A COMPARISON BETWEEN INTERNET ANTI-MONEY LAUNDERING STATUTES AND PREVENTATIVE MECHANISMS IN SOUTH AFRICA

By

2506906

Submitted in partial fulfilment of the requirements for the degree of
Master of Laws by Coursework and Research Report
at the University of the Witwatersrand, Johannesburg

Date: 1 October 2022

DECLARATION

I, _____, declare that this Research Report is my own unaided work. It is submitted in partial fulfillment of the requirements for the degree of Master of Laws (by coursework and Research Report) at the University of the Witwatersrand, Johannesburg. It has not been submitted before any degree or examination in this or any other university.

I have submitted my final Research Report through Turnitin and have attached the report to my submission.

_____

SIGNATURE

2506906

_____

STUDENT NUMBER

1 October 2022

_____

DATE

ABSTRACT

South Africa has come a long way since the apartheid era, transitioning to a country of democracy for its people and advocating for non-violence. However, struggles persist in inequality, poverty, unemployment and crime. Due to the social, economic, and political challenges and allegations of continuous corruption the country is often perceived negatively. Despite a growing body of laws, regulations, and systems geared to fight crime, the crime rate remains high and prosecution low. As a result, South Africa has become a soft target for criminals who conceal the proceeds of crimes through money laundering.

Through money laundering, criminals have exploited the banking and financial sector, the casino and gambling industry and the real estate business in South Africa. As a consequence of the onset of money laundering, the South African government has had to enact legislation and regulatory bodies in each sector to detect, prevent and prosecute organised crime. The latest challenge to combating money laundering is the advent of the internet which has created newer, faster and more evasive channels for criminals to launder money via cyberspace.

Given that the internet and technology are ever-changing, historic anti-money laundering laws and mechanisms may not be effective enough to combat the crime of 'cyberlaundering'. This thesis discusses pre- and post-internet methods of money laundering in the banking, casino and gambling and real estate sectors in the South African economy and focuses on whether current legislation and mechanisms are effective enough to combat developments in money laundering.

LIST OF ABBREVIATIONS

AI	Accountable Institution
AML	Anti-Money Laundering
AUSTRAC	Australian Transactions Reports Centre
BSA	Bank Secrecy Act
CDD	Customer Due Diligence
CPA	Consumer Protection Act
CTRs	Currency Transaction Report
EAAB	Estate Agency Affairs Board
ECTA	Electronic Communications and Transactions Act
EU	European Union
FATF	Financial Action Task Force
FIC	Financial Intelligence Centre
FICA	Financial Intelligence Centre Act
FIC Amendment Act	Financial Intelligence Centre Amendment Act
FIs	Financial Institutions
FinCEN	Financial Crimes Enforcement Network
ISPs	Internet Service Providers
KYC	Know Your Customer
ML	Money Laundering
MLCA	Money Laundering Control Act
NGB	National Gambling Board
NPA	National Prosecuting Authority
PCA	Proceeds of Crime Act
POCA	Prevention of Organised Crime Act
RICA	Regulation of Interception of Communications and Provision of Communication-related Information Act
SA	South Africa/South African
SAPS	South African Police Service
STRs	Suspicious Transaction Report
SWIFT	Society for Worldwide Interbank Financial Telecommunications S.C
USA	United States of America

TABLE OF CONTENTS

CHAPTER I
INTRODUCTION

I BRIEF HISTORY OF MONEY LAUNDERING

Money Laundering ('ML') is an age-old crime dating back to the 1900s in the United States of America ('USA') where money derived from illegal activities such as gambling, narcotics and liquor were concealed as legitimate funds in the financial market.[1] Allegedly one of the very first acts of ML was committed by mafia boss Al Capone who illegally brewed, distilled and distributed liquor and disguised the proceeds thereof through many front companies during the prohibition era.[2]

In order to detect and prevent ML activities in the USA, the Bank Secrecy Act, 1970 ('BSA') was enacted. Under that Act all financial institutions had to file a Currency Transaction Report ('CTRs') on transactions over $10 000.[3] The purpose was to urge financial institutions to keep records and report on transactions over $10 000 thus enabling officials to conduct investigations to identity suspicious transactions evading tax obligations or involved in criminal activity.[4] However this statutory obligation did not deter money launderers from passing transactions in smaller amounts under $10 000 through financial institutions to escape the reporting procedure and utilising other avenues to pass transactions such as cash smuggling across borders, currency exchanges and investments.[5]

Such weaknesses led to the enactment of the Money Laundering Control Act, 1986 ('MLCA') with the aim of imposing civil and criminal penalties on any person who actively engaged in

[1] Madelyn J. Daley 'Effectiveness of United States and International Efforts to Combat International Money Laundering' (2000) 2000 *Saint Louis-Warsaw Transatlantic Law Journal* 176.

[2] KYC-Chain 'The History of Money Laundering' 25 April 2019, available at *https://kyc-chain.com/the-history-of-money-laundering/*, accessed on 4 January 2022.

[3] Stephen Jeffery Weaver 'Modern Day Money Laundering: Does the Solution Exist in an Expansive System of Monitoring and Record Keeping Regulations?' (2005) 24 *Annual Review of Banking & Financial Law* 446- 47.

[4] Daley op cit note 1 189.

[5] Ibid.

the acts of ML whether it be initiating the transaction, receiving the proceeds or systematising how the proceeds are placed in the economy.[6]

Apart from implementing and enforcing domestic laws, the USA government saw a greater need for international co-operation to fight ML and terrorist activities after the al-Qaeda terrorist attacks on the USA in 2001. This led to the enactment of the USA-Patriot Act, 2001 which seeks to empower USA officials to enforce co-operation on foreign jurisdictions of any ML investigations conducted by the USA.[7] These legislative enactments are still relevant today and have shaped the way in which many jurisdictions respond to ML activities within its own borders. Legislation is of paramount importance to prosecute the offence of ML, however understanding the methods adopted by money launderers to hide the proceeds of illegal activity is consequential to developing AML legislation.

II BACKGROUND AND CONTEXT

The act of ML may look like a Hollywood movie scene where a drug mafia hides thousands of dollars in an apartment building and transports differing amounts in suitcases to multiple people. This may be a true depiction of how ML started, however the methods of ML have become more sophisticated overtime to avoid detection by authorities. This led to countries actively enforcing measures and laws to combat ML on a national and international scale. South Africa ('SA') is deficient in the collecting of statistics on the amount of money laundered every year. Therefore, there is no clear record of the investigations, prosecutions and convictions of all acts associated with ML.[8] This may well be the result of the discrete nature of the crime, the extreme measures criminals adopt to conceal the proceeds of illicit activities,[9] weak law enforcement agencies to detect and combat the crime[10] and the high corruption rate within the

[6] Ibid 190.

[7] Weaver op cit note 3 447.

