ESJ Social Sciences

Development Financial Institution (DFI) Employees' Awareness and Perceptions of Anti-Money Laundering (AML) Practices and Cybersecurity Techniques

Thatayaone Mpuchane
University of Derby, Kedleston Road, Derby, United Kingdom
Tapiwa Gande
School of Business and Leisure,
Botswana Accountancy College, Gaborone, Botswana

Doi:10.19044/esj.2023.v19n10p1

Submitted: 04 April 2023
Accepted: 25 April 2023
Published: 30 April 2023

Cite As:
Mpuchane T. & Gande T. (2023). *Development Financial Institution (DFI) Employees' Awareness and Perceptions of Anti-Money Laundering (AML) Practices and Cybersecurity Techniques.* European Scientific Journal, ESJ, 19 (10), 1.
https://doi.org/10.19044/esj.2023.v19n10p1

Abstract

The purpose of this study was to assess employees' perceptions of anti-money laundering practices at the National Development Bank in Botswana. The study used a quantitative approach. A population of 84 respondents who are employees of a development financial institution (DFI), the National Development Bank (NDB) of Botswana was sampled in this study. Out of these, 36 respondents were selected through a stratified random sampling method to ensure representation in all strata. A self-administered questionnaire was used to collect data. The study found that employees of National Development Bank understand the concept of money laundering and the stages involved in money laundering. Secondly, the study established that the main causes of money laundering were corruption, politicians and prominent person's influence, and weak banking and financial systems. Thirdly, the study established that money laundering is harmful to the economy in different ways that include increased national crime, increased corruption, and negative effects on the economy. The study recommended that the management of NDB should adopt anti-money laundering/ combating/ counter-terrorism financing (AML/CFT) regulations laid out by regulating bodies including those of the Financial Action Task Force (FATF), Bank of Botswana and the

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

Financial Intelligence Agency (FIA). In addition to this, the bank management should expose its employee to continuous knowledge of ML/FT through in-house training and external workshops with other industry stakeholders. The bank should also adopt a robust record management system that is able to capture all transactions taking place within it. The system should be robust enough to flag suspicious ML/FT activities taking place through transactions carried out within the bank.

Keywords: Anti-money laundering, counter-terrorism financing, financing of terrorism, money laundering, cyber security

Introduction

Money laundering (ML) is the concealing or disguising of proceeds of crime in mainstream financial systems. Anti-money laundering (AML) practices refer to policies geared towards combating proceeds ML (FATF, 2021). Closely related to ML and AML is cyber security which is the practice of securing computer programs and systems from intrusion by ransom wares or opportunistic malware (Zarreh et al., 2019; Aitel, 2013). Cyber security is associated with ML because unsafe cyberspace is a catalyst for ML activities (O'Neill, 2014). It is until the 9/11 USA attacks, that combating ML activities were taken seriously after its association with financing terrorism. Anti-money laundering and counter-financing of terrorism (AML/CFT) agencies were established, and governments globally took over the fight against ML (Levi, 2010; Levi & Gilmore, 2002).

Botswana has not been spared of ML acts. Most recently, embezzlement of BWP326 million, belonging to the National Petroleum Fund (NPF) reserved for inflationary petroleum prices cushion was allegedly laundered by senior government officials (Motshegwa et al, 2019). Topical cases such as this motivated this study to assess the perceptions of employees of the National Development Bank of Botswana (NDB) on the effectiveness of AML practices used by the bank to address the problem of ML.

The NDB was set up through an Act of Parliament of Botswana in 1963. The Bank is owned by the Government of Botswana. NDB is a non-commercial bank offering investment financing services to citizens. NDB's main objective is provision of a varied range of financial services to Botswana's business sector and the public at large. As a Development Financial Institution (DFI), NDB is viable and self-sustaining and continues to contribute immensely to the growth of the local economy.To achieve this, the study addressed the following specific objectives.

- To examine the concept, stages, and techniques of ML.
- To determine the major causes of ML practices.
- To investigate the impact of ML practices on the economy.

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

- To determine the link between ML and cyber security.
- To examine the perception of NDB employees regarding AML practices used by the bank to curb ML.

The research sought to educate stakeholders of development financial institutions, particularly in the third world, such as the National Development Bank of Botswana, the Bank of Botswana, other financial sector entities, scholars, and academic institutions about ML activities. Secondly, this study sought to identify and address gaps in the literature thus contributing to the corpus of knowledge on ML and cyber security.

