to witness - a shift toward continual customer risk assessment.

Following applicable rules and regulations, a bank shall take the actions to freeze the cash or other assets of designated persons and businesses without any delay and without prior warning.

4.11 Record-Keeping

The information collected from CDD conduct must be kept and recorded by a bank. This comprises: “(i) recording the documents submitted to the bank for verifying the identification of the client or beneficial owner, and (ii) transcription of the appropriate CDD information included in such documents or gained through other means into the bank's own IT systems”.

A bank must also design and enforce specific guidelines about the records preserved to filing customer due diligence and transactions. If possible, all mandated privacy safeguards should be taken into consideration in these guidelines. They must include an explanation regarding the sort of information that must be kept as records and the time of this record, which should be at least five years after the banking relationship or the end of the transactions resulted from this relationship. Even in case of accounts closed, all records should be kept until the case is closed if there is an ongoing inquiry or litigation. A bank's ability to “adequately monitor its relationship with its customer, understand the customer's ongoing business and activities, and, if necessary, provide an audit trail in the event of disputes, legal action, or inquiries or investigations that could lead to regulatory action or criminal prosecution depends on keeping complete and up-to-date records”.

Maintaining sufficient records detailing the evaluation process connected to continuing monitoring, as well as any conclusions reached, would aid in demonstrating the bank's CDD compliance and ability to manage the risk of ML and FT.

4.12 Data Mining of Collected Transaction Data

Every day, banking institutions get massive amounts of data from processed transactions. Data, on the other hand, is only useful if it can be used to extract information. The banking institution can use the acquired data to determine what to do if an unwelcome past behaviour occurs again in the future (Subramanian, 2014, p. 46).

Financial intelligence units (FIUs) must also assess financial data received from banking institutions for patterns that could indicate TBML activity, such as SAR filings and counterparty identification (FATF, 2008, p. 3; Hoffmann, 2013, p. 331). If at all practicable, data mining should include a review of SAR files that have resulted in the discovery of money laundering operations (Levy & Reuter, 2006, p. 342). This approach to knowledge discovery in databases enables the detection of bigger patterns of irregular or anomalous transactions, which may then be utilized to improve existing algorithms for detecting potentially suspicious activities (Gao & Ye, 2007).

According to Subramanian (2014), recording data at the granular level enables for improved analysis and modeling (p. 49). This includes text data, which is crucial for the construction of networks via link formation (Gao & Ye, 2007, p. 175). AML investigators can use network link analysis to find relationships between consumers and third parties, as well as the frequency and intensity of activity (Gao & Ye, 2007, p. 176). This is frequently done by hand. However, there are technologies available to help automate the process. Knowing the important participants, according to Gao and Ye (2007), enables for network disruption because the hubs may be located and disconnected (p. 177). They can also be barred from doing business with the banking institution's clients in the future.

4.13 Escalate possible TMBL activity to law enforcement officials

The filing of a SAR is the most common way of bringing suspicious activities to the notice of law authorities (Levy & Reuter, 2006, p. 340). When suspicious transactions are discovered, they should be reported to law enforcement officials to alert them to probable illegal behavior that needs to be investigated further and to the presence of court-acceptable evidence (Levy & Reuter, 2006, pp. 292-293).

This is a crucial aspect of the AML compliance system; yet, law enforcement authorities only have so much time to follow up on SAR filings (Simser, 2013, p. 43). Direct interaction with law enforcement can increase efficiency and help law enforcement sift through the massive number of SARs filed (Levy & Reuter, 2006, p. 349). Furthermore, Levy and Reuter (2006) argue that the quality of SAR filings must be improved in order for law enforcement to focus on the most heinous activities (p. 342). The SAR filing procedure can often be automated to improve quality and reduce the time it takes to prepare the SAR, lowering AML investigators' reluctance to file (NICE, 2018).

The rise of terrorism-related SARs between September 2001 and June 2004 demonstrates the importance of quality escalations of suspicious behavior. According to Levy and Reuter, most of the SARs filed for terrorism immediately after 9/11 were due to watch list matches. Most SARS were filed proactively from October 2002 onwards as a result of banking institution due diligence processes. Furthermore, between April 2003 and June 2004, banks reported 23.4 percent of SARs filed for terrorism to law enforcement as requiring immediate attention (2006, p. 341).