[8] FATF Mutual Evaluation Report: Anti-money laundering and counter-terrorist financing measures: South Africa (2021) 218.

[9] Humphrey P B Moshi 'Fighting money laundering: The challenges in Africa' (2007) *Institute for Security Studies* 2.

[10] Ibid.

country.[11] In a 2020 report it was estimated that an amount between $10 billion and $25 billion is lost every year as a result of illicit activities in SA.[12] This is a growing concern for vulnerable sectors such as banking and financial institutions,[13] real estate[14] and casino and gambling sectors,[15] which comprise the largest sectors in the SA economy[16] and have been rated medium to high-risk vehicles of ML.[17] In spite of these risks, these sectors have succumbed to the convenience of the internet to increase footprint and capital, subjecting their operations to cyberlaundering.

III RESEARCH PROBLEM

ML has a destabilising effect on the economy and places power in the hands of criminals to corrode social, financial and policy systems. When this happens citizens of the country become doubtful of ruling parties, the laws, enforcement agencies and financial and social establishments which strengthen the economy of a country.[18] This research is based on the negative effects of ML and the seemingly unanswered question of 'how much money is actually laundered in SA every year both online and offline?' SA has sought to combat ML since 1990,[19] which evidences that SA has been exposed to ML activities for over three decades. Despite statutory developments to combat conventional ML methods since the late

[11] Sagwadi Mabunda 'Cyberlaundering and the Future of Corruption in Africa' (2018) 2(2) *Journal of Anti-Corruption Law* 214.

[12] BusinessTech 'How to reduce money laundering in 2020' 23 January 2020, available at *https://businesstech.co.za/news/industry-news/367824/how-to-reduce-money-laundering-in-2020/*, accessed on 12 January 2022.

[13] FATF op cit note 8 para 114.

[14] Ibid para 113.

[15] FIC Report released on risks of money laundering facing the gambling sector (2022) 1.

[16] International Monetary Fund (IMF) Country Report No. 21/227 Detailed Assessment Report on Anti-Money Laundering and Combating the Financing of Terrorism (2021) para 69 and 99.

[17] Ibid 28.

[18] Moshi op cit note 9 1.

[19] Charles Goredema 'Chapter 4: Confronting money laundering in South Africa: An overview of challenges and milestones' available at *https://issafrica.org/topics/organised-crime/01-may-2007-monograph-no-132-confronting-the-proceeds-of-crime-in-southern-africa-an-introspection-edited-by-charles-goredema/chapter-4-confronting-money-laundering-in-south-africa-an-overview-of-challenges-and-milestones,* accessed on 10 January 2022.

1900's,[20] the evolution of the internet has provided criminals with a platform to expand ML operations which may extend far beyond the regulatory control of the current AML regime in SA.

This requires an analysis of the AML framework to combat ML methods pre and post the advent of the internet to expose possible gaps in the AML regime. This will provoke recommendations to improve the current AML framework in SA.

IV RESEARCH QUESTION

Based on the glaring negative effects of ML pre and post the internet, this research report seeks to provide answers to the following questions:

(a) How, if at all, has the internet heightened ML activities?
(b) Does South African AML legislation, regulations and industry specific regimes[21] effectively detect, prevent and reduce conventional and modern-day ML activities?
(c) If there are shortcomings in the current regulatory framework,
(d) How can these be addressed?

Through an analysis of the literature underlying these questions, this research report seeks to form a better understanding of ML methods pre and post the advent of the internet, inform the reader of the institutional role players, regulatory framework and offer guidelines which might contribute to the fight against ML. Further, it seeks to identify the sectors of the economy highly exposed to ML and expects to identify shortcomings in AML regime.

---

[20] Howard Chitimira and Sharon Munedzi 'Selected Challenges Associated With The Reliance On Customer Due Diligence Measures To Curb Money Laundering In South African Banks And Related Financial Institutions' (2021) 8(1) *Journal of Comparative Law in Africa* 43.

[21] Charles Goredema 'Chapter 4: Confronting money laundering in South Africa: An overview of challenges and milestones' available at *https://issafrica.org/topics/organised-crime/01-may-2007-monograph-no-132-confronting-the-proceeds-of-crime-in-southern-africa-an-introspection-edited-by-charles-goredema/chapter-4-confronting-money-laundering-in-south-africa-an-overview-of-challenges-and-milestones*, accessed on 10 January 2022.

CHAPTER II
MONEY LAUNDERING

I DEFINITION OF MONEY LAUNDERING

There are various definitions of ML depending on the jurisdiction and the laws governing the crime where it is committed. In SA, there are a number of legislative enactments which define ML and its elements. The Financial Action Task Force ('FATF') defines ML as 'the processing of these criminal proceeds to disguise their illegal origin.'[22]

The UN Vienna 1988 Convention describes the crime of ML as,

> 'the conversion or transfer of property, knowing that such property is derived from any offense(s), for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in such offense(s) to evade the legal consequences of his actions.'[23]

In SA an unofficial text for the Financial Intelligence Centre Act, 38 of 2001 ('FICA'), and the Money Laundering and Terrorist Financing Control Regulations, defines ML as 'an activity which has or is likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds.'[24]

The Prevention of Organised Crime Act 121 of 1998 ('POCA') defines 'proceeds of unlawful activities' as;

> 'any property or any service, advantage, benefit or reward which was derived, received or retained, directly or indirectly, in the Republic or elsewhere, at any time before or after the commencement of this Act, in connection with or as a result of any unlawful activity carried on by any person, and includes any property representing property so derived.'[25]

---

[22] FATF 'What is Money Laundering' available at *https://www.fatf-gafi.org/faq/moneylaundering/*, accessed on 9 April 2022.

[23] United Nations Office on Drugs and Crime 'Money Laundering' available at *https://www.unodc.org/unodc/en/money-laundering/overview.html*, accessed on 9 April 2022.

[24] FIC Anti-Money Laundering and Counter-Terrorism Financing Legislation (2018) at 15.

[25] The Prevention of Organised Crime Act 121 of 1998, s1.

'Unlawful activity' is 'any conduct which constitutes a crime or which contravenes any law whether such conduct occurred before or after the commencement of this Act and whether such conduct occurred in the Republic or elsewhere.'[26] Defining ML and establishing the elements of the crime are important in determining criminal liability. In addition, proving criminal liability under POCA and FICA requires an understanding of the process of ML.

II THE MONEY LAUNDERING PROCESS

The ML process occurs in three stages.

(a) Placement

The first stage is placement which is the introduction of the proceeds derived from illegal activity into the financial market or system.[27] At this stage the illegal proceeds are collected and deposited into various financial institutions both locally and internationally.[28]

(b) Layering

The second stage is layering, which involves multiple transactions being made by the money launderer to hide the source of the money.[29]

(c) Integration

The last stage is integration where the illegal proceeds are integrated into the economy with legitimate money through the purchase of asset investments in finance or commercial ventures.[30] The above stages may not be present in every ML transaction in sequence; stages may occur simultaneously, in isolation or occur numerous times throughout the entire

[26] Ibid.