Literature review

This study is informed by the *Theory of Crying Wolf* by Takats (2011). This theory is an analogy of a shepherd boy who used to cry that he has been attacked by a wolf while tending his father's sheep. Every time he would cry out loud, villagers would run to him armed to rescue him and find no wolf. One day when he cried wolf, the real wolf had attacked him, and neighbours were tired of his false alarms and never came to his rescue. Sadly, the wolf killed him together with part of the flock (Gara & Pauselli, 2015).

Application of the above theory to ML is explained by Rizzolli & Saraceno (2013) who assert that banks are essentially supposed to report every suspicious transaction. But it turns out that in so doing, they may make many false positive mistakes which government agencies dealing with ML will keep excusing and not acting. On a different occasion, banks may report real ML cases but because of the constant false positives, government agencies may not take those cases seriously and that will give a loophole for a laundered transaction to go through. Alternatively, since banks incur huge costs in scrutinising each transaction, they may also relax, and just like the boy who cried wolf when the real wolf appeared, they will authorise a laundered transaction and commit a false negative mistake and be penalised for it.

Stages of ML activities

ML is made up of three key stages (Teichmann 2017). These are placement, layering and integration. Placement, the initial stage is where the proceeds of ML are channelled into the financial system. Since these proceeds are usually huge, criminals break them down into smaller amounts which are deposited into bank accounts in bits or used in purchasing financial instruments to obfuscate investigators.

The second stage of ML is layering, (Oke 2016) describes this stage as the most complex as it involves concealing the proceeds of ML further to make them impossible to detect. This may involve the purchase of legit property or investment in genuine businesses. The third stage is integration in which the

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

illegitimate money is introduced back into the financial system in a manner to appear it is coming from genuine sources (Oke, 2016).

Causes of ML

Tax evasion takes the form of not paying or declaring incorrect taxes by manipulating the figures indicating the correct incomes entities derive from different investments (Cassara, 2015; Osakede, 2015). Makochekwane (2014) opines that tax evaders can also covertly reassign their income generating investments to individuals who usually have no capacity to execute business transactions hence shifting these activities from actual owners of those investments, as mostly committed by politicians.

Bribery and corruption are other major causes of money laundering. According to Osakede (2015) corruption and bribery as a cause of ML is perpetrated mostly by political elites. Corruption accounts for a significant portion of national ML activities. For instance, Lannegren & Ito (2017) observed that between ZAR 25-30 billion is lost very year by the Republic of South Africa in the hands of high-ranking officials.

Since banks and other financial institutions deal with large transactions every day, some banks do not carry out due diligence or have weak detection systems to detect proceeds of ML (Sotelino & Finel-Honigman, 2015). Sotelino & Finel-Honigman (2015) observe that the Hong Kong and Shanghai Banking Corporation (HSBC) Ltd was in 2010 fined close to USD 2 billion by international AML agencies for failure to restrain and account for money laundered through its branches.

National borders are also a major cause of ML. Mozambique is an African country blacklisted by FATF for ML particularly because of its porous borders. In Mozambique, economic crimes such as high echelon corruption and ML from illicit deals are the order of the day (Kavanagh, 2013).

The United Nations Conference on Trade and Development (UNCTAD) (2020) notes that Africa loses USD 89 billion annually due to illicit money exchange in borders of some countries carried out by individuals not duly registered to act as financial institutions. UNCTAD (2020) observes that it is common practice to find young men at borders of African countries converting currencies for arriving and departing visitors. Such practices are common in Kenya, Tanzania, Uganda, Zambia, Zimbabwe, Mozambique, Malawi, just to name but a few, and catalyse or exacerbate ML activities.

Impact of ML on the economy

Stancu & Rece (2009) observe launderers may take more time 'hoarding' the illicit money or invest it in the underground economy that is not productive to the legitimate economy. However, Henry & Moses (2020) argue

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

that if laundering takes place within the financial system, then it has no effect on economic activities and the economy will run as usual.

Hetemi, Merovci & Gulhan (2018) allude that ML is positively associated with social problems such as increase in crime. Predicate crimes such as drug and human trafficking, prostitution, extortion, and terrorism potentially generate illicit money, motivating money launderers to engage in them.