CHAPTER FIVE

TBML Vulnerabilities

5.1 Overview

Terrorist financing has been linked to TBML, which is one of the most common ways of money laundering used by criminal organizations. Indeed, banking institutions have the ability to evaluate both sides of a trade transaction for red flags and report suspicious activity as needed as a facilitator for the exchange of funds between trade counterparties. Banking institutions, on the other hand, appear to be less capable of detecting this type of money laundering in comparing when detecting other types of money laundering. The majority of SARs submitted in 2017 were for conduct that is frequently a red flag indicator for TBML, with only 1,120 SARs designated as likely TBML, bolstering the argument that banking institutions are not categorizing the activity accurately (FinCEN, 2018b). As a result, while the behavior is identified as suspicious, it is not logged as part of the bigger TBML problem.

To identify the probability of suspicious behaviour, banking institution compliance procedures rely on the systemic creation of warnings and the receipt of non-systemic signals. Investigative team carefully reviews the warnings and determines whether they are a false-positive clear or a true positive for AML issues. This is a very subjective process that strongly relies on the knowledge base of the person processing the alert. The widely accepted FATF (2008) definition of TBML/FT focuses on the transfer of value through trade transactions, while commercial TBML tactics are described as the means of achieving such value transfer. Many of the indications that characterize commercial TMBL occur outside of the linked financial transaction and are difficult for investigators to gather or analyze without specific trade finance skills. The low number of TBML SAR filings is clearly due to an overreliance on this narrowly limited categorization of red flag activities. Nonetheless, depository institutions can take steps to strengthen their current TBML reporting practices.

The complexity of trade-based money laundering schemes varies, but they always rely on the transfer of value. As a result, red flag indications other than those used for commercial TBML can be used to detect the behavior. The fact that TBML activity varies greatly aids investigators' capacity to better spot it and report it accurately through improved training. To effectively combat TBML, banking institutions must concentrate on what can be seen within completed transactions and ensure that their AML/CTF compliance program supports the proper identification, escalation, and obstruction of illicit value transfer activities.

5.2 TBML/FT Activity Varies Widely

Most discussions of red flag indications focus on those seen in commercial TBML schemes, and TBML is generally characterized only in using of trade transactions to transfer value. Soudijn (2014) found from his study of the literature that this definition is too narrowly focused and fails to account for many cases that can be categorized as TBML but do not display the predicted activity (pp. 230-233). In fact, investigations show that criminal organizations and terrorist financiers are using TBML/FT in different ways, from simple systems to complex schemes. Location, product kind, access to technology, and any predicate offense can all influence the techniques used. They are frequently used in combination, which adds to the complexity. As a result of the methodology's intricacy, distinguishing between genuine commerce and TBML-related trade is intrinsically difficult, increasing the danger of criminal behavior being misdiagnosed as legitimate transactions and legitimate trade being reported suspiciously.

Although the TBML methodologies examined differ, each shows a pattern that can be leveraged to improve the acceptable list of red flag indicators. Wire or check activity is common in trade transactions, and it can include additional information about the transaction. Through invoice manipulation or multiple invoices, the inclusion of invoice numbers, the sort of items involved, and price information can show suspected commercial TBML activity. The trade counterparty may also distribute the transaction across many bank accounts at different banking institutions. To balance the accounts, modernized IVTS transactions are settled via wire transfer or monetary instrument deposits to an established firm maintained by the IVTS owner. Finally, the movement of funds through BMPE is more complicated, and it frequently involves structured cash activity, third-party monetary instrument deposits, wire transfers, and the participation of high-value low-volume commodities like electronics.

Value is also transferred through less traditional payment methods such as digital money transfer services, prepaid cards, crypto-currencies, and virtual currencies. These products are popular in part because they provide consumers with anonymity and convenience of use. Furthermore, compared to other aspects of the financial industry, crypto-currency and virtual currencies are subject to less regulatory scrutiny. Even the ultimate destination of payments might be obscured using prepaid access cards. However, there are red flag indicators of TBML activity that may be utilized to identify whether or not transaction activity is legal. Frequently, the amount of money moved or the pattern of movement differs from that of other users of these payment methods.

By abusing current mechanisms intended to offer asset protection and enable trade, criminal groups and terrorist financiers conceal their identities and the scope of their activity. With red flag indicators that are outside of the financial element of the transaction, this activity enables for anonymous ownership and minimal control for shipments. Corporations with hidden beneficial ownership, as well as entities registered in offshore jurisdictions or privacy haven countries, are red flags in terms of ownership. Geographical locations are also a concern, as globalization has resulted in criminal and terrorist groups cooperating in TBML activities all over the world. Shipments through FTZ zones, which lack monitoring and transparency, are prevalent, and they provide a chance to conceal the true origin of a shipment or smuggle in more illicit goods. These places have been linked to trade that is used to launder criminal money, fund terrorists, and assist the proliferation of weapons of mass destruction.