[27] Weaver op cit note 3 445.

[28] Ibid.

[29] Ibid.

[30] Moshi op cit note 9 2.

transaction.[31] In every stage adopted by the money launderer, the motive throughout the entire ML process is to mask the trail of the origins of illicit money which was derived from illegal activity with the intention of bypassing AML laws, controls and processes.[32]

III MONEY LAUNDERING METHODS

(a) General

Methods of ML have developed over the years due to criminals finding new techniques to avoid triggering law enforcement mechanisms and internal controls from pinpointing that money is being laundered through a specific system.[33] Some of the most rampant ML methods in SA are accomplished through the banking system, shell or front companies, the casino and gambling industry and the real estate business.[34]

(b) The Banking System

There are five dominant banks in SA, Standard Bank, Absa, First National Bank and Investec Ltd which control 90% of the total banking assets.[35] In 2001, former Finance Minister Trevor Manuel estimated that around 2 to 8 billion US dollars are laundered through SA institutions.[36] Overtime financial institutions have introduced a wide range of financial products from cheque and saving accounts to investment, mortgage loans and vehicle finance options for customers. These options offer varying benefits to customers allowing a person to decide which product to place their money in or transfer value into.[37] With this being said a person or company will

---

[31] James Chen 'Money Laundering: What It Is and How to Prevent It' *Investopedia*, available at *https://www.investopedia.com/terms/m/moneylaundering.asp*, accessed on 13 January 2021.

[32] Moshi op cit note 9 2; Mabunda op cit note 11 217.

[33] Moshi op cit note 9 2.

[34] Ibid 2; Daley op cit note 1 176.

[35] IMF op cit note 16 para 97.

[36] Charles Goredema 'Chapter 4: Confronting money laundering in South Africa: An overview of challenges and milestones' available at *https://issafrica.org/topics/organised-crime/01-may-2007-monograph-no-132-confronting-the-proceeds-of-crime-in-southern-africa-an-introspection-edited-by-charles-goredema/chapter-4-confronting-money-laundering-in-south-africa-an-overview-of-challenges-and-milestones,* accessed on 10 January 2022.

[37] Ibid.

become a customer of more than one financial institution during its lifetime or operation. The idea of being able to hold multiple accounts at different financial institutions both locally and internationally is particularly attractive for money launderers who wish to hide the proceeds of illegal criminal or economic activity.[38]

Through the banking system a money launderer may transact using cash and bank accounts. In such an instance, this will involve a cash deposit of a large sum of money or multiple deposits of smaller amounts.[39] The money launderer may use a number of people, front or shell companies to deposit or receive the money to appear legitimate.[40] Placing money in investments and offshore banking accounts is attractive to a money launderer as laws and regulations may not be as stringent in other countries.[41]

The money will usually not remain in the account/s for a long period of time and will be transferred to its destination once it has been legitimised in the financial market. The purpose of structuring transactions is to create a paper trail that cannot be traced to the origins of the illegal activity or funds.[42]

(c) The Casino and Gambling Sector

There are eight casino groups in SA holding a gross gambling revenue of 1.3 billion US dollars.[43] Due to its capital-intensive nature this sector is more susceptible to ML activities through the purchase of chips, tokens and machine cards which hold monetary value.[44]

The Financial Intelligence Centre ('the FIC') has set out triggers by which ML at a casino or a gambling platform can be identified.[45] These include but are not limited to; when a person

[38] Rajeev Saxena 'Cyberlaundering: The Next Step for Money Launderers?' (1998) 10(3) *St. Thomas Law Review* at 691.

[39] Ibid 691- 94.

[40] Ibid.

[41] Ibid.

[42] Ibid 691.

[43] IMF op cit note 16 para 99.

[44] FIC Typologies and Case Studies (2019) 5-6.

[45] Ibid.

purchases or cashes in gambling chips or tokens and cannot and/or refuses to provide identification or provides false identification for verification purposes, when purchases of chips are made for a large amount of money and does not correlate to the gambling activities of the person (the person plays for a lesser amount), a request by the patron that the cash-in value be forwarded to a third party and not themselves and when a person opens a casino account and uses the account as a transactional or savings account.[46]

On the one hand this sector can be subject to simple ML transactions which are detectable and on the other hand more complex or structured transactions which require further investigation. Some of these typologies would include the structuring of transactions to avoid triggering the reporting requirement over a certain cash threshold.[47] In this instance a money launderer would construct multiple deposits of smaller denominations made by intermediaries or third parties, play at different casinos, split winnings into cash and keep value in chips and move between different gambling games and tables.[48] Another method to avoid the reporting requirement is feeding smaller amounts of money in machines and cashing out the value in larger denominations of banknotes.[49] Lastly a money launderer would buy or fix a game, this involves setting the outcome of the game which would involve bribing casino staff or playing with an accomplice with the pretense of playing an actual game and generating higher winnings.[50] From the above typologies and triggers on how money is laundered, it is identified that criminals will utilise casinos and gambling institutions in the placement stage of the ML process.[51]

[46] Ibid.

[47] Ibid.

[48] Ibid.

[49] Ibid 5.

[50] Ibid 6.

[51] Ibid 4.

(d) The Real Estate Industry

Similar to the banking, casino and gambling industries, the real estate industry in SA has fallen prey to ML as a method of hiding illegal funds through the purchase of property.[52] The real estate industry in SA comprises more than 40 000 estate agencies which attract both national and international customers wanting to invest in the SA property market.[53]

The FIC has identified methods of how money is laundered through the purchase of property. One method is a money launderer will require the property bond to be registered in the name of a front company or some other person or business associate. This hides the illegal source of funds which is used to purchase the property and the true ownership thereof.[54]

A second method entails a money launderer requesting a property developer or construction company to purchase a property on its behalf. The money would then be laundered through estate agencies and the institute providing the bond.[55] The main motive is for the money launderer to not place a large amount of his/her own money into the property which would attract suspicion.[56] A third method is purchasing property with the aim of providing a rental service on the property. This method allows the money launderer to open a bank account for the rental income and simultaneously conceal illicit income with the rental income in the same account.[57] A fourth method is 'flipping property'. This occurs when a money launderer purchases a property with the intention of reselling the property within a short period of time or after he/she has considerably renovated the property with the illicit proceeds thereby increasing the value of the property.[58] Lastly the FIC reported that attorneys are used in the facilitation of a property transaction to hold illegal proceeds in its trust account and transfer

[52] Rebecca Worthington 'South Africa Publishes More About Money Laundering Vulnerabilities' Squire Patton Boggs – The Anticorruption Blog 17 April 2019, available at *https://www.anticorruptionblog.com/africa/south-africa-publishes-more-money-laundering-vulnerabilities/* accessed on 10 January 2022.

