Anti-money Laundering Law in Ethiopia: Issues of Enforcement with Specific Reference to Banks

Kalkidan Misganaw Jember ♣

Abstract

Banks are among the institutions which take the leading role in the combat against the crime of money laundering. They, however, remain highly vulnerable to an ever growing means and mechanisms of perpetration of the crime. This reality demands a continuous adoption of necessary measures. In what appears to be responding to this demand, Ethiopia has enacted several laws that impose obligation on banks to take preventive measures that can prevent the manipulation of the financial system towards the commission of laundering. This article examines whether banks (both private and public) in Ethiopia are implementing measures intended to prevent money laundering. Secondly, it examines the relationship and collaboration between banks and the regulatory organs (such as the Financial Intelligence Center and the National Bank of Ethiopia) in identifying and safeguarding against the schemes that allow the use of banks as intermediaries in the commission of money laundering.

Key terms

Money laundering · Banks · Compliance · Preventive measures

DOI http://dx.doi.org/10.4314/mlr.v14i1.3

Received: 10 February 2020 **Accepted**: 4 September 2020

Suggested citation:

Kalkidan Misganaw Jember (2020), 'Anti-money Laundering Law in Ethiopia: Issues of Enforcement with Specific Reference to Banks', 14 *Mizan Law Review* 1:31-60

♣ Kalkidan Misganaw Jember (LL.B, LL.M), Lecturer, School of Law, Jimma University; Tel: +251991740167
Email: kalshamisganaw@gmail.com or kallemisganaw85@gmail.com
ORCID: https://orcid.org/0000-0002-1856-3026

Introduction

As Ethiopia's economy is highly cash-based, there are some vulnerable institutions whose services are exploited by launderers. Banks are among these institutions, and they are usually in the frontline in the combat against illicit money movements. "Banks have been the major targets of laundering operations" because "they provide finance related products and services, facilitating domestic and international payment" which has nexus with techniques employed to launder dirty asset.[1] They are thus entrusted with different anti-money laundering responsibilities.

Failure to effectively control these institutions would likely expose them for launderers. It is thus imperative to empower and strengthen these institutions with different tools so that they can combat money laundering. This article examines the adequacy of Ethiopian law in the combat against money laundering and assesses the existing practices of anti-money laundering tools by banks. In addition to analysis of the law, questionnaires and interviews were employed as specific data collection tools. Eight (out of sixteen) private banks discussed in this article were randomly selected. With regard to the Commercial Bank of Ethiopia, purposive sampling was employed as it is the only government owned commercial bank in the country. This methodology is necessary to answer the question of assessment of the practice of selected banks concerning their compliance with anti-money laundering laws. Interviews were made with regulatory organ officers.

Acronyms:

AML	Anti-money laundering
CDD	Customer due diligence
CTRs	Cash transaction reports
FATF	Financial Action Task Force
FDRE	Federal Democratic Republic of Ethiopia
FIC	Financial Intelligence Center
KYC	Know your customer
PEPs	Politically exposed persons
STRs	Suspicious transactions

[1] Biniam Shiferaw (2011), 'Money Laundering and Countermeasures: A Critical Analysis of Ethiopian Law with Specific Reference to the Banking Sector' LLM Thesis on file at Addis Ababa university, pp. 47-48. *See* also Isa Yusarina et.al (2015), 'Money Laundering Risk: From the Bankers' and Regulators perspectives' *Procedia Economics and Finance* vol.2 8, p.7. Among the techniques employed to launder dirty asset *placement* is the prominent one in which the criminal may simply "deposit" the cash (he/she derives from commission of a crime) at certain financial institution or may transfer the money to somebody in order to evade forfeiture of the asset.

Section 1 briefly highlights the concept of money laundering. Sections 2 and 3 discuss the Ethiopian legal framework that governs money laundering. These sections respectively deal with criminalization of money laundering (Section 2), and the responsibilities of banks in combating the crime and the enforcement of the law (Section 3).

1. The Concept of Money Laundering

The Financial Action Task Force (FATF), an international organization responsible for standard-setting in anti-money laundering, defines money laundering as "the processing of criminal proceeds to disguise their illegal origin."[2] Money laundering is the process of converting or transferring ill-gotten asset to evade its true source and make it reappear as legitimate one. To this end, there are three well known techniques that launderer may use; namely *placement*, *layering* and *integration*.[3] The *Placement* stage refers to the act of removing bulky cash that criminals derive from the scene of the crime; and usually at this stage they go to financial institutions to avoid detection by authorities. At *layering* stage, the money goes through complex transactions which are important to layer the true origin of the money; and in

[2] FATF, *http://www.fatf-gafi.org/faq/money laundering/* accessed on January 26, 2019. The FATF was established by the G7 Summit, held in Paris in 1989. It was held with the intention of giving an appropriate response to the threat posed by money laundering. Initially, it was empowered with the power of examining money laundering techniques and trends; and, setting out the measures that are necessary for averting the danger. Accordingly, the FATF came up with Forty Recommendations on how to fight money laundering. However, in 2001, following the September 11 terrorist attack, the FATF mandate is expanded to include the combat against the financing of terrorism. As a result, nine special recommendations that targeted at fighting terrorism financing were added. At present there are 40 + 9 FATF recommendations. There are, currently, 37 states members to the FATF; specifically, 35 jurisdictions and 2 regional organizations (the Gulf Cooperation Council and the European Commission). These 37 states members are at the core of global efforts to combat money laundering and terrorist financing. There are also 31 international and regional organizations which are associate members or observers of the FATF and participate in its work. In collaboration with other international stakeholders, the FATF also works to identify national-level vulnerabilities with the objective of protecting the international financial system from misuse. Ensuing its endorsement by 180 countries, the FATF is currently recognized as international standard on anti-money laundering and countering the financing of terrorism.