5.3 Identification Must Be Multifaceted

As part of the AML/CTF procedures designed to combat the movement of illegal funds, regulators require banking institutions to have a compliance program in place. Typically, these programs comprise a method for producing warnings for strange transactional patterns, investigative staff to analyze the alerts, and a mechanism for reporting suspected conduct to law authorities. The complexity of TBML activity, as well as the reliance on red flag signs that necessitate access to data not held by the bank, leaves the detection of probable TBML-related activity to the investigative team. A right determination is then based on the investigator's training, expertise, and ability to connect the red flags to the typology. This strategy leads to inconsistency throughout the organization and increases the chance that people with less experience would mistake the activity for routine business.

5.3.1 Technology:

Financial organizations are required to gather a variety of information about their customers and the transactions they handle. This information must be held for a certain period of time from five to ten years, while some may be kept for even longer. The high volume and number of data available to huge financial organizations, as well as the quantity of information it can provide when arranged into a meaningful fashion, is vast. To optimize coverage strategy and detect likely patterns of TBML activity, technology should be used to evaluate both financial and consumer data.

5.3.1.1 Coverage strategy:

To detect potentially suspicious activity among the vast volume of transactions completed each day, banking institutions use a combination of measures. Manual referrals, such as teller referrals for behavior observed in the branch, as well as law enforcement referrals resulting from subpoenas and demands for information, are examples. They also involve the use of monitoring software to generate automated alerts, which provides the possibility to proactively discover behaviour that displays red flags indicative of TBML.

Many banking institutions utilize activity monitoring software that automates warning creation using a rule-based approach rather than a risk-based one, according to the study. Rule-based techniques are unable to adapt to rapid change and train behavioral models insufficiently, resulting in a higher number of false positive alerts and a failure to uncover logical behavioral relationships. A scenario for structured cash activity, for example, could result in false positive alerts if a customer conducts cash activity over the weekend totaling more than $10,000 or makes many withdrawals on the same day but files a CTR at the branch. Additional features should be added to check the real dates of transactions and for customer-filed CTRs to reduce false positives. Risk-based techniques can combine features to reduce false positives, eliminate rule overlap and conflicts, and enable predictive alerting scenarios that create warnings based on a mix of risk behaviors.

While the many employed strategies may differ, each contains red flag indicators to separate it from legitimate trade activity, according to the examination of the TBML methodology. According to Soudijn (2014), lawful trade involving illicit funds is frequently conducted in cash, which could indicate red flag indicators such as multiple small cash payments, a change in payment pattern type, and even business activity with counterparties in unrelated industries (pp. 239-240). Advanced algorithms that seek for red flag signs specific to each typology may be able to generate typology-specific alerts using a combination of risk behaviors. This method could allow numerous rules to warn on the same activity, resulting in a single typology-specific alert. This type of warning mechanism can be used not only for TBML, but also for any other complex money laundering scheme.

5.3.1.2 Data mining:

Banking institutions collect data that may be used to figure out not just what happened in the past, but also what should happen in the future. The acquisition of granular data and subsequent mining of that data can yield information on TBML activity patterns that can be utilized to improve existing algorithms. It can also make the manual aspect of the investigation more efficient, particularly when text data is collected and transformed to a more useful format. A study of SAR filings and counterparties related to probable TBML activity should be part of the data mining process. Data mining can assist provide better alerts and enable a faster response to the detection of TBML-related activities.

For the assessment of larger instances or in situations where cases appear to include related activity, network link analysis employing both text and numerical data is extremely useful. It may be used to discover trade counterparty relationships, the frequency and intensity of activity, and the identities of significant actors. Investigators can use data analysis to see the relationships between transaction counterparties and alter the data in ways that aren't possible with a traditional spreadsheet. The flow of cash involving a number of high-risk countries and offshore banking jurisdictions must be identified promptly. Trading with companies that supply unrelated commodities, bidirectional fund flow, and a plurality of overall activity occurring with only two counterparties are all red flag indicators for TBML activities.

5.3.2 Training:

The subject of TBML will be integrated into Banks' AML and CFT (hereafter referred to as "AML/CFT") training based on staff job specifications. The training program's content must refer to and include frequently-occurring transaction typologies and suspicious transaction cases that are likely to occur, in order to fit each bank's level of risk and to improve staff's ability to identify TBML (such as trade-related operations staffs, AML/CFT staffs, and internal audit staffs). Furthermore, banking institutions must provide organized training to relevant employees to keep them up to date on current laws and regulations, business demands, and TBML development trends, allowing them to be fully aware of the risks involved.