[53] IMF op cit note 16 para 99.

[54] FIC op cit note 44 8.

[55] Ibid.

[56] Ibid.

[57] Ibid 9.

[58] Ibid.

these proceeds when instructed to do so.[59] The above methods can have many role players, such as a bank, a property developer, an estate agent, an attorney, a conveyancer, a seller, purchaser and the deeds registry. Despite the audit trail it creates, this does not deter money launderers from using the SA property market to launder illicit proceeds.[60] The purchasing of property coincides with the integration stage of the ML process as the illicit funds are used to purchase legitimate assets.[61] The attraction to the SA property market to launder money stems from the perception that investigative and enforcement agencies are not as well equipped as other countries in preventing and prosecuting ML.[62]

This harmful perception shines a light on the AML laws, regulations and agencies in place to combat ML. The discussion which pursues is the international and SA legal and institutional framework established to combat ML and how the above-mentioned three sectors of the economy assist in the fight.

CHAPTER III
COMBATING MONEY LAUNDERING

I INTERNATIONAL STANDARDS

In 1989 an inter-governmental body, the Financial Action Task Force ('FATF') was developed by Ministers of Member countries.[63] The purpose of the FATF is to 'set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related

[59] Ibid.

[60] Gregory Mthembu- Salter 'Chapter 2: Money Laundering in the South African real estate market today' June 2006, available at *https://issafrica.org/chapter-2-money-laundering-in-the-south-african-real-estate-market-today*, accessed on 10 January 2022.

[61] FIC op cit note 44 4.

[62] Gregory Mthembu- Salter 'Chapter 2: Money Laundering in the South African real estate market today' June 2006, available at *https://issafrica.org/chapter-2-money-laundering-in-the-south-african-real-estate-market-today*, accessed on 10 January 2022.

[63] FATF International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations (2021) 7.

threats to the integrity of the international financial system.'[64] These measures are known as the Forty Recommendations.[65]

The FATF obliges member countries to criminalise and prosecute ML and imposes sanctions in the event of non-compliance with its recommendations.[66] SA has been a member of the FATF since 2003 and has been subject to the FATF evaluations of its AML framework.[67] The next section discusses the SA AML framework and highlights the FATF's analysis of the shortcomings of AML compliance.[68]

II LEGISLATIVE ENACTMENTS

There are three legislative enactments in SA law which criminalise ML: the POCA, the FICA and the Financial Intelligence Centre Amendment Act 1 of 2017 ('FIC Amendment Act').[69]

(a) POCA

The POCA was introduced in SA in 1998 to repeal the Proceeds of Crime Act of 1996 ('PCA') and deal with ML activities on a much wider scale.[70] In relation to ML, the objectives of the POCA are to criminalise and combat ML through mechanisms such as mandatory reporting structures, and to recover and forfeit proceeds and assets derived from criminal activity.[71] In order to achieve this purpose, the POCA sets out three provisions detailing the offences which constitute the crime of ML.[72]

---

[64] Ibid.

[65] David Tuba 'Prosecuting Money Laundering The FATF Way: An Analysis of Gaps and Challenges In South African Legislation From a Comparative Perspective' (2012) *South African Journal of Criminology* 106.

[66] Ibid.

[67] Ibid 107.

[68] Ibid.

[69] Ibid 109.

[70] Ibid.

[71] POCA at 1.

[72] Tuba op cit note 65 109.

The first offence noted in section 4 of the POCA states that 'a person is guilty of money laundering if he/she enters into any engagement or engages in any arrangement or transaction with another person to conceal or disguise the nature, source, location or movement of the property deriving from his or her criminal activities.'[73] From the wording of section 4 the legislature intended for the provision to apply to a person who commits both the criminal activity and hides the proceeds thereof, commonly referred to as self-laundering.[74]

The second offence under section 5 applies to any other person acting on behalf of the perpetrator. This section provides that a person who retains or controls the proceeds of the criminal activity or acquires property with the same proceeds on behalf of or for the benefit of the perpetrator will be guilty of the offence of ML.[75]

The third offence is stated in section 6 which applies to a person who uses, acquires or has in his/her possession property which forms part of the proceeds of another person's criminal activity.[76] The wording of section 6 suggests that the person referred to is not the perpetrator nor the third party mentioned in section 5, but rather an accessory after the fact.[77]

The provisions of the POCA came under scrutiny by the FATF in 2009 and 2021. The FATF rated SA largely complaint in relation to criminalising ML. FATF stated that although section 4 covers self-laundering it does not provide for a wide range of scenarios which may occur.[78] FATF further stated that sections 4, 5 and 6 do not extend to predicate offences nor to the perpetrator of predicate offences.[79] FATF pointed out that SA does not apply a threshold to predicate offences nor requires a conviction to be obtained for predicate offences.[80]

[73] Ibid.

[74] Ibid.

[75] POCA, s5.

[76] POCA, s6.

[77] Tuba op cit note 65 110.

[78] FATF op cit note 8 at 162.

[79] Ibid 161-63.

[80] Ibid.

(b) FICA

The FICA was enacted in 2001 with the aim of establishing the FIC to fight ML by holding institutions accountable through various mandatory requirements,[81] provide advice to Government on the formulation of ML policies,[82] collate data and provide financial intelligence to agencies involved in the process of investigating and enforcing AML measures.[83]

The ML measures set out in the FICA requires an Accountable Institution ('AI') to engage in Customer Due Diligence ('CDD') and the derivative thereof being the 'Know Your Customer' ('KYC') processes. This involves identifying a client or a person acting on behalf of a client,[84] holding records of the identity of a client and persons acting on behalf of the client, the business relationship with the client and all transactions and accounts of the client.[85]

Further to this the FICA creates a cash reporting threshold which requires an AI report to the FIC on all transactions which exceed the threshold of R25 000.00 which were paid by a client or received by a client.[86] In addition to reporting cash transactions the FICA requires persons and businesses to report suspicious or unusual transactions.[87]

The CDD process was rated partially compliant in 2009 by FATF. FATF pointed out that no legal obligation was imposed on an AI to comply with the CDD process in relation to suspicious transactions.[88] No provision provided for continuous CDD or that enhanced CDD should be conducted on higher risk categories of individuals or businesses.[89] Furthermore, the reporting of unusual transactions was rated partially compliant due to the FICA not enacting a provision

[81] The Financial Intelligence Centre Act 38 of 2001 at 2.

[82] FATF op cit note 8 at 25.

[83] Charl Hugo and Wynand Spruyt 'Money laundering, terrorist financing and financial sanctions: South Africa's response by means of the Financial Intelligence Centre Amendment Act 1 of 2017' (2018) *TSAR* 227.

[84] FICA s21.

[85] FICA s23.

[86] FICA s 28.