[3] Angela Leong (2007), *The Disruption of International Organized Crime: An Analysis of Legal and Non- Legal Strategies,* p. 33.

integration phase the money is repatriated to the economy seemingly legitimate by mixing it with the legal assets.[4]

There is controversy as to the origin of the term money laundering; some believe that it was coined in the 1920s in USA when Al Capone who led the Chicago mafia and concealed the money derived from gambling, rackets and liquor by intermingling it with the cash generated from doing launderettes and car washes.[5] There are also authors such as Jeffery Robinson, who state that the term was first used –in newspaper reporting– in 1973 in relation with the Watergate scandal.[6] The term was judicially recognized in 1982 in the US case United States v $4,255,625.39.[7]

Although it is difficult to estimate the exact amount of assets laundered globally (due to the mysterious nature of the crime), the IMF estimates it to be somewhere between two and five percent of the world GDP or between 1.5 trillion USD and 2.8 trillion USD.[8] In Africa, there is no separate study conducted as to the amount of assets laundered per year. Humphrey Moshi revealed that the existence of chronic public corruption and conflict coupled with the low level capacity of law enforcement organs has made Africa safe haven for launderers.[9] In Ethiopia, different studies point out that the country is susceptible to money laundering due to corruption,[10] human and arms

[4] Ibid.

[5] Lilley Peter (2006), *The Untold Truth about Global Money Laundering, International Crime and Terrorism*, 3rd edn, p.7; see also Bajram Ibraj (2016), 'Money Laundering in Albania for the Years 2008-2015' *European Journal of Economics and Business Studies* vol.6(1), p. 101.

[6] Financial Action Task Force (FATF), http://www.fatf-gafi.org/faq/money laundering/ accessed on January 24, 2019.

[7] Sirajo Yakubu (2017), 'A Critical Appraisal of the Law and Practice Relating to Money Laundering in the USA and UK' PhD thesis submitted to School of Advanced Study University of London, p. 33.

[8] Financial Action Task Force (FATF), http://www.fatf-gafi.org/faq/money laundering/ accessed on January 24, 2019.

[9] Humphrey Moshi (2007), 'Challenges of fighting money laundering in Africa' *Institute for Security Studies*, p.1.

[10] As per the Transparency International Corruption Perception Index Report of the Year 2017 Ethiopia scored 34. Available at *http://www.transparency.org/news/feature/corruption_perceptions_index_2017* accessed on January 27, 2018. The Corruption Perceptions Index measures the perceived levels of public sector corruption worldwide. When the score is proximate to "0" the country is highly corrupt and when its score is approaching to "100" it becomes a clean nation.

smuggling, contraband, tax evasion and illegal livestock trade.[11] At present, drug trafficking has also become a threat to Ethiopia, as it would inevitably involve money laundering activities.[12]

2. Criminalization of Money Laundering

Starting from the 1988 Vienna Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances,[13] many international legal initiatives targeted at thwarting the commission of money laundering and gave due emphasis to the protection of the financial system from criminal abuses.[14] Ethiopia has promulgated legislation against money laundering and is party to different international treaties adopted to this end.

Even though Ethiopia's Penal Code was promulgated in 1957,[15] the criminal offence of money laundering was introduced under the 2004 Criminal Code.[16] Money laundering is "the process of disguising the true

[11] ESAAMLG *Mutual Evaluation Report on Anti-Money Laundering and Combating the Financing of Terrorism*: The Federal Democratic Republic of Ethiopia (2015), p.3. This mutual evaluation of Ethiopia was conducted by the World Bank and ESAAMLG.

[12] United Nations Office on Drug and Crime (UNODC), *Market analysis of Plant-based Drugs: opiates, cocaine, cannabis World Drug Report* (2017). Accordingly, in 2015, 35 % of the heroin found in Belgium had transited the southern route (mainly via Burundi and Ethiopia).

[13] Whilst the main rationale for adopting the 1988 Vienna convention was suppressing the trafficking of drugs, at this time the international community was also aware of the fact that the main factor that helps criminals to persist their evil action was the huge sum derived from drug trafficking. So, to avoid the problem of drug trafficking from the source, targeting the profit also makes the weapons aimed at alleviating drug trafficking meets its goal of hitting the backbone of the criminal. To this end, the Vienna Convention contains provisions that criminalize the conversion of asset derived from drug trafficking. For further detail see the preamble.

[14] As it can be inferred from different international as well as regional responses to money laundering the main rational for their promulgation was to empower and strength those vulnerable institutions for money laundering. See for instance, the preamble of Basel principle for Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering (December 1988).

[15] The 1957 Penal Code of the Empire of Ethiopia, proclamation No.158/1957, Extraordinary Issue No. 1 of 1957 of the Negarit Gazeta, 23 July 1957, *entered into force* 5 May 1958.

[16] The Criminal Code of the Federal Democratic Republic of Ethiopia, Proclamation No. 414/2004, *entered into force* 9 May 2005, Art. 684, [herein after FDRE Criminal Code].

origin of ill-gotten money or property into seemingly legitimate money or property and it includes concealing or disguising the nature, source, location, disposition or movement of the proceeds of crime or knowingly alerting, remitting, receiving or possessing such tainted money."[17] Article 684 of the Criminal Code contains three basic elements, namely, (*i*) disguising the source of money derived from corruption, drug trafficking, arms smuggling or other serious crimes through investment, transfer or remission; [18] (*ii*) aiding in concealment of proceeds of crime;[19] and (*iii*) acquisition, use and possession of property or money while knowing the unlawful source.[20]

Predicate offences for money laundering are all serious crimes. For the purpose of punishing money laundering, serious crime means a crime punishable with rigorous imprisonment of ten or more years or where the amount of money or the value of the property involved in the crime is at least fifty thousand Birr.[21] The Criminal Code follows different definitions for the term serious crime for different criminal acts.[22] Nonetheless, it is not clear why the Criminal Code uses a different threshold (relating to the range of punishment) for defining serious crimes in case of money laundering. Normally, the Code recognizes as serious any crime punishable by rigorous imprisonment for a period of one to twenty-five years. [23]