Because so much of TBML activity detection is based on AML compliance staff's subjective ability to spot the signals, effective training is essential. According to the Bank of China (2017), all employees should be trained to recognize red flag activities, particularly when it comes to required trade paperwork (pp. 15-16). The FATF (2008) advises that banks supervisors undergo further training in assessing the adequacy of trade finance controls and monitoring systems, sample testing trade finance accounts, and delivering anti-money laundering (AML) training to trade services personnel (p. 4).

TBML/FT training should be integrated into existing AML/CTF training programs, according to the FATF (2008). (p. 2). Integration with current systems, according to Hoffmann (2013), is not a powerful enough solution and simply elicits a bare minimum response. Because TBML offers different hazards than other types of money laundering, she believes that training programs for it should be focused and conducted separately from conventional AML training (p. 331). Regardless, rather than general material, training programs should focus on the significance of existing data and analysis tools (FATF, 2008, p. 3).

“Artificial intelligence (AI), machine learning (ML), and the Internet of Things (IoT)” made it easy to build algorithms that automatically acquire public information on people for the sole goal of spear phishing them, or even counterfeit their voices to imitate them — all at scale. The fact that the entire scenario may be automated and highly based at the same time, much like a smart missile, is possibly the most worrying aspect of this ML-assisted type of social engineering.

From the perspective of social engineers, ML sample may be used to practice AI and its algorithms to target specific types of files to focus on their metadata. Attackers can train their models with type-specific ML classifiers. The tools will be tuned to execute several engineering operations and even learn to develop them as a result of this. “K-means, random forests, and neural networks” are just a few of the grouping and classification techniques that may be used in conjunction with “NLP analysis” on a victim’s social media posts, for example.

As one of the earliest channels for thieves to utilize this technology for evil purposes, ML is well acquainted with email spam. Instead of manually writing spam texts, the bad guys might save a much time and effort by letting a nervous network handle the hard lifting in terms of well-crafted trash emails.

AI and machine learning can understand the whole context and mimic natural writing styles. Through information available on social networks and elsewhere, algorithms can examine how a person records, speeches, his habits, contacts, and so forth. Attackers can utilize ML through image recognition technologies, for example, if they have an image of the victim or at least know how he or she looks, to discover social media accounts associated with him or her. Trustwave, for example, has a technology called “Social Mapped” that can handle all of this.

Types of social engineering

Vishing. Probably the scariest aspect of AI is that it may learn to imitate very good personal qualities of humans you may know by constantly improving its machine learning capabilities. For instance, machine learning can train an algorithm to rise vishing assaults by evaluating a voice's pattern over time and then replicating it in a persuasive manner.

This form of social engineering has already yielded results: hackers stole $243,000 by impersonating a UK business owner using AI-driven voice technologies.

Twitter. Bots can apparently learn to automatically establish credible interactions with software-generated people that appear entirely natural, or will soon be able to do so. A 'honey trap' is a type of social engineering in which an attacker creates the appearance of an attractive person in order to establish an online romantic relationship with a victim in order to coerce him into sharing information classified as sensitive. The

“Ashley Madison” data breach is a case study worth mentioning in this area, because this dating site deployed bots that pretended to be genuine people, mostly females, to attract customers and finally persuade them to pay subscription fees and other costs.

Scareware. In order to persuade the targeted user to acquire malware protection software, ML can determine what kind of cybersecurity dangers are relevant to him. This is a type of cybercrime that takes advantage of the victim's astonishment, anxiety, and fear of being attacked. Cybercriminals are taking advantage of every facet of the COVID-19 problem, for example, because many individuals are afraid at this time. In their press report on cybercrime in the first half of 2020, the FBI noted the massive increase in cyberattacks – roughly the same number of complaints up to May 28, 2020 compared to the entire year of 2019.

While using technology to improve warnings and aid in the investigation process is beneficial, the literature review also stressed the importance of ensuring that compliance professionals are adequately trained to spot TBML behavior. Because of the complexity of TBML, it can be difficult to spot red flag indicators if investigators are unfamiliar with them. Because TBML activity is frequently mixed in with legitimate business operations, investigators must learn to distinguish between the two. Furthermore, employees of banking institutions who do customer KYC must be trained to determine when information provided by the consumer is incorrect.