[87] FICA s29.

[88] FATF Mutual Evaluation Report: Anti-Money Laundering and Combating the Financing of Terrorism: South Africa (2009) 215.

[89] Ibid 215-16.

which requires financial institutions to keep track of unusual patterns or of the size and complexity of transactions.[90] Government sought to address the shortcomings of the FICA in the following legislative enactment.

(c) FIC Amendment Act

This Act undertook new focuses in relation to financial crimes. A few of these are the introduction of a risk-based approach as a means of identifying and verifying a client; an increased obligation on CDD processes for beneficial ownership and prominent persons; and to implement programmes and training of risk management and compliance with AML measures.[91]

The risk-based approach follows a two-step process. First it requires an AI to identify and assess ML risks.[92] Depending on the type of relationship or transaction a suitable ML risk rating must be assigned to each relationship or transaction. This must be monitored and reviewed continually.[93] The second requires an AI to develop, maintain and document a risk and compliance management program, policies, controls and systems to combat ML and its associated risks.[94]

III INSTITUTIONAL ESTABLISHMENTS

There are many establishments which drive AML. However, for the purposes of this paper the roles of a few establishments will be discussed. As mentioned in paragraph (b) above the function of the FIC is to collect financial data and provide financial intelligence to agencies who attend to the investigation and prosecution of financial crimes.[95] A misconception is that the FIC is responsible for prosecution of ML. However, it merely acts as a support function,[96]

[90] Ibid 217.

[91] The Financial Intelligence Centre Amendment Act 1 of 2017, s7, s9, s10.

[92] Hugo and Spruyt op cit note 83 238.

[93] Ibid at 240-42.

[94] Ibid 248-49.

[95] Ibid 227.

[96] Ibid.

and enforces compliance with AML measures.[97] The South African Police Service ('SAPS'), is supposed to effectively investigate ML cases in collaboration with other units.[98] The National Prosecuting Authority ("NPA"), is primary responsible for investigating and prosecuting ML and all other crimes.[99]

The duty of the National Gambling Board ('NGB') is to regulate the gambling sector.[100] The Estate Agency Affairs Board ('EAAB') regulates estate agencies and ensures compliance with the FICA.[101] It is imperative for institutional bodies to work closely with legislative and regulatory policies to implement, monitor and review AML mechanisms to combat ML in line with international standards.

V AML MECHANISMS

This section identifies the AML measures most heavily relied upon to combat ML, namely CDD processes and Suspicious Transaction Reports ('STRs') and the associated challenges experienced in the banking, casino and gambling and real estate sectors in the adoption of these mechanisms.

(a) CDD

The CDD process is an AML measure which is highly recommended by FATF.[102] The FICA and the FIC Amendment Act place a legal obligation on an AI to comply with the CDD provisions prior to commencing a business relationship with an individual or a company.[103] The mandatory processes of identification and verification is set out in both Acts,[104] but does not detail the documentation which is to be accompanied to comply with the process fully. This is so because the FIC obliges an AI to implement a risk-based approach to determine the

[97] IMF op cit note 16 para 81.

[98] Ibid para 82.

[99] Ibid para 84.

[100] Ibid para 89.

[101] Ibid para 91.

[102] Chitimira and Munedzi op cit note 20 44.

[103] FICA s21; The FIC Amendment Act s7-9.

[104] Ibid.

type of information required to comply with the identification and verification provisions.[105] The change from a rigid approach to combating ML and allowing an AI to adopt discretionary methods[106] certainly leaves more room for money launderers to manipulate the CDD process. Financial institutions have adopted the KYC approach to essentially build a profile on each prospective client.[107] The following information is commonly required, namely full names, identity number, nationality, residential address, occupation and type of income.[108] In implementing the KYC approach various challenges in relation to the documentation required has been encountered.[109]

The first challenge is the identification and verification of the identity of a person. In SA, financial institutions, will require a customer's identification document, proof of address and proof employment prior to establishing a business relationship with such customer. A socio-economic challenge exists wherein unemployed individuals, individuals from lower income households and individuals with no proper housing are unable to participate in the formal financial sector because of the CDD process.[110] Should a financial institution ease its CDD process to accommodate these individuals, it will run the risk of being non-compliant with the FICA and FATF recommendations and attract individuals who will manipulate the relaxed CDD process to launder money.[111] The second challenge is that money launderers will professionally create false identification documents and present it to financial institutions to avoid detection. False documents are difficult to determine and requires examination by experts.[112] The third challenge is the issue of privacy. In the past financial institutions may have been reluctant to disclose customer sensitive or confidential information to law enforcement agencies due to privacy concerns. However, the newly enacted Protection of Personal Information Act 4 of 2013, does not apply to the processing of personal information used in

[105] FIC Guidance Note 7 on the Implementation of Various Aspects of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001) 28.

[106] Ibid.

[107] Louis De Koker 'Client identification and money laundering control: Perspectives on the Financial Intelligence Centre Act 38 of 2001' (2004) 4 *TSAR* 721.

[108] Ibid 722.

[109] Chitimira and Munedzi op cit note 20 45.

[110] Ibid.

[111] Ibid 49.

[112] De Koker op cit note 107 723.

the combating of money laundering[113] therefore an AI will be compelled to disclose certain client information in the investigation and prosecution of ML.

Similar to the financial sector, the casino and gambling sector may experience difficulties in effectively implementing CDD procedures and monitoring ongoing CDD as a result of the high cash environment with millions of transactions taking place every second of the day, not only nationally but also with the international community.[114] Casinos also offer array of financial services to its patrons and may find itself not applying strict CDD measures to all its offerings.[115] Lastly this sector may also be faced with fraudulent KYC documentation presented by a patron. This requires front line staff to undergo rigorous training programs on CDD policies, laws and means of identifying such risks.[116]

In comparison to the above sectors, the real estate sector was assessed to being underdeveloped in identifying and understanding ML risks owing to their reliance on counterparts such as financial institutions to take the lead in CDD processes on transactions.[117] The real challenge of not complying with FICA requirements presents itself when there is a cash sale of a property, a shell company is used as a party to the transaction or when the services of an agent is not utilised to facilitate the transaction.[118] This makes ML activities more difficult to detect.

Further to this the adoption of the CDD process causes transactions to become slow and not materialise because of the stringent requirements.[119] Despite the loss of business, the advantage

---

[113] The Protection of Personal Information Act 4 of 2013 s6(1)*(c)(ii).*

[114] PWC 'Effectively meet your regulatory obligations – Anti-Money Laundering in the Casino and Gaming Industry' available at *https://www.pwc.co.za/en/assets/pdf/anti-money-laundering-july-2011.pdf,* accessed on 14 February 2022.

[115] Ibid.

[116] Ibid.

[117] IMF op cit note 16 para 317-18.