The deviation of Article 108 of the Criminal Code from the common definition of 'serious crimes' appears to be a deliberate in light of what the FATF requires. In this regard, the FATF requires all predicate offences to be serious offences. The difference lies on the question of what serious offence constitutes. Under its interpretive note 3 paragraph 3, the FATF states that serious crimes comprise crimes punishable by a maximum of more than one-year imprisonment, or for those countries with a minimum threshold in their legal system predicate offences should comprise offences which are punishable with a minimum penalty of more than six months imprisonment.[24]

---

[17] Biniam Shiferaw, *Supra* note 1, pp. 43-44.
[18] The Criminal Code, *supra* note 16, Art. 684(1).
[19] Id, Art. 684(5).
[20] Id, Art. 684(2).
[21] Id, Art. 684(7).
[22] Ibid. For instance, 'serious crime' for the sake of crime of conspiracy refers crimes which are punishable with rigorous imprisonment for five years or more are taken as serious crime.
[23] Id, Art. 108(1).
[24] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (2012), Interpretive Notes to the FATF Recommendation 3, p.34.

Therefore, the FDRE Criminal Code contains only few predicate offences and is not compatible with the minimum threshold required by the FATF.[25] Biniam argues that the definition given for the word serious crime under the FDRE Criminal Code is too narrow; because, it does not include offenders of different crimes that generate large amounts of money in the course of crimes (such as trafficking in women for prostitution) unless the profit derived is beyond 50,000 Birr, and in effect, such offenders are not prosecuted for money laundering and other similar acts as they do not fall under the category of serious crimes. [26]

In 2009, a specific proclamation was enacted which aims at the effective implementation of the Criminal Code provision on the prevention and repression of the crime of money laundering.[27] Despite the efforts made to criminalize money laundering, the FATF had categorized Ethiopia (in 2010) as a jurisdiction with a strategic deficiency in terms of adequately criminalizing money laundering and relating to the level of effective functioning of the Financial Intelligence Center (FIC).[28] On the basis of this recommendation, Ethiopia has repealed its anti-money laundering law and has enacted a new proclamation in 2013 with a view to effectively and comprehensively fight money laundering.[29] Under Proclamation No. 780/2013, money laundering refers to:

> an offence, or any person who knows or should have known that a property is the proceeds of a crime and who converts or transfers the

[25] The Ethiopian case, however, is ten or more years of imprisonment or if the amount of money or property involved is more than 50,000 birr without regard to year of imprisonment.

[26] Biniam Shiferaw, *supra* note 1, p. 45.

[27] Prevention and Suppression of Money Laundering and the Financing of Terrorism Proclamation No. 657 of 2009. Hereinafter Proclamation No. 657/2009, preamble para. 2 provides that "it has become imperative to legislate special law to have an effective implementation of the provisions of the Criminal Code criminalizing money laundering as an offence."

[28] FATF Public Statement – Public Statement No.1 available at http://www.fatf-gafi.org/publications/high-riskandnoncooperativejurisdictions/documents/fatfpublicstatement-february2010.html Accessed on January 31, 2018.

[29] Proclamation for the Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation No. 780 of 2013, hereinafter Proclamation No. 780/2013. The preamble, para. 3 of the Proclamation provides that "it has become necessary to have comprehensive legal framework to prevent and suppress money laundering and financing of terrorism."

> property for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of the predicate offence to evade the legal consequences of his actions; conceals or disguises the true nature, source, location, disposition, movement or ownership of or rights with respect to the property; acquires, possesses or uses the property; or participates in the commission, conspires to commit, attempts to commit or aids, abets, facilitates or counsels the commission of any of the elements of the offence.[30]

Under this provision, money laundering refers to the act of obscuring the true source of the criminal proceeds to make it appear as legal. Compared to its predecessor, the current law embodies a wider definition of money laundering, which includes acquisition, possession or use of the property which at the time of acquisition, possession or usage of that property, the individual knows or should have known that the thing is the proceed of a crime. [31] Counseling, assisting any person involved in the commission of that offence and even conspiracy to commit money laundering is also a punishable offence.[32] The definition given to the crime is broad and contains a wider range of predicate offences than its predecessor.[33] However, the issue of terrorism financing as predicate offence is not clearly addressed.

Ethiopia has criminalized terrorism financing under its Anti-Terrorism Proclamation. The proclamation prohibits rendering support for terrorism in any form. The Anti-Money Laundering Proclamation also criminalizes the act more broadly by prohibiting the provision of direct or indirect aid for a terrorist person or terrorist organization, or the collection of fund with the intention or knowledge that it may be used for carrying out terrorist activities; the act is punishable with rigorous imprisonment from 10 to 15 years and with fine not exceeding Birr 100,000.[34]

Although, the law clearly includes terrorist financing as predicate offence for money laundering, this author thinks that terrorist financing could not be

[30] Id, Arts. 2(10) and 29.
[31] Id, Art. 29(1)(c).
[32] Id, Art. 29(1)(d).
[33] *See* for example, id, Art. 2(4) which defines predicate offence as 'any offence capable of generating proceeds of crime and punishable at least with simple imprisonment for one year'.
[34] Id, Art. 31.

predicate offence for the crime.[35] Money laundering relates to making ill-gotten asset appear legitimate by tunneling it through various processes. Terrorism financing is an offence that results from an act of (material or moral) support to the terrorist or terrorist organization. The asset may come from the individual's legal or illegal asset.

Apparently, support that comes from a legal asset does not fall under money laundering, but constitutes another offence. The second scenario is, when a person funds a terrorist from ill-gotten assets. This does not also fulfill the criteria of obscuring or concealing the true nature of the asset to make it reappear as licit, even though the individual is criminally liable in another offence. Therefore, I argue that terrorism financing either from legal or illegal income would not make the crime predicate offence for money laundering because there is no seemingly legit income to be derived out of it.