Root (2019) showcases two positive effects of ML. Firstly, when laundered money comes into a country, it has a potential to significantly impact the consumption levels. The multiplier effect of this accelerates production resulting in positive economic growth. Secondly, higher levels of corruption in a country also accelerates economic growth since corruption has a greasing effect, describe by Gorsiga, Steg, Denkers & Huisman (2018) as the *quid pro quo* effect.

ML and cyber security

Cyber security and Anti-Money Laundering (AML) systems are closely associated since both are attempts to safeguard electronic devices, networks, and data (Anichebe, 2020). The accuracy and efficiency of AML systems depend on the data's integrity and the security of the systems used to store and process it. Dixon (2017) demonstrates how cybersecurity can be compromised in different organisations including security agencies, financial institutions, private and government websites among other through cyber-attacks. For instance, through cyber-attacks, cybercriminals can transfer money using crypto currency such as bit coin across blockchains which are meant to identify and freeze such malicious transactions.

Financial institutions must conduct a thorough risk analysis, implement appropriate controls and safeguards, take part in data exchange programs, have an incident reaction strategy in place, and continuously evaluate and improve their cyber security program to address new and emerging threats if they want to ensure the effective integration of cyber security into AML programs (Arner et al., 2019; Arner & Janosa, 2015). Other innovative approaches have involved using Artificial Intelligence (AI) based fraud detection systems to provide ongoing screening on fraud, internet banking security as well as AML (Maruatona, 2013). A further discussion is provided by Maruatona, Vamplew, Dazeley & Watters (2017) on why this approach is relevant for Fraud Detection and AML specifically and why conventional systems may not be sufficient for modern, sophisticated cyber-attacks, online fraud and money laundering.

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

Strategies to combat ML

Typically, the current and most common strategy for combating money laundering is the FATF's AML/CFT approach (Sotelino & Finel-Honigman, 2015). Henry & Moses (2020) describe it as an approach designed by the supra-national AML body with standards on how to identify activities of ML. Financial institutions are tasked to assist their national FATF agents to identify money laundering through a tripod model of placement, layering and integration. In addition, any model that can successfully combat ML must focus on all possibilities whereby the financial system can be used to commit crime.

Methodology

Paradigm

This study confined itself to the objective ontological perspective (Saunders et al., 2009). Wahyuni (2012) describes ontology as the belief that truth exists independent of the researcher, while epistemology is the belief that truth about a phenomenon is subjective and can therefore be socially constructed by the researcher. This choice was informed by the fact that money laundering is a phenomenon that exists and has been defined within well-known boundaries of what constitutes and what does not constitute money laundering. In carrying out a study on perceptions of bank employees on anti-money laundering practices, the researchers felt it important to be objective in establishing and reporting the perceptions of employees without distorting them through giving these perceptions their own socially constructed perspective of those employees' perceptions.

Design

This study used the explanatory design (Rahi, 2017). This is preferred as the researcher collects quantitative data and analyses it using statistical techniques and use the results to explain the perceptions of bank employees regarding anti-money laundering practices in their organisation.

Approach

This study utilised the quantitative methods as the researchers collected quantitative data and analysed it using statistical software. According to Crowe & Sheppard (2010) quantitative method is where the researcher collects quantitative data and uses statistical software to analyse the data, the objective of this method is to utilise mathematical models, theories, and hypotheses to draw inferences from results generated from the data.

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

Population, sample, and sampling

The population of this study was all the employees of the National Development Bank, Gaborone Branch in Botswana. This population is 84 staff members **(**National Development Bank, 2020). This study used a probabilistic stratified random sampling method (Rahi, 2017). The researchers demarcated the population into categories using demographic characteristics such as gender, age groups, education level, employment levels, and years of work experience. A total of 36 respondents were selected for inclusion in the study using the method.

The details of the sample demographics are outlined below. The demographic data shows the characteristics of the respondents to indicated how selection of respondents was done and to enhance representation and validity (Saunders et al 2009). **Table 1** below presents the demographics. These cover the gender, age group, highest level of education, employee type and years of experience of the sample of NDB staff in the sample of respondents.