5.3.2.1 Formal Training Program:

The FATF (2008) recommends that TBML/FT training be integrated into a banking institution's existing AML/CTR training program. Hoffman (2013), on the other hand, believes that because TBML is a complicated typology, it should have its own training program separate from regular AML/CTR training. TBML training programs, whether integrated into existing programs or done separately, should be tailored to available data and analysis methodologies rather than a generic description.

5.3.2.2 Develop research skills:

It is not enough for AML investigators to be conversant with the TBML/FT approach; they must also learn how to do research in order to distinguish between legitimate and unlawful transactions. External research for customers, counterparties, and transactions is frequently required. As needed, investigators should request paperwork for suspicious trade transactions, and the findings should be kept on file for future reference. Third-party databases that track past shipping data can potentially be used to do additional research. "The significance of open-source information... is underestimated," according to Passas (2016), and while the data may be stored in different locations, it does exist (Trading with the Enemy, p. 12).

Due diligence should be done for all parties to transactions with indicators of probable TBML activity, including noncustomers, according to several sources. The collection of pertinent information about all counterparties to an alerting transaction is considered noncustomer due diligence. This involves looking for beneficial owners, duplicate addresses, negative information, and the location of incorporation in public records. In addition, data mining may be used to look for duplicate invoice numbers and payments to see if there are any indicators of numerous payments, and the noncustomer's relationship to other customers can be determined. Internal customer due diligence data may be available for examination if the noncustomer's bank joins in the KYC Registry (Swift, 2017).

5.3.2.3 Learn to identify problem customers:

Customers are reviewed during onboarding and as needed during the customer relationship. All legal entity customers must have their beneficial owners identified, and this information must be updated if there is a major or inexplicable change in activity (FinCEN, 2016a). Banking institutions should also figure out who a company's planned trade partners are and whether it's a front or shell company. Customers who display red flags indicating that they are seeking to conceal the genuine owner or activity type should be subjected to greater scrutiny. More emphasis should be placed on conduct than on demographics, as behavior is a better predictor of risk (Gao & Ye, 2007).

Delston and Walls (2009) believe that regulating foreign supply chain traders would reduce the risk of banking these businesses. Hoffmann (2013), on the other hand, noted that while risk would be decreased, trade might be hampered. Customer due diligence measures that are overly tight, according to De Koker (2006), might lead to financial exclusion and a rise in unregulated financial operations. Finally, Soudijn (2014) warns his audience not to be misled by due diligence activities into believing that every trade activity is TBML-related (p. 231).

5.3.3 Information Sharing:

Compliance inspectors at banking institutions just look to see if the transactions they're looking at are indicative of illegal conduct. When probable TBML activity is discovered, it must be reported to law enforcement for further investigation and notification of evidence. Because law enforcement organizations have limited resources to comb through all of the SARs filed, they will concentrate on those that contain key terms that match their area of emphasis. Furthermore, direct contact with a designated individual at the banking institution allows law enforcement officials to concentrate on SARs that require immediate action.

It is also necessary to share information through collaboration across the numerous companies and organizations that execute financial transactions and fight financial crime on a much wider scale. Transparency and information exchange can take place on both a national and international level, and can be accomplished through direct interaction or awareness training. Hoffmann (2013) advises establishing formal partnerships between data sharing parties, including a memorandum of understanding agreement addressing the usage of shared data, to alleviate any legal impediments (p. 332).

5.4 Limitations of Research

Because trade-based money laundering is a complicated and dynamic process, there is a scarcity of peer-reviewed research on the most recent tactics discovered._Red flag indications for these strategies could not be generated without further information about casino transactions, real estate purchases, and bogus Amazon sales. Furthermore, peer-reviewed publications on TBML activity detection tended to focus on entities other than banking institutions, law enforcement and trade agencies. This necessitated sifting through the research for data that applied to several industries or could be extrapolated to apply to banking institutions. Finally, because the banking industry is heavily regulated for AML/CTF compliance, there was very little dissenting material available, and the opposing viewpoints identified focused on the repercussions of individual activities rather than the general problem addressed by this capstone work.