3 Responsibilities of Banks in Combating Money Laundering and Its Enforcement in Ethiopia

Stringent professional standards of secrecy in banks had created great opportunity for criminals to hide their illegally amassed asset in bank accounts. However, the FATF recommendations, have brought about changes in this regard since the 1980s. In effect, states individually started to address the impediments caused by bank secrecy in the fight against economic crimes such as money laundering. Currently, the anti-money laundering discourse makes it clear that bank secrecy cannot be as strict as it used to be thereby allowing exception with the aim of fighting the menace of money laundering.

A closer look at Proclamation No. 780/2013 reveals that the Proclamation gives due attention to the regulation of banking services so that financial transactions shall not be conducted in a manner that facilitates money laundering. In that sense, banks are considered the principal institutions that are required to implement various anti-money laundering measures.

3.1 Implementation of risk-based approach

According to the *risk-based approach,* countries, competent authorities, and banks shall identify, assess, and understand the money laundering and terrorist financing risk to which they are exposed, and take the appropriate

[35] Id, Art. 2(4). Terrorist financing is punishable with rigorous imprisonment from 10 to 15 years and with fine not exceeding Birr 100,000. It may be argued that terrorist financing is predicate offence to money laundering.

mitigation measures in accordance with the level of risk. Under the FATF, countries are required to follow *risk-based approach* while fighting money laundering. This approach enables countries to conduct national risk assessment and identify their risk and level of the respective risk in order to take effective action to mitigate it. Risk-based approach has the advantage of effectively allocating scarce resources by focusing on assessing the customers with highest money laundering risks[36] which in turn enables banks to prevent the commission of money laundering efficiently. According to this approach, banks shall assess the risk posed by each customer as high and low risk based on the types of customers,[37] types of the customer's business, and the product and geographical location of the customer.[38] The implementation of appropriate mitigation measures vary depending upon their risk level. The review of the risk rating for high risk customers may be undertaken more frequently than for other customers.[39]

Accordingly, countries shall identify and assess the money laundering and financing of terrorism risks on a continuous basis. National risk assessment has three benefits: (i) it is informative with regard to need for changes to the country's anti-money laundering laws, regulations and other measures; (ii) it assists the implementation of risk-based approach; and (iii) it provides banks and other responsible institutions information which is important to them to make their own risk assessment. [40]

Conducting risk assessment is important to have a common understanding of the available risk of money laundering in the country by different stakeholders and to work on such identified risk which in turn implies on the use of scarce resources. In Ethiopia, since its establishment, the FIC is engaged in identifying the risk of money laundering. To this end, it has collected relevant data. However, the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) had stated (in 2015) that the

---

[36] FATF, *supra* note 24, Recommendation 1 and interpretive note to recommendation 1.

[37] Politically exposed person or his/her close relative and family will have high risk of committing laundering as compared to a certain civil servant.

[38] Tim Parkman [2012] *KYC and Risk Based Approach in Mastering Anti-Money Laundering and Counter Terrorist Financing: Compliance guide for practitioners*, Pearson publisher, p. 192.

[39] Federal financial Institutions Examination Council Bank Secrecy Act Anti-Money Laundering Examination Manual available at https://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm ; accessed on April 12, 2018.

[40] FATF, *Guidance on National Money Laundering and Terrorist Financing Risk Assessment* (2013), pp. 7-8.

collected data has lapsed many years and may fail to depict the current risk thereby suggesting review of collected data.[41]

FIC responded positively by deciding to update the data; and the national risk assessment of Ethiopia was finalized at the end of 2016 although the identified risk areas were not made publicly available.[42] The national risk assessment is a basis for banks to categorize their customers as high, medium and low money laundering risks. [43] Nonetheless, banks in which the author has made assessment do not know the national risk assessment result conducted in Ethiopia by the FIC. From interviews made with compliance officers, each bank has done its own risk assessment and identified high risk customers as indicated by the law.

3.2 Know your customer (KYC)

The starting point for banks in the fight against money laundering is knowing and identifying their customers. The aim of this obligation is elimination of anonymous accounts and the identification of hidden principals or beneficial owners. Financial institutions should establish the actual ownership of accounts and should refuse to enter into transactions with clients who fail to provide proof of their identity. Financial institutions should be required to obtain proof of a client's identity when a business relationship is established or when a transaction is concluded with that client. KYC has two basic elements; the first is *customer identification*; and the second element is *customer due diligence* (CDD).[44]

For natural persons, customer identification involves given or legal name and all other names used; permanent address; telephone number, fax number and e-mail address, if available; date and place of birth, if possible; nationality; occupation, public position held and/or name of employer; type

[41] ESAAMLG (2015), *supra* note 11.

[42] Interview made with compliance officers of Abay Bank, Abyssinia Bank, Dashen Bank, Nib International Bank, Oromia Cooperative Bank, Oromia International Bank, Wegagen Bank, Commercial Bank of Ethiopia and Zemen Bank. (May 22 to 24, 2018)

[43] In interviews conducted with FIC officials, they said there is no obligation to make the assessment result public and that is why the center fails to do so.

[44] Sullivan Kevin (2015), *Anti-Money Laundering in a Nutshell: Awareness and Compliance for Financial Personnel and Business*, Verlag: Apress, p. 71.

of account; and signed statement certifying accuracy of the information provided.[45]

There are also separate requirements needed for identifying legal persons such as, name, legal form and proof of existence, some form of official identification number such as tax identification number (if available), address (which includes country, City/Town/*Wereda*/ Kebele in which the head office is located and if available, house number, mailing address, telephone number and fax number) and identification of those who have authority to operate the account.[46] This relevant information has to be collected by the respective banks when they start relation with customers for both natural and legal persons.[47]

Apart from collecting the above information, banks shall verify the validity of the information provided by the customer.[48] But the appropriate mechanism necessary for verification is not indicated in the law which imposes a duty (on financial institutions in general and banks in particular) to verify the veracity of the required information provided by the customer. The absence of a national identity system is a gap that should be addressed, and the manner in which the required proof is to be obtained should be clarified by regulation.