[118] Jeffrey R. Boles 'Anti-Money Laundering Initiatives for the South African Real Estate Market' (2017) 1 *Journal of Comparative Urban Law and Policy* 201.

[119] Gregory Mthembu- Salter 'Chapter 2: Money Laundering in the South African real estate market today' June 2006, available at *https://issafrica.org/chapter-2-money-laundering-in-the-south-african-real-estate-market-today,* accessed on 10 January 2022.

in enforcing the CDD process is that it would deter money launderers from exploiting the property sector.[120]

(b) STRs

Another mechanism created by the FICA and FATF is requiring accountable and reporting institutions to report suspicious or unusual transactions in terms of section 29 of FICA.

To assist accountable and reporting institutions to identify suspicious or unusual transactions, the FIC has set out various transaction indicators of ML. Some of these include; requesting that funds be transferred immediately nationally or internationally, the use of trusts and other corporate vehicles, structuring of complex transactions, a transaction which does not align with a customer's financial history and status and a customer who refuses to comply with CDD processes.[121] A financial institution will track client transaction behaviours through the profile built via the CDD/KYC and ongoing CDD processes to determine whether a particular transaction is out of the ordinary course of the business relationship.[122] In the real estate sector, there are two types of transactions which are considered suspicious, the first is buying a property cash and the second is buying a property on behalf of someone else.[123] The trend to bypass STRs is to acquire a bond over the property through a financial institution and make payments over time.[124] In general, the casino and gambling sector tend to focus on increasing a customer's participation, gambling behaviours such as winnings and the amount of money played, thus detracting from identifying suspicious transactions.[125] It was reported by FATF that the FIC receives approximately 30 000 STRs, mostly filed by banks.[126] Casinos do lodge sufficient STRs and were considered an exception to other sectors which underreported.[127]

[120] Ibid.

[121] FIC Guidance Note 4 on Suspicious Transaction Reporting 9-10.

[122] Gregory Mthembu- Salter 'Chapter 2: Money Laundering in the South African real estate market today' June 2006, available at *https://issafrica.org/chapter-2-money-laundering-in-the-south-african-real-estate-market-today*, accessed on 10 January 2022.

[123] Ibid.

[124] Ibid.

[125] FATF Report – Vulnerabilities of Casinos and Gaming Sector (2009) para 207.

[126] FATF op cit note 8 at 49.

[127] Ibid 10.

Estate agents were reported to file the worst quality STRs.[128] The CDD process and the filing of STRs are integral mechanisms in combating ML in the physical medium. Notwithstanding the difficulties institutions may encounter in enforcing these mechanisms, mastering the dynamics of these mechanisms will assist in combating ML activities presented through electronic mediums.

CHAPTER IV
CYBERLAUNDERING

I THE CONCEPT OF CYBERLAUNDERING

The advent of the internet has created an 'information society'[129] which is heavily reliant on electronic databases to extract information, conduct transactions on a business and personal level and as a communication base for social and economic constructs.[130] Despite the many benefits of the internet, the danger is that it provides criminals a platform to commit a plethora of cybercrimes, one being ML.[131]

This new breed of ML coined 'cyberlaundering' is the process whereby 'individuals use the Internet and associated technologies to transform criminal proceeds into clean funds that are untraceable.'[132] Cyberlaundering was catapulted by the introduction of e-commerce. With the many components of e-commerce such as e-finance, e-money and other electronic payment methods, a cyberlaunderer has jumped on the bandwagon to use these electronic avenues to launder money,[133] leaving AML role players with the urgency to keep abreast of technological advancements to identify new techniques of cyberlaundering.

---

[128] Ibid.

[129] Sylvia Papadopoulos 'Chapter 1: An introduction to cyberlaw' in Papadopoulos @ Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 1.

[130] Ibid.

[131] Saxena op cit note 38 710.

[132] Shawn Turner 'U.S. Anti-Money Laundering Regulations: An Economic Approach To Cyberlaundering' (2004) 54(4) *Case Western Reserve Law Review* 1407.

[133] Cecily Raiborn, Chandra Schorg and Christie Bubrig 'Guarding Against E-Laundering of Dirty Money' (2003) 18(1) *Commercial Lending Review* 37.

II MECHANISMS OF CYBERLAUNDERING

The techniques of cyberlaundering are akin to conventional ML methods, in that the three-stage process of placement, layering and integration is still applied. However, the process is enhanced and made easier by the speed, convenience and anonymity of the internet.[134]

A hypothetical scenario was put forth by *Mabunda* in an article describing the ways in which money is laundered through cyberspace using online banking and gambling methods. She states that at the placement stage a money launderer will, as a first step, use a legitimately registered business and its services as a front company. The customers of the business will be charged a high membership fee which is paid into the bank account of the business and not in cash, this is to ensure that the bank's CDD requirements are met and STRs are not triggered.[135] The second step involves creating bank accounts for each member under fictitious names obtained via the deep web. The membership fee is laundered and the members are de-identified from the unlawful activity. Here multiple accounts can be opened in any jurisdiction.[136] In the layering stage of the process, the business would also offer a licensed online gambling service to members and the general public. A high fee is charged to participants to access the platform. The business would allow members to login with fictitious identities created and public users would be required to register with their true information. This enables the business to pool legitimate and illegitimate funds together to create a trail which authorities cannot easily identify.[137]

To control the gambling service, the business will use algorithms to rig games to not raise a suspicion regarding the winner or the amount of winnings. In the integration phase of the cyberlaundering process a patron's winnings would be paid into a legitimate account, which funds can then be integrated into the economy.[138]

---

[134] Turner op cit note 132 1407.

[135] Mabunda op cit note 11 225-26.

[136] Ibid.

[137] Ibid 227-30.

[138] Ibid 231.

The above hypothetical scenario displays the need for cyberlaundering investigators to advance technological skills and knowledge to keep abreast of criminal innovations which the internet creates.[139] Further to this an examination of sector specific online pursuits which have fallen prey to cyberlaundering is necessary in an attempt to enact preventative measures.

(a) Online Banking

The financial services sector has over the years proven to be a leading sector in the adoption of technology. The shift from traditional banking methods came about through the emergence of 'FinTech or financial innovations technology.'[140] FinTech companies caused a stir in the industry forcing leading banks to implement technologies to deliver improved financial services to the online client market to avoid losing the customer base. The services included wire transfers, smart cards and internet and mobile banking payment methods.[141] It is certain that the advancement of banking services to online platforms offers an array of benefits to the economy, it is for this reason that authorities cannot obstruct technological advancements to stop cyberlaundering, but should rather understand its methods to prevent it from occurring.[142]

(i) Wire Transfers

Dating back to the 1970s wire transfers emerged through financial institutions which required 'a set of instructions be sent from one bank to another bank which results in the transfer of funds from one account to another or several other accounts.'[143] To facilitate wire transfers the Society for Worldwide Interbank Financial Telecommunications S.C ('SWIFT') created a system which a member bank could utilise.[144]

---

[139] Ibid.