Table 1. Demographic characteristics of respondents

Characteristic	**Categories**	**Count (n)**	**Percentage (%)**
Gender	Male	23	63.9
	Female	13	36.1
	Total	**36**	**100,0**
Age group	21-30	9	25.0
	31-40	20	55.6
	41-50	6	16.7
	50+	1	2.8
	Total	**36**	**100.0**
Highest level of education	Diploma	11	30.6
	Degree	16	44.4
	Masters	8	22.2
	Other	1	2.8
	Total	**36**	**100.0**
Employee type	Junior employees	22	61.1
	Middle management	11	30.6
	Senior management	3	8.3
	Total	**36**	**100.0**
Years of work experience	0-5	4	11.1
	6-10	15	41.7
	10+	17	47.2
	Total	**36**	**100.0**

Instrumentation

Data for this study was collected using a questionnaire. The questionnaire was designed in five sections. The first section investigated demographic characteristics of respondents to show they type of respondents who will take part in the study. The second part of the questionnaire

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

investigated respondents' knowledge on money laundering. The third section investigated the cause of money laundering. The fourth part investigated the impact of money laundering. The last section investigated the perceptions of respondents towards anti-money laundering practices available in their organisation.

Data analysis

Data was analysed for descriptive and inferential statistical analysis. Under descriptive analysis, means and standard deviations were calculated to show the general responses of respondents to questionnaire items. Under inferential statistics analysis of variances (ANOVA) was done to test difference in means of perceptions between various groups of respondents based on their demographic characteristics.

Validity and reliability of instrument

To ensure that the instrument is valid, a pilot study was conducted by the researchers using a random sample of a few selected respondents. Items that were vague were corrected and those that were irrelevant to the study were discarded or replaced by relevant ones.

Reliability is often calculated by SPSS using the Cronbach alpha value. Cronbach values range from 0 to 1 (Gliem and Gliem 2003). The study generated overall reliability alpha of 0.883 (refer **Table 2** below).

Ethical concerns

Firstly, the researchers sought permission from the National Development Bank (NDB) management as well as the research department of the university at which the researchers are based, to carry out the study.

Secondly, the researchers made the purpose of the research clear in an introductory statement of the questionnaire and required respondents to sign an informed consent form before participating.

Thirdly, privacy and anonymity of the respondents was assured as not data to identify respondents was collected nor included in the analysis.

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

DATA ANALYSIS

Reliability analysis

Table 2. Instrument's reliability

Objective category	**Item count (n)**	**Alpha**
Awareness of ML/FT issues	4	.859
Techniques of ML/FT	5	.745
Cause of ML/FT	5	.699
Impact of ML/FT	6	.808
Respondents' perception on effectiveness of AML/CFT practices	9	.768
Overall, Alpha	**30**	**.883**

As indicated in **Table 2**, awareness of ML/FT was investigated using 4 items and had an alpha of .859; techniques used in ML/FT was investigated using 5 items and had an alpha of .745; cause of ML/FT was investigated using 5 items and had an alpha of .699; impact of ML/FT was investigated using 4 items and had an alpha of .808; and respondents' perceptions on the effectiveness of AML/CFT practices was investigated using 4 items and had an alpha of .768. The overall alpha for the 30 items of the instrument was .883.

Descriptive analysis

Table 3. Descriptive analysis

Item	**Mean**	**SD**
I am aware of "Money Laundering"	4.50	.655
I am aware of "Financing of Terrorism" (i.e., supply of funds for activities of terrorism)	4.36	.723
I am aware of FIA and its role (i.e., the Financial Intelligence Agency)	3.92	.906
I am aware of the concept 'Know Your Customer' (KYC)	4.61	.494
Money laundering is the concealment of sources of 'dirty' money	4.64	.487
Launderers place, layer and then integrate 'dirty' money to the system	4.47	.609
Launderers follow the steps of money laundering systematically	3.69	.951
Money laundering aids in financing terrorist activities	4.33	.862
Stages of money laundering are very evident	3.22	1.174
Launderers use the same techniques repeatedly	2.94	1.308
Money laundering results from corrupt practices of individuals	4.22	.797
Weak banking and financial systems result in money laundering	4.31	.749
Weak judicial and legal systems result in money laundering	3.97	.878
Banks are conduits for money laundering activities	3.94	.924
Politicians are major perpetrators of money laundering	3.53	.878
Money laundering negatively affects the operation of the economy	4.36	.798
Money laundering increases likelihood of terrorist activities	4.50	.697
Money laundering increases corruption and bribery	4.56	.695