Customer due diligence (CDD) is among the preventive measures to be employed by banks to prevent or at least mitigate the commission of money laundering and helps to protect the reputation of the institution.[49] Banks have to know who their customers are. In other words, they are responsible for verifying the identity of their customers and beneficial owners before or during the course of establishing a business relationship or conducting transactions for occasional customers. As these institutions are obliged to adopt *Risk-Based Approach* to categorize their customers based upon their risk for this crime, this approach reveals the risk levels based on which banks should implement adequate CDD measures.

[45] Financial Anti-Money Laundering and Countering the Financing of Terrorism Compliance Directives Number 01/2014, hereinafter FIC Compliance Directive, Art.16 (1).
[46] Id, Art. 17 (2(C)).
[47] Id, Art. 16 and 17.
[48] Ibid.
[49] Guy Stessens, *Money Laundering: A New International Law Enforcement Model* (Cambridge University Press, 2003), p. 146.

CDD is not one-time obligation, and the institution shall take necessary measures to review and update customer's information at intervals.[50] Depending on the updated information, the risks associated with these accounts shall have to be assessed again without delay. The risk level of the customer determines the frequency of the review to avert the danger of money laundering.

As pointed out by the FATF and other regional bodies (established for suppressing money laundering and terrorist financing), some clients such as politically exposed persons (PEPs)[51] should be subjected to Enhanced Customer Due Diligence (ECDD) measures as they are more vulnerable to corruption and other crimes. While establishing relationships or maintaining the existing relation with PEPs, banks are required to be highly cautious. FATF requires the same measure to be applied to their close family members and close associates without defining who those close family members and close associates are.[52]

The same works in Ethiopia, and where a customer is identified as PEP, the bank must request the approval of senior management before it establishes a business relationship with such customer. In the event that the bank establishes a business relationship with PEP, the institution must take reasonable measures to establish the source of the PEP's wealth and conduct ongoing enhanced monitoring of its relationship with the PEP. Under Proclamation No. Proclamation 780/2013, PEP means "any natural person who is or has been entrusted with prominent public function in any country or international organization" and the definition includes "a member of such person's family or any person closely associated" with him/her.[53]

However, the Proclamation does not give the definition of "family members and close associates" that may fall under this domain. For the purpose of asset disclosure and registration, close relatives (under Article 2/8 of the Disclosure and Registration of Assets Proclamation No. 668 /2010)

[50] Kevin, *supra* note 44, p.71.

[51] International legal instruments show that there is no consistent terminology or comprehensive definition of PEPs. They use different phrases such as Politically Exposed Persons and Senior Public Official. Politically Exposed Persons (PEPs) refer to "Individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials."

[52] FATF (2012), *supra* note 24, Recommendations 12.

[53] Proclamation 780/2013, *supra* note 29, Art. 2 (11).

include "ascendants, descendants, siblings and other persons related to an appointee, elected person or a public servant by consanguinity or affinity up to the third degree".

Yet, the basic question in this regard is whether PEPs are 'made known by those responsible institutions' for the purpose of due diligence. Even assuming that public officials are known by those banks, a question arises whether their close relatives and families are known. This gap in the law enables PEPs to clean ill-gotten assets by using their relatives and even family members, and banks will not be able to conduct the proper CDD measures due to gaps in information regarding the risk of these individuals.

It may be irrational to expect a senior government official to accumulate and transact huge amount of money, which is not commensurate with his/her monthly income in the presence of asset disclosure requirements for public officials. According to Article 2(7) of the Disclosure and Registration of Assets Proclamation No. 668/2010, the definition of 'family' includes "spouse, dependent child under the age of 18, … and includes a person living together under irregular union and an adopted child". Although this seems to open the room for asset accumulation in the name of the PEP's child who is above 18, children of the PEP who are above 18 years of age fall under Article 2(8) of the Disclosure and Registration of Assets Proclamation No. 668 /2010.

Indeed, it is pointless to oblige financial institutions in general and banks in particular to apply enhanced due diligence measures on PEPs as well as their families and close relatives without notifying them who they are. Both Proclamation No. 780/2013 and the FIC Compliance Directives No. 1/2014 do not provide any procedure or yardstick that can be used in identifying PEPs.[54] In an interview with compliance officers and frontline officers of banks, they stated that there is no means that enables them identify family members of PEPs. Likewise, the interview conducted at the FIC directorate, revealed lack of clarity with regard to the organ that shall provide a list of PEPs and their close relatives and families because this is not stipulated in the law and FIC is not empowered to do so. This shows that frontline and compliance officers encounter challenges in this regard because the center does not periodically provide banks with the list of PEPs.[55] Therefore, CDD

[54] Especially under the Financial Anti-Money Laundering and Countering the Financing of Terrorism Compliance Directives Number 01/2014, it could have been possible to provide definition of family members and close relatives but it failed to do so.

[55] Interview with Ato Kidane Mariam G/tsadik, FIC Financial Transaction Inspection and Analysis officer (May 25, 2018).

measures on these individuals could not be implemented by banks.[56] The same problem holds true in identifying PEPs when they are the beneficial owners.

The other issue that is worth discussing is identifying customers from high risk jurisdictions. FATF stipulates that financial institutions shall afford special attention to their business relationships and transactions with both natural and legal persons from countries which fail to sufficiently comply with the FATF Recommendations.[57] The background and purpose of these business relationships and transactions must be examined when their business or legal purpose is not apparent. The findings of the examination must be recorded in writing and be made accessible to the competent authorities.