CHAPTER SIX

Recommendations

6.1 TBML’s position

TBML is one of the most common and misunderstood methods of money laundering. Because of its complexity and ever-changing nature, it's tough to spot it in financial transactions. Criminal groups and terrorist financiers are also resourceful. As a result, certain TBML procedures are so new that there is little information available. Banking institutions must implement AML/CTF compliance programs to detect and report suspicious activity for further investigation by law enforcement, according to banking rules. The system, on the other hand, functions best when the activity is correctly detected and escalated to the appropriate type. Every year, hundreds of thousands of SARS cases are filed, with just a small percentage of those for TBML and TF. The majority of SARs, on the other hand, are for red flag indicators that could be related to TBML. This shows that banking institutions can improve the detection and escalation of TBML/FT activities by implementing or improving protocols.

Banking institutions that have not yet implemented these practices, as well as those looking to improve an existing AML compliance program, should consider the following advice. Implementing typology-specific training that includes guidance on added analytical practices to assist investigators in identifying TBML activity, leveraging collected data to improve the identification and investigation processes, and learning to share information with other banks and law enforcement as applicable within the current regulatory and legal framework are all recommendations to better protect banking institutions against their use to facilitate TBML/FT activity. The execution of these recommendations will result in a more effective and efficient detection and escalation of TBML/FT activity, as well as the implementation of actions to fight the use of the banking system for this type of financial crime.

6.2 Implement TBML Specific Training

Knowledge is required to successfully identify TBML activities. While some aspects of the AML/CTF compliance procedure can be automated, investigative employees make the final determination on whether or not the behavior is suspicious. As a result, banking institutions should strongly consider providing TBML training to their workers. This includes not only training in the typology, but also assistance with investigative skills and access to the resources needed to locate the information. Additionally, staff who do KYC tasks should receive training to assist them in identifying consumers who may be at high risk for TBML.

Banking institutions should establish a customized training program that addresses the TBML methodology's particular threats. The training must be in a format that can readily be updated with new knowledge, accommodate queries, and be made available to investigators as needed. It is suggested that computer-based training be used as the primary type of instruction, with classroom training serving as a complement to allow for investigator questions and experience exchange. The TBML typology and its many methodologies should be covered in the training program, as well as specific difficulties to be aware of, such as beneficial ownership and high-risk location information. It should also include red flag signs that are particular to client and transaction activity from the perspective of the banking institution. A provision for the regular transmission of information on evolving TBML techniques, regulatory guidelines, and case studies should be included in the program.

Customers and counterparties should also be given the tools and training they need to do effective customer and counterparty research. This includes read-only access to any internal systems with relevant data as well as the necessary training to use them.

Investigators must develop an internal inquiry mechanism that allows them to collect information from customers concerning trade activities, including the ability to request copies of papers and, if required, banker site visits. External resources, such as websites that provide particular shipping information for international commerce transactions, should also be made available to investigators. Banking institutions should also provide instructions on how to do further opensource searches that can be relevant when researching TBML activities. These include verifying beneficial ownership, the legitimacy of a company website, the predicted revenue of a certain business type, and signals that the company is not operating normally.

Staff collecting KYC data should be taught to ascertain the true nature of the firm, its beneficial owners, and areas of activity in order to gain a realistic evaluation of the risk associated with business banking customers. Staff must also be taught to spot red signals that suggest that the expected activity is out of the ordinary. Any signers, as well as credit card-only consumers, should be thoroughly investigated. The consumer should not be allowed to open an account if red flag indicators or a reluctance to share information are identified during the onboarding process. If additional red flags are discovered during the ongoing assessment process, the banking institution should think about terminating the connection.

6.3 Leverage the Data

Banking institutions' vast amounts of data on consumers and their financial transactions are a valuable asset in the fight against TBML/FT. It is the major source of transactional alerts, and investigators utilize it to determine whether the warnings are related to actual suspicious conduct. However, the knowledge gathered from this data can also be used to improve the detection and investigation of TBML activity. As a result, banking institutions should mine their stored data for information that may be utilized to better the investigative process, optimize alert production, and find existing patterns of questionable behaviour.

The identification of preset alerting scenarios within transactional activity is used to generate alerts. Banking institutions should perform a periodic evaluation of recent TBML SAR filings for red flag signs that may need to be integrated into alert generation algorithms to ensure alerting situations are kept current. Large round dollar wires and activity involving places that have been classified as high-risk for TBML activity should be mined from data caches for patterns of activity that appear to be typology related. To find plausible rings of TBML activity linked to customers and counterparties identified in TBML SAR filings, network link analysis software should be employed. For large cases, link analysis can also be employed during the investigation phase to improve efficiency. It can help determine the authenticity of transactions based on volume and trading direction, detect related cases, and identify counterparties who have been sanctioned for similar behavior. Finally, data mining software like Optical Character Recognition software should be employed to improve efficiency by automating the manual inspection of checks and other monetary instruments.