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

Money laundering leads to increased national crime	4.28	.741
Money laundering leads to thriving of the black market	4.53	.654
Proceeds of money laundering do not benefit the economy	4.14	1.046
Banks should put in place KYC regulations that require customers to provide adequate identity information about themselves	4.64	.487
Where customers breach KYC regulations their accounts should be frozen by the bank	4.36	.762
Banks should not suspend the customer transactions, such as withdrawal of money, transfer of money, etc., in case the customer fails to submit updated KYC documents after repeated requests	3.78	1.174
Banks should establish the natural persons (company shareholders) even for complex company structures	4.08	.841
Customer due diligence (i.e., collection of relevant information about the client and evaluating for potential risks) on all bank clients before acceptance is important	4.39	.803
Prominent influential persons (PIPs) (previously known as PEPs) should be classified as high risk for AML /CFT	3.92	.967
Reporting suspicious financial activities to regulators is tedious and time wasting	4.08	.967
Banks should report suspicious transactions to regulators	4.53	.506
Where customers engage in suspicious financial activities their accounts should be frozen and closed	4.28	.849

Regarding the concept, stages and techniques of ML, there was a strong general agreement amongst respondents that money laundering negatively affects the operation of the economy (Mean=4.64); launderers place, layer and then integrate 'dirty' money to the system (Mean=4.47); and money laundering aids in financing terrorist activities (Mean=4.33). There was a mild agreement amongst respondents that launderers follow the steps of money laundering systematically (Mean=3.69). There was indecisiveness amongst respondents on stages of money laundering being evident (Mean=3.22) and launderers use the same techniques repeatedly (Mean=2.94). On the causes of ML, there was a strong general agreement amongst respondents that weak banking and financial systems result in money laundering money (Mean=4.31); laundering results from corrupt practices of individuals (Mean=4.22); weak judicial and legal systems result in money laundering (Mean=3.97); and banks are conduits for money laundering activities (Mean=3.94). There was a mild general agreement that politicians are major perpetrators of money laundering (Mean=3.53).

Regarding the impact of ML there was a strong general agreement amongst respondents that money laundering negatively affects the operation of the economy (Mean=4.36); money laundering increases likelihood of terrorist activities (Mean=4.50); money laundering increases corruption and bribery (Mean=4.56); money laundering leads to increased national crime (Mean=4.28); money laundering leads to thriving of the black market

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

(Mean=4.53); and proceeds of money laundering do not benefit the economy (Mean=4.14).

Lastly, on the perceptions of respondents regarding the efficacy of AML/CFT practices there was a strong general agreement amongst respondents that banks should put in place KYC regulations that require customers to provide adequate identity information about themselves (Mean=4.64); where customers breach KYC regulations their accounts should be frozen by the bank (Mean=4.36); banks should not suspend the customer transactions, such as withdrawal of money, transfer of money (Mean=3.78); banks should establish the natural persons (company shareholders) even for complex company structures (Mean=4.08); banks to conduct customer due diligence on all bank clients before acceptance is important (4.39); prominent influential persons (PIPs) should be classified as high risk for AML /CFT (3.92); reporting suspicious financial activities to regulators is tedious and time wasting (Mean=4.08); banks should report suspicious transactions to regulators (Mean=4.53); and where customers engage in suspicious financial activities their accounts should be frozen and closed (Mean=4.28).

Inferential analysis
Correlations

Table 4. Correlation matrix

		Awareness	Techniques	Causes	Impact	Perception
Awareness	Pearson Correlation	1	.224	.000	.629**	.224
Techniques	Pearson Correlation		1	.065	.124	.398*
Causes	Pearson Correlation			1	.274	-.008
Impact	Pearson Correlation				1	.271
Perceptions	Pearson Correlation					1

******. Correlation is significant at the 0.01 level (2-tailed).
*****. Correlation is significant at the 0.05 level (2-tailed).

From the table, awareness of AML/CFT issues was positively and significantly correlated with the knowledge on impact of ML/FT (r=.629, ρ=.000) at .01 level of significance. Knowledge of the techniques used in ML/FT was also positively and significantly correlated with perceptions of employees regarding the efficacy of AML/CFT practices (r=.398, ρ=.016) at .05 level of significance.

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

Conclusion

The study concluded that employees of NDB were aware of ML and the three stages of ML. Secondly, ML was attributed to three main causes namely corrupt practices of individuals (corruption), the influence of politicians, and weak banking and financial systems. Thirdly, the impact of ML three-fold. ML leads to increased national crimes, ML negatively affects operations of the economy, and ML increases corruption and bribery. Fourthly, in terms of strategies to counter ML and FT, PIPs should be classified as high risk for AML/CFT; customers who engage in suspicious accounts should have their accounts frozen; banks should do customer due diligence; and banks should establish natural persons behind companies that the banks deal with. The NDB has put in place a cybersecurity security system to counter cyber-attacks that could lead to money laundering attempts. These include network security products, data loss prevention tools, e-crime intelligence tools and machine learning tools to learn and detect e-crime attempts.