Likewise, there is a Directive in Ethiopia that renders customers from high risk jurisdictions to be subject to Enhanced CDD measures.[58] Customers from other jurisdiction could be categorized as high risk due to lack of proper anti-money laundering regulation in their country and these customers may pose danger to Ethiopia. The FIC is thus responsible to provide a list of these jurisdictions to the banks and also annually update the situation of every jurisdiction. In spite of the stipulation under the Proclamation, however, the FIC (while promulgating CDD directive) only mentioned that customers from high risk jurisdictions are among the categories that need Enhanced CDD measures and/or senior management approval before a bank establishes relation with the customer. [59]

3. 3 Reporting of suspicious transactions (STRs)

STR is a fundamental element of international anti-money laundering systems. Banks are required to report suspicious transactions made by customers. Reporting would facilitate the detection of predicate offences and consequently prevent and/or reduce crime. Compliance with AML laws would also protect the reputation and integrity of banks. All suspicious transactions, including attempted transactions, should thus be reported

[56] Interview made with compliance officers of Abay Bank, Abyssinia Bank, Dashen Bank, Nib International Bank, Oromia Cooperative Bank, Oromia International Bank, Wegagen Bank, Commercial Bank of Ethiopia and Zemen Bank (May 22, 2018)..

[57] FATF, *supra* note 24, Recommendation 21.

[58] FIC Compliance Directive Number 01/2014, *supra* note 45, Art. 12 (b (i). Enhanced customer due diligence involves making extra checks on a customer's identification, collecting additional information and doing additional verification.

[59] Ibid.

regardless of the amount of the transaction. As some authors noted, reporting "suspicious transaction is the backbone of preventive measures under the FATF Standard." [60]

However, it must be noted that a transaction that appears unusual is not necessarily suspicious. Even customers with a profile of stable and predictable transactions will have periodic transactions that are unusual for them. Many customers may, for perfectly good reasons, have an erratic pattern of transactions or account activity. So, unusual transaction is, only a basis for further inquiry, which may in turn require judgment as to whether it is suspicious or not. The personal judgment of the person who faces this situation is necessary; and the issue of competence to identify whether or not the money is a proceed of crime needs further training so that it does not result in having lots of unnecessary reports.[61] The FATF interpretative note to Recommendation 20 clarifies that the term criminal activity should be understood as any predicate offence for money laundering, as defined by the national laws of individual countries.[62] Therefore, banks shall notify, the FIC, an organ established for receiving and analyzing suspicious reports, if they suspect that the money is a proceed of crime which is categorized as predicate offence by the respective nation.

In this respect Ethiopian anti-money laundering law with regard to suspicious transaction obliges banks to report on mere suspicion. As stated above, the problem of this reporting method is that the reporting institution, in its quest to comply with the law, will send false positive reports to the financial reporting center and overwhelm it with unnecessary reports. In this regard, the technical competence of the frontline officers and individuals who assess the risk of money laundering should be steadily enhanced through consistent training organized by the regulatory organ established to undertake this task.

In many jurisdictions, it is the compliance officer who is entrusted with the power of reporting any suspicious transaction to the authority. The responsibility to ensure compliance with anti-money laundering rules is a relatively new function in the banks. Therefore, employees are obliged to work diligently with high precaution of identifying and preventing the commission of money laundering by using banks. Where frontline officers

---

[60] Julia Braun *et al* (2016), 'Drivers of Suspicious Transaction Reporting Levels: Evidence from a Legal and Economic Perspective' 2 *Journal of Tax Administration* vol. 2(1), p. 98.

[61] Yusarina, *supra* note 1, p. 10.

[62] FATF, *supra* note 24, Interpretive note to Recommendation 20, para. 1.

fail to detect a risk posed by a customer, the remedy devised by the law envisages that the compliance officer shall analyze transactions made by customers and submit report if there is suspicious transaction. This creates an opportunity to assess risks before reporting to the authorities, and reduce the number of low risk reporting.

The practice also reveals that an unusual change in the pattern of customer's transaction should be observed in order to file the STR.[63] However, no further inquiry is made by the frontline officers, because such inquiry relating to the reason for the change of pattern in their transaction, will lead the customer towards decisions and acts of moving assets to avoid prosecution. Frontline officers thus prefer to simply report the situation to the compliance officers and the report is ultimately made to the FIC.

The FIC claims that various suspicious transaction reports they received from banks have gaps in clarity and adequacy. The problem may be related to lack of pre-investigation for the cause of abnormal change or frequency of customer's transaction. According to a compliance officer of a bank, there are red flags identified by a banks to file STR such as:[64] (i) having many transactions (deposit or withdrawal) five times within a day although the amount is too minimal, (ii) accounts which remain inactive for long time, but starts to make frequent transaction, and (iii) a customer who sends money for many individuals unless it is *per diem*, or salary or he/she has relation with them.

3.4 Record keeping

Maintaining record is important both for the prevention and detection of money laundering and terrorist financing purposes. The record shall consist full customer identification information, account opening forms, copies of identification documents, business correspondence and other relevant details. This record maintenance helps to detect those involved and provides a financial trail to help competent authorities pursue those involved. It thus serves as evidence for prosecution of criminal activity. [65]

FATF requires banks to keep all records for at least five years after the termination of the business relationship or after the date of the occasional

[63] Questionnaires distributed among frontline officers of selected banks revealed that the officers simply fill the form prepared by FIC if they see unusual change in the pattern of transaction of that customer.

[64] Interview conducted with Awash Bank Compliance Officer, May 22, 2018.

[65] Proclamation No. 780 /2013, *supra* note 29, Art. 55.

transaction. But the period of retention of the recorded information may be extended depending upon domestic regulation. Article 10 of Proclamation No. 780/2013, requires retention of the record for at least 10 years from the date of the attempt or execution of the transaction, and in case other laws require maintaining of the record for longer periods, such laws shall have effect. This is indeed effective in the fight against money laundering. The banks covered in this study keep the necessary and required information under the law. The FIC also acknowledges this activity, and when it needs additional information and if it wants to consult the recorded document, the records are available at the banks.[66] Therefore, banks are complying with the record keeping requirement.