6.4 Learn to Appropriately Share

This capstone project's third proposal is that banking institutions communicate TBML-related information with other institutions, law enforcement, and training groups as needed. Banking institutions should use the PATRIOT Act 314(b) program to not only request transaction information, but also to initiate a conversation with the other institution about the activities they have noticed. When this communication has an impact on the filing decision, it should be included in the SAR narrative. To guarantee that reported behavior is useful to law enforcement, banking institutions must describe the activity observed and why it is suspicious in order for the SAR to reach the proper agency. This involves choosing the necessary checkboxes and FinCEN advisory phrases on the SAR form, as well as using the terms TBML and BMPE in the SAR narrative as needed. In addition, anytime the information discovered appears to be time-sensitive or exceptionally egregious, the BSA compliance officer should contact criminal enforcement. Finally, banking institutions should actively participate in awareness training, both as attendees and presenters, in order to benefit from the overall money laundering knowledge that each firm acquires via daily business activity.

6.5 Topics for Further Research

Money laundering through trade is a vast and ever-changing topic. As a result, there are various avenues for future investigation. More data on the rapidly emerging techniques of the TBML methodology, for which few resources were located during this assessment, will become available as time goes on. More study is needed to ensure that alerting mechanisms and TBML training can be updated to include new red flag indicators. Additional research on coverage strategy could be conducted to discover best practice approaches for detecting TBML activity at the alert generating level. While the recommendations involve a more focused strategy to alert production, the specifics are beyond the scope of this capstone article.

Data mining, trade finance, and KYC best practices are some areas that could benefit from additional in-depth research. A review of the data mining techniques and tools available could reveal further approaches for banking institutions to uncover TBML activity using acquired financial and consumer data. Because trade finance, while conducted by banking institutions, falls outside of the scope of AML/CTF compliance, it was not included in this capstone project. It would be good to do research on this topic in order to create recommendations tailored to the trade finance departments of banking institutions. Finally, during the literature review, customer due diligence techniques were discussed. More in-depth study on KYC, on the other hand, might be performed to discover best practices that banking institutions can use to lower the risk of supplying customers who engage in illegal activities.

CHAPTER 7

Conclusion

The most common technique of unlawful money transfer is thought to be trade-based money laundering. TBML is used by criminal organizations to launder money, and it has also been identified as a new means of terrorism financing. Banking institutions are appealing for the flow of cash generated by or destined for criminal activities since they offer a variety of financial products and make international payments transfers simple. Enhanced banking rules, on the other hand, have moved money laundering away from traditional routes of money transmission and toward value transfer through commerce. Because of TBML's intricacy, it's simple to pass it off as routine trading transactions amid the enormous volume of transactions performed by numerous banking institutions on a daily basis. As a result, banking institutions must be able to detect and escalate TBML behavior as soon as it is detected.

The TBML/FT methodology entails the transfer of value through trade, which is frequently accomplished by mixing money with genuine trade in order to conceal the activity. It can range from extremely simple systems to complex schemes, and it rarely consists of just one strategy, making it much more difficult to spot. Several proven mechanisms, such as IVTS and BMPE, can be used to transfer value, but criminal groups and terrorist financiers will employ whichever method best suits their objectives. This has resulted in the development of new TBML strategies, such as the use of alternative payment methods, casino gambling, real estate transactions, and online sales. Additional obstacles include the desire for secrecy and the constant shifting of geographical places when more advantageous options emerge. Banking institutions are in a unique position to detect this behavior since monies will undoubtedly travel via the formal banking system at some point during the process.

Knowledge is the key to detecting TBML activity after it enters the banking system. Familiarity with the many TBML methodologies and the red flag indicators unique to each enables for better alert production and investigations, as well as the capacity to search for patterns in past data. Knowing what tools are available and what questions to ask during an investigation can help you distinguish between legitimate and illegal conduct and communicate suspected activity to law enforcement more effectively. Sharing information across banking institutions, law enforcement, regulators, and industry groups promotes collaboration among the various entities fighting TBML. Banking institutions must have AML/CTF processes that involve customer due diligence, transaction monitoring, and escalation provisions, according to current banking legislation. As a result, the majority of banks and credit unions are already on the correct track. The fight against TBML will simply be more effective if the existing process is refined by targeted training, algorithm enhancement, data mining, and information exchange.