In many contexts, including the case of NDB particularly, ML is a legally based issue, therefore the legal framework of the countries have a high correlation with the ML or AML. In the case of BND, this was covered by Botswana's enabling laws, regulations and acts of parliament, including supporting contextual national institutions, such as the FIA of Botswana, which enhance legal shortfalls and lack of regulation in developing and underdeveloped countries. However, the evaluation of the adequacy of these laws and regulations was beyond the scope of this study.

This aspect however is mitigated, in the Botswana context, with membership to, regional, global and supranational bodies such as, the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG 2021), a regional body subscribing to global standards to combat money laundering and financing of terrorism and proliferation and the Financial Action Task Force (FATF). The FATF is a global money laundering and terrorist financing watchdog which sets international standards aimed at preventing these illegal activities and the harm they cause to society.

Recommendations for policy

- The management of development financial institutions (DFI's) should adopt AML/CFT regulations and recommendations laid out by regulating bodies including those of, ESAAMLG, FATF, Bank of Botswana and the Financial Intelligence Agency (FIA). These regulations criminalize acts of ML/FT and their adoption will therefore provide a framework through which the bank identifies and deals with criminal acts of ML/FT.
- In addition to this, development financial institutions' management

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

should expose employees to continuous knowledge on ML/FT through in-house training and external workshops with other industry stakeholders.

- DFI's should adopt a robust record management system that is able to capture all transactions taking place within them. The system should be robust enough to flag suspicious ML/FT activities taking place through transactions conducted within the development financial institution (DFI).

Recommendations for future studies

- Future studies should focus on the comparative progress made by developing countries such as Botswana vis-a-vis other (developed) countries in combating AML/CFT issues. These studies will be robust enough to depict changes that have taken place in the money laundering arena especially due to increased access and use of sophisticated technology and how cyber security contributes to detecting and combating these ill practices.
- Additionally, future research could provide either a qualitative or mixed philosophy approach to allow for more in-depth perceptions to be solicited from participants through methods such as focus group interviews.

References:

1. Aitel, D. (2013). Cybersecurity essentials for electric operators. *The Electricity Journal*, 26(1), 52-58.
2. Anichebe, U. (2020). Combating money laundering in the age of technology and innovation. *Social Science Research Network,* 12, 1-35.
3. Arner, D. W. & Janosa, B. (2015). Fintech in China from the shadow. *Journal of Financial Perspectives*, 3, 78-91.
4. Arner, D. W., Dirk, A. Z., Ross, B. & Janos, B. (2019). The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities. *European Business Organisation Law Review,* 20, 55-80.
5. Cassara, J. A. (2015). *Trade-based money laundering: the next frontier in international money laundering enforcement*. New York: Wiley.
6. Crowe, M. & Sheppard, L. (2010). Qualitative and quantitative research designs are more similar than different. *Internet Journal of Allied Health Services and Practice,* 4 (8), 1-6.
7. Dixon, H., (2017). Maintaining Individual Liability in AML and Cybersecurity at New York's Financial Institutions. *Penn State Journal of Law and International Affairs*, 5(1), 1-40.