[140] Yen-Te Wu 'FinTech Innovation and Anti-Money Laundering Compliance' (2017) 12(2) *National Taiwan University Law Review* 204.

[141] Ibid 204-5.

[142] Wojciech Filipkowski 'Cyber Laundering: An Analysis of Typology and Techniques' (2008) 3(1) *International Journal of Criminal Justice Sciences* 17.

[143] Saxena op cit note 38 at 694.

[144] Ibid.

Money launderers found a way to manipulate wire transfer systems. With SWIFT each member bank has its own SWIFT code identifying its name and the country and city of its location.[145] These systems can be manipulated with false information obtained via the Dark Web from the start of opening of a bank account to making electronic payments.[146] To circumvent abuse of this payment method, FATF recommended that financial institutions 'include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain.'[147]

In SA wire transfers are known as EFT's and are popularly used on a daily basis.[148] FATF rated SA largely compliant with wire transfer regulations as SA legislation did not require 'all wire transfers to be accompanied by full originator information… and to ensure beneficiary FIs to consider restricting or terminating the business relationship with FIs that fail to meet the wire transfer requirements.'[149]

(ii) Stored value cards

Another payment system is stored value cards or bank cards, such as debit and credit cards. These cards have either a magnetic strip or computer chip upon which information and value can be stored and removed through bank certified devices.[150] Stored value cards are attractive to cyberlaunders for a number of reasons, the first being that 'their value is self-contained'[151] and can be increased, withdrawn or transferred via an ATM or electronic device such as a mobile phone or computer.[152]

---

[145] Shobhit Seth ' How the SWIFT Banking System Works' *Investopedia 28 February 2022,* available at *https://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp#toc-swift-for-electronic-funds-transfers,* accessed on 9 March 2022.

[146] Filipkowski op cit note 142 19.

[147] FATF op cit note 63 at 17-8.

[148] FATF op cit note 8 at 187.

[149] Ibid.

[150] Saxena op cit note 38 711-12.

[151] Ibid 712.

[152] Filipkowski op cit note 142 18.

The second is that a stored value card can be used anywhere in the world provided the international roaming feature of the account holder is activated.[153] Thirdly transactions are self-approved by the user and do not require the authorisation of the bank. For these reasons stored value cards provide a cyberlaunderer with a faster way of receiving and transferring small to large amounts of money without the interference of the bank.[154]

The FATF notes that recommendation 16 relating to wire transfers does not apply to credit and debit cards unless the transactions made via debit or credit card are accompanied by the relevant card numbers and information.[155]

(b) Online Gambling

The online gambling industry ranges from online gaming, sport betting, lotteries and tournaments.[156] Most gambling sites require participants to register with personal information in order to play further. Due to the virtual nature and the inability to verify participant identity or information, this exposes online gambling platforms to underage usage, theft of identity and payment methods to play. Another issue is mobility and the fact that online gambling sites can be set up and shut down in seconds thus hijacking participants information and money. Lastly as with in person gambling activities, games can be rigged and participants defrauded.[157]

The present position of online gambling in SA is that it is illegal as envisaged in section 11 of the National Gambling Amendment Act 7 of 2004 which provides that 'a person must not engage in or make available an interactive game as authorised in terms of this Act or any other national law.'[158] The future of online gambling depends on the pending enactment of the National Gambling Amendment Act 10 of 2008 which proposes the legalisation of online

[153] Ibid.

[154] Ibid 18-22.

[155] Mabunda op cit note 11 229.

[156] Sizwe Lindelo Snail 'Online Gambling in South Africa' (2007) 15(3) *Juta's Business Law* 114-15.

[157] Ibid.

[158] National Gambling Board South Africa 'Frequently asked Questions' available at, *https://www.ngb.org.za/faqs.aspx,* accessed on 11 March 2022.

casinos provided they are licensed.[159] Unlike online gambling, online betting is not illegal in SA.[160] A 2010 judgment in *Casino Enterprise (Pty) Limited (Swaziland) v Gauteng Gambling Board and Others* pronounced on the illegality of activities related to online gambling stating that it is unlawful for internet operators which host, persons who participate, entities which facilitate the transactions and entities which promote online gambling even if the gambling site is international.[161] The proposed amendment would be beneficial to AML mechanisms as it could possibly deter a cyberlaunderer from using online casino and gambling platforms to layer illicit proceeds if a penalty is attached to the unlawful use of online gambling platforms.[162] The FIC has not given much attention to ML which can occur on anonymous online gambling platforms nor on online betting platforms. The FIC seems to imply that risk assessments and CDD processes are to continue to be performed even if a client is onboarded via an electronic platform. In this regard FIC requires that should a service provider or technology be used to onboard a client to a gambling platform and the responsibility rests on the service provider or technology to properly obtain and verify the client's information.[163]

(c) Online Auctions

Virtual property transactions are fast becoming a popular avenue for a cyberlaunderer to buy property from auction companies.[164] If it is a cash sale, the transaction is simple as the cyberlaunderer will deposit the money in the auction company's account and thereafter take occupation of the property.[165] The cyberlaunderer will attempt to make the highest bid so a more than large enough sum of money is layered and integrated into the legitimate economy without suspicion being raised.[166]

[159] Murdoch Watney 'Chapter 15: Cybercrime and the investigation of cybercrime' in Papadopoulos @ Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 347.

[160] FIC Assessment of the inherent money laundering and terrorist financing risks – Gambling Sector (2022) 16.

[161] Watney op cit note 159 347.

[162] Ibid.

[163] FIC op cit note 160 15.

[164] Fillipkowski op cit note 142 22.

[165] Ibid.

[166] Ibid.

Comparable with cash and private transactions, online auctions pose increased problems for AML mechanisms. With face-to-face property auctions a bidder's identity was known and verified in person at the start of an auction, however with online auctions it is easier for a bidder to produce fraudulent identity documents as a result of not be subject to a face-to-face check.[167] In SA, the Consumer Protection Act 68 of 2008 ('CPA') makes specific provision for auctions occurring on any electronic platform. Specific to the online medium the CPA demands that the electronic platform over which an auction is conducted is to maintain security of a high standard, ensure that records are easily accessible and obtain from a prospective bidder their 'full names, identification or passport numbers, age, physical address, internet protocol address, login code or name and password.'[168]

The CPA further states that an auctioneer must refrain from, receiving any form of compensation prior to the goods being delivered to the purchaser, not accepting a bid from a non-registered bidder, misrepresent the composition of the goods, falsify the auction record or conduct a mock auction.[169]

III CYBERLAUNDERING REGULATIONS AND CONTROLS

Cyberlaundering can be classified as a cybercrime, this owing to the definition of cybercrime being, 'any unlawful conduct involving a computer or computer system or computer network, irrespective of whether it is the object of the crime (such as a DoS attack) or instrumental in the commission of the crime (such as fraud) or incidental to the commission of the crime.'[170] Thus, 'a cybercrime may be committed either on the internet…or on a computer which is not connected to the internet.'[171]

---

[167] Gary Murphy 'Preventing money laundering in the age of Covid' *Allsop* 9 December 2020*, available at https://www.allsop.co.uk/media/preventing-money-laundering-in-the-age-of-covid/,* accessed on 8 April 2022.