3. 5 Tipping off

Employees of banks who have access to a report of suspicious transaction shall not disclose the information.[67] This prohibition is meant to prevent loss of evidence and possible interference in the investigation process. But this prohibition is not without any exception; divulging information between and among directors, officers and employees of the financial institutions and appropriate competent authorities regarding suspicious money laundering or financing of terrorism is allowed.[68]

Tipping off is a criminal act, but the FATF advises countries that while they criminalize tipping off it should be made with due care. The criminalization should not adversely affect the anti-money laundering struggle by imposing undue fear on professionals such as bankers. For example, a banker who conducts its CDD obligations may unintentionally tip off the customer. However, this should not be an excuse for gross negligence. Therefore, if banks suspect that transactions relate to money laundering or terrorist financing, they should take into account the risk of tipping-off while performing the CDD process. If the bank reasonably believes that performing the CDD process will tip off the customer or potential customer, it may choose not to pursue that process, and should file

[66] Interview with Ato Kidane Mariam G/tsadik, FIC, Financial Transaction Inspection and Analysis officer, May 25, 2018.

[67] Proclamation No. 780 /2013, *supra* note 29, Art. 20(1).

[68] For instance, art. 20(2) of the Ethiopian anti-money laundering law allows communication of acquired information regarding suspicious money laundering or financing of terrorism with the financial institution itself or even for other competent organs.

STR.[69] Banks should ensure that their employees are aware of, and sensitive to, these issues when conducting CDD.

Ethiopia's anti money laundering law prohibits disclosure of information (to the suspect or third parties) with regard to reports that have been made or will be made, and this is liable to punishment.[70] But this prohibition needs careful interpretation so that it does not discourage CDD measures under the fear that the customer may be aware of something bad that is going to happen to him/her. Therefore, the law should only criminalize intentional tipping off, and Ethiopia's law has failed to do so.

3.6 Cash transaction report (CTR)

Banks are required to report to FIC each transaction made with a customer which comprises the receipt or payment of an amount of money exceeding the amount set by the FIC Compliance Directive No. 1/2014.[71] Unlike reports of STR, there is no need to suspect the money as the proceeds of crime to report cash transactions; and the mere fact that a transaction meets the minimum threshold stipulated by the FIC (either in a single transaction of several but linked transactions) is sufficient.[72] The linkage requirement is developed to cope up with evolving techniques of laundering such as smurfing.

Countries should consider the possible benefits of requiring all cash transactions that exceed a fixed threshold amount to be reported for the fight against money laundering.[73] Each country or jurisdiction establishes its own reporting threshold based upon its own circumstances. Likewise, Ethiopia also obliged financial institutions to report to the FIC all cash transactions in any currency above the sum of ETB 300,000.00 or USD 15,000 or foreign currency equivalent for both individuals and legal persons whether the transaction is conducted as a single transaction or several transactions that appear to be linked.[74]

In this regard, there were many individuals who oppose the stipulation of minimum amount of cash as ETB 300,000. Due to highly prevalent usage of cash in the country there would be high probability that innocent business persons will have some inconvenience as a result of this threshold. However,

[69] FIC Compliance Directive, *supra* note 45, Art. 39.
[70] Proclamation No. 780/2013, *supra* note 29, Art. 20.
[71] Id, Art. 18 and FIC Compliance Directive, *supra* note 45, Art. 26(2).
[72] Ibid.
[73] FATF, *supra* note 24, Recommendation 19.
[74] FIC Compliance Directive 01/2014, *supra* note 45, Art. 26(2).

there is automatic software that detects transactions above ETB 300,000; and manual checking becomes necessary to only identify whether structured transactions are related or not.[75]

3. 7 Identification of beneficial ownership

A beneficial owner is someone who essentially owns the benefits or controls a customer and/or the natural person on whose behalf a transaction is concluded.[76] A person who exercises ultimate effective control over a legal person or arrangement also constitutes a beneficial owner.[77] In the context of money laundering, a beneficial owner is someone who controls or has an interest in illicit proceeds but conceals this fact through the misuse of corporate vehicles. Corporate vehicles refer primarily to companies, foundations, trusts, fictitious entities and unincorporated economic organizations.[78] Given the increased risks that accompany alternative money laundering techniques, the use of corporate vehicles has become the preferred method to launder ill-gotten gains. In the light of this, when the FATF revised its Recommendations in 2012, it expanded significantly the ambit of the requirements in relation to the establishment of the beneficial owner. But it is mandatory to exactly know who those beneficial owners are, and some jurisdictions use quantitative method (possession of certain percentage or share or voting rights in corporate vehicle) to qualify as the beneficial owner. For instance, the 4th European Union money laundering directive provides a guideline to identify beneficial owners in corporate vehicle as 25 + 1 % of the share.

Banks in Ethiopia are required only to identify and verify the identity of any person who acts on behalf of the customer. And they shall take appropriate measure to determine if a beneficial owner is a politically exposed person (PEP) and if so, they shall obtain approval from senior management before establishing business relationship with the customer. The challenge in this regard is that PEPs, as indicated earlier, are not made known for those responsible institutions. Therefore, it becomes difficult to apply this in the absence of appropriate mechanisms of enforcing such duty.

---

[75] All the selected banks have automatic software to identify the transaction made by each customer which reaches the threshold.

[76] General Glossary - International Standards on Combating Money Laundering the Financing of Terrorism and Proliferation: The FATF Recommendations (2012), p. 113.

[77] Proclamation No. 780/2013, *supra* note 24, Art. 2 (18).

[78] FATF, *The Misuse of Corporate Vehicles, Including Trust and Company Service Providers*, (2006), p. 1.

The minimum threshold that helps financial institutions to identify beneficial owners in case of corporate vehicles is not regulated in Ethiopia's anti-money laundering law. This gap will help launderers to use different companies to clean and wash out their dirty money using the company as a layer. Lessons can be drawn from the threshold used by European Union with some adjustments based on the pragmatic realities in Ethiopia so that the responsible organ can determine the minimum numbers of shares, and in effect, enable financial institutions to easily identify and verify the true beneficial owner.