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

8. Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) (2021) Anti-money laundering and counter-terrorist financing measures Mutual Evaluation Report Mozambique. Available at: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Mutualevaluations/Mer-mozambique-2021.html
9. Financial Action Task Force (FATF) (2021) Annual Report 2020-2021. Available at: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfgeneral/Annual-report-2020-2021.html
10. Gara, M., & Pauselli, C. (2015). Looking at 'Crying wolf' from a different perspective: An attempt at detecting banks under- and over-reporting suspicious transactions. *Banca d'Italia - Quaderni Dell'antiriciclaggio*, 4, 1–26.
11. Gliem, J.A. and Gliem, R.R. (2003). Calculating, Interpreting, and Reporting Cronbach's Alpha Reliability Coefficient for Likert-Type Scales. 2003 Midwest Research to Practice Conference in Adult, Continuing, and Community Education, pp.1-7
12. Gorsiga, M., Steg, L., Denkers, A. & Huisman, W. (2018). Corruption in organizations: ethical climate and individual motives. *Administrative Sciences*, 8(4), 1-19.
13. Henry, L. & Moses, S. (2020). *An analysis of money laundering and Economic growth in Trinidad and Tobago*. San Fernando: UWI Press.
14. Hetemi, A., Merovci, S. & Gulhan, O. (2018). Consequences of money laundering on economic growth. The case of Kosovo and its trade partners. *Acta Universitatis Danubius OEconomica*, 14(3), 113-125.
15. Kavanagh, C. (2013). Getting smart shaping up: Responding to the impact of drug trafficking in developing countries. A case study of Mozambique. Washington, DC: NYU Center on International Cooperation.
16. Lannegren, O. and Ito, H. (2017). The End of the ANC Era: An analysis of corruption and inequality in South Africa. *Journal of Politics and Law*, 10(4), 55-59.
17. Levi, M. & Gilmore, B. (2002). Terrorist finance, money laundering and the rise and rise of mutual evaluation: A new paradigm for crime control? *European Journal of Law Reform*, 4(2), 337-364.
18. Levi, M. (2010). Corruption and *money laundering*. *Journal of Financial Crime*, 17(1), 168-169.
19. Makochekwane, A. (2014). Is corruption really harmful to growth? Evidence from Zimbabwean. *University of Zimbabwe Business Review*, 2 (2), 1-17.
20. Maruatona, O. (2013). Internet Banking Fraud Detection Using Prudent Analysis. *Federation University*

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

21. Maruatona, O., Vamplew, P., Dazeley, R., Watters, P. (2017). Evaluating accuracy in prudence analysis for cyber security. *ICONIP 2017*.
22. Teichmann, F.M.J. (2017). Twelve methods of money laundering. *Journal of Money Laundering Control*, 20(2), 130-137.
23. Motshegwa, B., Mutonono, P. & Mikhazu, T. (2019). Embezzlement of the National Petroleum Fund in Botswana. A paper presented at the 4th Annual International Conference on Public Administration and Development Alternatives 03-05 July 2019, Southern Sun Hotel, OR Tambo International Airport, Johannesburg, South Africa.
24. National Development Bank (NDB) (2020). Annual Prospectus. Gaborone: NDB.
25. O'Neill, M. (2014). The Internet of Things: do more devices mean more risks? *Computer Fraud & Security*, 14(1), 16-17.
26. Oke, T. (2016). Money laundering regulation and the African PEP: case for tougher civil remedy options. *Journal of Money Laundering Control*, 19(1), 32-57.
27. Osakede, K. (2015). Corruption in the Nigeria public sector: an impediment to good governance and sustainable development. *Review of Public Administration and Management*, 4 (8), 76-87.
28. Rahi, S. (2017). Research design and methods: A systematic review of research paradigms, sampling issues and instruments development. *International Journal of Economic Management Science,* 6(2), 1-5.
29. Rizzolli, M., & Saraceno, M. (2013). Better that ten guilty persons escape: Punishment costs explain the standard of evidence. *Public Choice*, 155(3), 395–411.
30. Root, V. (2019). The compliance process. *Indiana Law Journal*, 94 (1), 203-251.
31. Saunders, M., Lewis, P. & Thornhill, A. (2009). *Research methods for business students*. (5th Ed). Essex, England: Pearson Education Limited.
32. Sotelino, F. & Finel-Honigman, I. (2015). *International Banking for a New Century*. Paris: Routledge. ISBN 9780415681339
33. Stancu, I. & Rece, D. (2009). The relationship between economic growth and money laundering – a linear regression model. Asociatia Generala a Economistilor din Romania, 9(538), 3-8.
34. Takats, E. (2011). A theory of "Crying Wolf." The economics of money laundering enforcement. *Journal of Law, Economics and Organization*, 27(1), 32-78.
35. United Nations Conference on Trade and Development (UNCTAD, 2020). Africa could gain $89 billion annually by curbing illicit financial flows. Available online at: https://unctad.org/news/africa-

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

could-gain-89-billion-annually-curbing-illicit-financial-flows (Accessed June 29, 2021).

36. Wahyuni, S. (2012). *Designing qualitative research*. London: SAGE Publication Ltd.
37. Zarreh, A., Wan, H. D., Lee, Y., Saygin, C. & Al Jahani, R. (2019). Cybersecurity concerns for total productive maintenance in smart manufacturing systems. *Procedia Manufacturing*, 38, 532-539.