References

Trade-Based Money Laundering A Comprehensive Approach to Combat TBML. Retrieved 19 February 2022, from https://www.oracle.com/us/industries/financial-services/fs-trade-based-money-laundering-4029018.pdf

Trade-based money laundering - fatf-gafi.org. FATF. (n.d.). Retrieved February 19, 2022, from https://www.fatf-gafi.org/media/fatf/content/Trade-Based-Money-Laundering-Trends-and-Developments.pdf

Sullivan, C., & Smith, E. (2011). Combat: Multi-party Solutions for Trade-based Money Laundering. (2022). Retrieved 19 February 2022, from https://www.r3.com/wp-content/uploads/2021/03/Solutions_for_Trade_Based_Money_Laundering_Whitepaper_R3_2021.pdf

Trade-Based Money Laundering A Comprehensive Approach to Combat TBML. Retrieved 19 February 2022, from https://www.oracle.com/us/industries/financial-services/fs-trade-based-money-laundering-4029018.pdf

Ifc.org. 2018. Navigating Essential Anti-Money Laundering and Combating the Financing of Terrorism Requirements in Trade Finance: A Guide for Respondent Banks. https://www.ifc.org/wps/wcm/connect/bde5bd94-46a9-43be-862d-379708973e9c/20180918_Guide-for-Respondent-Banks.pdf?MOD=AJPERES&CVID=mpuzBch

Wolfsberg-principles.com. 2019. The Wolfsberg Group, ICC and BAFT Trade Finance Principles.https://www.wolfsbergprinciples.com/sites/default/files/wb/Trade%20Finance%20Principles%202019.pdf

Gov.im. 2018. Notice 1000 MAN Trade-Based Money Laundering. https://www.gov.im/media/1348726/notice-1000-man-trade-based-money-laundering-july-18.pdf

https://media.proquest.com/media/hms/ORIG/2/dhV4K?_s=3fxg7DMG0SHUziinKjC4u9UEoa4%3D

Eurasiangroup.org. 2010. Money Laundering vulnerabilities of Free Trade Zones. https://eurasiangroup.org/files/FATF_docs/ML_vulnerabilities_of_Free_Trade_Zones.pdf

Static1.squarespace.com. 2021. TRADE-BASED MONEY LAUNDERING JACK OF ALL TRADES AND MASTER OF NONE. https://static1.squarespace.com/static/5c12a68fc258b4c36480afb6/t/6034e7407e6ae709881e3671/1614079838665/Trade-based+money+laundering_+jack+of+all+trades+and+master+of+none.pdf

Jyx.jyu.fi. 2020. BEST PRACTICES IN CONTROLLING TRADE-BASED MONEY LAUNDERING. https://jyx.jyu.fi/bitstream/handle/123456789/69763/1/URN%3ANBN%3Afi%3Ajyu-202006084020.pdf

Wto.org. 2022. Trade finance and the compliance challenge A showcase of international cooperation. https://www.wto.org/english/res_e/booksp_e/tradefinnace19_e.pdf

Amlc.nl. 2017. Combatting Trade Based Money Laundering: Rethinking the Approach. [online] Available at: <https://www.amlc.nl/wp-content/uploads/2018/11/baft17_tmbl_paper.pdf>

USING INTELLIGENCE TO COMBAT TRADE-BASED MONEY LAUNDERING. (2020). Retrieved 19 February 2022, from https://www.insaonline.org/wp-content/uploads/2020/04/INSA_WP_TBML.pdf

GUIDANCE ON ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM CONTROLS IN TRADE FINANCE AND CORRESPONDENT BANKING. (2015). Retrieved 19 February 2022, from https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/Guidance-on-AML-CFT-Controls-in-Trade-Finance-and-Correspondent-Banking.pdf

APG Typology Report on Trade Based Money Laundering. (2012). Retrieved 19 February 2022, from https://www.fatf-gafi.org/media/fatf/documents/reports/Trade_Based_ML_APGReport.pdf

NAHEEM, M. (2017). TRADE BASED MONEY LAUNDERING: EXPLORING THE IMPLICATIONS FOR INTERNATIONAL BANKS. Retrieved 19 February 2022, from https://wlv.openrepository.com/bitstream/handle/2436/620745/NAHEEM%20PhD%20Thesis.pdf?sequence=1&isAllowed=y

Davidson, H. (2014). THE PHENOMENON “MONEY LAUNDERING” Whose money is dirty and what are the effects? Retrieved April 15, 2022, from https://www.theseus.fi/bitstream/handle/10024/97595/Hanna+Davidsson+Master+Thesis+Money+Laundering.pdf?sequence=1