3.8 Obligation to assess the risk of money laundering during the use of new technology

Technology makes life easy by performing huge tasks in the most efficient way, but it can also facilitate criminal acts in various sectors of the economy including the financial sector. Recent developments have witnessed the instrumental function of technology such as mobile phones in facilitating finance related services. Mobile banking can be defined as "financial services delivered via mobile network and performed on a mobile phone."[79] Following the development of the Internet, new forms of laundering (cyber laundering)[80] have emerged. It is thus the responsibility of financial institutions to made risk assessment of every new technology. To this end, the FIC Compliance Directive obliges financial institutions in general and banks in particular to make risk assessment on the use of new technology for money laundering and terrorism financing.[81] Criminals have been benefitting from the lacuna created in the regulatory regime.

FATF and its regional bodies require states to assess the risk and vulnerability of new technology. To this end, FATF and other regional initiatives require banks to conduct risk assessment on the vulnerability of the new technology for money laundering, terrorist financing or any other transnational organized crime.[82] Ethiopian law adopts this measure, as banks steadily develop more efficient banking technology. The FIC Customer Due Diligence Directive specifically regulates this issue and it obliges financial

[79] Lawack Vivienne (2013), 'Mobile Money, Financial Inclusion and Financial Integrity: The South African Case', *Washington Journal of Law, Technology & Arts,* vol. 8, p. 319.
[80] Cyber laundering is use of technology payment system for laundering criminal asset.
[81] FIC Compliance Directive, *supra* note 45, Art. 7.
[82] FATF, *supra* note 24, Recommendation 15.

institutions in general and banks in particular to make risk assessment while adopting and making use of new technology.

The data gathered during the research indicate the awareness of banks regarding the vulnerability of new technology and have taken preventive measures such as limiting the amount that a customer can transact within a day. Although there is no independent risk assessment that focuses on identifying the vulnerability of new technology for money laundering at the bank level, there is limit on the amount of the transaction that the customer can make (through ATM and internet banking) in 24 hours.[83] For some services, the system automatically notifies the bank that specified amount of money is transferred or payment is effected by the service user. But this procedure is not free from pitfalls as laundering techniques such as smurfing will benefit from the gaps. Smurfing is a placement technique in which a launderer makes multiple deposits into multiple accounts (often using various pseudonyms) or by using multiple individuals at a number of financial institutions to lower the amounts below the reporting threshold.[84]

The proper implementation of a certain law requires awareness. However, the interview held with FIC shows that training was provided only to compliance and risk management officers of banks.[85] In addition to these capacity building pursuits of the FIC, banks are responsible to give training to their employees on the importance of fighting money laundering and their respective responsibilities. According to the FIC Compliance Directive No. 1/2014, newly recruited bank employees are expected to take awareness creation training within one month from the commencement of employment.[86]

Compliance officers have an important role in fighting money laundering, and compliance officers of all banks covered under this research have received training by the FIC on the basic concepts of money laundering, techniques of laundering and the nefarious consequences of money

[83] In the selected banks, the amount that a customer can withdraw per day is not similar. It varies from 6,000 ETB to 10,000 ETB and transferring to other account is allowed up to 100,000 ETB. For internet banking (within 24 hours), the amount varies from 50,000 to 200,000 ETB. But the CBE allows the withdrawal from the ATM up to 10,000 within a day and internet banking up to 500,000. So, their vulnerability to abuse is not the same.

[84] FATF Glossary available at https://www.fatf-gafi.org/glossary/ last accessed on September, 2020.

[85] Interview with Ato Kidane Mariam G/tsadik, FIC Financial Transaction Inspection and Analysis officer on May 25, 2018.

[86] FIC Compliance Directive, *supra* note 45, Art. 42(4).

laundering on banks and the country at large.[87] Based on the information and materials prepared by FIC as a guide, compliance officers offer training on anti-money laundering programs to bank employees.

Conclusion

Money laundering obscures the true origin of an asset acquired through a criminal act and makes it reappear as legitimate and lawful. Owing to its adverse effects at domestic, regional and global levels, there are legal responses to combat it, which, inter alia, include the 1988 Vienna Convention, Palermo Convention, the FATF 40+9 recommendations, and various domestic laws. The preceding sections have examined Ethiopia's legal framework in this regard and have assessed the compliance practice in some selected banks. Banks are on the frontline in the combat against money laundering owing to their vulnerability as instruments in the efforts of money launderers to wash out dirty assets and make them clean. In this regard, Ethiopia has taken legislative measures and has entrusted some institutions with specific tasks to thwart money laundering that can potentially be committed through services provided by banks.

However, Ethiopia's anti-money laundering law has some inadequacies with regard to preventive measures such as (i) customer identification in case of politically exposed persons (PEPs), (ii) high risk jurisdiction customers, (iii) verification of the veracity of customer information in the absence which banks simply accept the information provided by the customer as true and valid without further verification, and (iv) lack of minimum threshold to identify beneficial owners. There is thus the need to enhance the capacity of regulatory organs that coordinate responsible institutions involved in the fight against money laundering and to supervise their activities. In this regard, the FIC faces challenges and gaps in clarity relating to STRs and owing to the level of understanding of the nature of the crime by the prosecution and the judiciary. Although the monitoring and reporting practices of banks with regard to STRs and CTRs is good, there is lack of preliminary investigation on STRs made by bankers, and this results in duplication of unnecessary reports.

The banks included in the research have awareness about the techniques and reprehensible consequences of money laundering. Yet, they have encountered problems in properly and meaningfully applying their

[87] Interview with Ato Kidane Mariam G/ tsadik, FIC Financial Transaction Inspection and Analysis officer on May 25, 2018.

responsibilities owing to gaps in the clarity of the law. Record keeping, has played the roles of prevention and control in the fight against money laundering because banks have good performance in keeping records in consonant with the terms of the law. The standards of performance with regard to *KYC* and *customer identification* are indeed commendable because banks take the necessary information from customers when they start business relations with them. However, updating and reviewing the information (even for high risk customers such as PEPs) needs improvement. Other concerns include gaps in the effective application of Enhanced CDD measures and lack of proper risk and vulnerability assessment of money laundering while developing and adopting new technology in the financial services of banks thereby creating the possibility of abuse by launderers. ■