[168] Sylvia Papadopoulos 'Chapter 5: Online consumer protection' in Papadopoulos @ Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 83.

[169] Ibid 84.

[170] Watney op cit note 159 at 336-37.

[171] Ibid 337.

The investigation of physical crimes entails a criminal investigation and prosecution depending on the laws of the country in which the crime was committed.[172] Cybercrimes on the other hand require the traditional criminal laws and investigative methods to be developed to identify and regulate crimes occurring on any electronic platform.[173]

There are three phases of the regulation of cybercrimes. First is the 'no legal regulation of the internet'.[174] In the past SA laws did not regulate crimes committed via the internet.[175] However, a newly enacted piece of legislation, the Cybercrimes Act 19 of 2020, provides for offences relating to cybercrimes, empowers investigation of cybercrimes, obliges reporting of cybercrimes and promotes co-operation with foreign jurisdictions to detect, investigate and prevent cybercrimes.[176]

The second phase is the 'legal regulation of conduct'.[177] This phase saw authorities implementing legislation to criminalise conduct constituting cybercrimes.[178] Even though the Electronic Communications and Transactions Act 25 of 2002 ('ECTA') was enacted to address the problems which electronic platforms posed, traditional methods of criminal investigation were not effective enough.[179] The nature of the internet required co-operation by internet service providers ('ISPs'), website owners and other third parties,[180] and a timeous approach to detecting the crime and identifying the perpetrator.[181] The importance of this phase is to gather enough information for evidential purposes.[182]

The third phase is 'supplementing conduct regulation with laws providing for investigatory methods aimed at accessing and gathering information.'[183] This phase introduces methods of

[172] Ibid 334.

[173] Ibid.

[174] Ibid 338.

[175] Ibid.

[176] The Cybercrimes Act 19 of 2020 at 2.

[177] Watney op cit note 159 at 338-39.

[178] Ibid 338-39

[179] Ibid.

[180] Ibid.

[181] Ibid 339.

[182] Ibid.

[183] Ibid.

gathering information such as 'surveillance, interception or censorship.'[184] In this regard the SA legislature introduced the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 ('RICA') to regulate the employing of methods to gather information on electronic platforms.[185]

Criminalisation of internet conduct and employing methods to secure developing technologies is a progressive approach to preventing cybercrime.[186]

CHAPTER V
EVALUATION

I THE PRESENT POSITION

Prior to the popularity of the internet, ML existed for decades,[187] and has seen money launderers hide the proceeds of their illicit activities through the banking system,[188] legal and illegal gambling[189] and the purchase of property.[190] Although the crime of ML is non-violent[191] and its impact is not seen on the average citizen,[192] the objects of combatting ML are to curb the dangers of future activities with which the laundered money can fund[193] and its long-term negative effect on the economy of a country.[194] This saw SA government take proactive steps to implement legislative acts, regulations and guidance notes[195] for an AI[196] as well as institutional and enforcement bodies to abide by and consider, when detecting, prosecuting and

[184] Ibid.

[185] Ibid.

[186] Ibid 342.

[187] Daley op cit note 1 176.

[188] Ibid.

[189] Ibid.

[190] Boles op cit note 118 202.

[191] Tuba op cit note 65 106.

[192] Daley op cit note 1 179.

[193] Ibid 181.

[194] Ibid 179.

[195] Hugo and Spruyt op cit note 83 253.

[196] Ibid.

penalising ML.[197] The aim behind this was for SA to comply with an internationally recognised standard enforced by FATF.[198] However the need to adopt international mechanisms to combat ML, overlooked the country's socio-economic status.[199]

The current mechanisms prescribed by the FIC to combat ML focuses on the implementation of risk assessments, risk management and compliance programmes,[200] enhanced CDD processes[201] and the filing of STRs.[202] FATF has highlighted that the number of prosecutions and convictions of ML cases in SA have been for self-laundering based on predicate offences but fewer prosecutions on third party and foreign ML and predicate offences.[203] It has been recommended by FATF that institutional bodies must prioritise identification and investigation of ML, its networks and enablers apart from predicate offences.[204] To conclude, the current AML regime needs to be actively strengthened to prevent exploitation by money launderers and close any loopholes in the AML framework which may be further exploited by the internet.[205]

II THE INTERNET ERA

The internet can be described as a 'value-neutral tool,'[206] the reason being that while it has many social benefits it can also be quite detrimental when misused.[207] One of the detrimental effects of the internet is the fact that it has heightened ML techniques, creating a crime of cyberlaundering and providing cyberlaunders with the ease of conducting criminal activity remotely, much faster and a vanishing trail.[208]

---

[197] Ibid 233.

[198] Ibid 253.

[199] Chitimira and Munedzi op cit note 20 56.

[200] Hugo and Spruyt op cit note 83 237-38.

[201] FICA s21; The Amendment Act s7-9.

[202] FICA s29.

[203] FATF op cit note 8 at 50.

[204] Ibid 51.

[205] Kilian Strauss 'How can we effectively combat the use of the internet for money laundering' available at *www.academia.edu*, accessed on 10 July 2022.

[206] Turner op cit note 132 1410.

[207] Ibid.

[208] Raiborn et al op cit note 133 37-8.

For this reason, authorities are faced with a difficult task of regulating cyberlaundering without obstructing the beneficial use of the internet.[209] In South Africa legislative enactments such as the ECTA and the Cybercrimes Act regulate the use of electronic platforms and crimes occurring in cyberspace. However, the investigation and prosecution outcomes of these crimes are still to be revealed.[210] Furthermore legislative enactments alone are not sufficient to combat cyberlaundering.[211] To strengthen the AML regime a consideration of the below-mentioned recommendations will be helpful.

III RECOMMENDATIONS

(a) International co-operation and co-ordination

The internet has created a borderless environment for money launderers to exploit different jurisdictions.[212] Chasing a paper and an audit trail across borders to investigate cyberlaundering activities requires co-operation between countries,[213] the sharing of information[214] and legal assistance.[215] While most countries are slow to adapt existing laws and regulations to changing technology,[216] several countries have created organisations, policies and regulations to combat cyberlaundering.[217] The Council of Europe ratified the Convention of Cybercrime in 2004 to highlight the need to legislate crimes committed on the internet and the call for international

[209] Turner op cit note 132 1410.

[210] Watney op cit note 159 350.

[211] Nkateko Nkhwashu 'Is South Africa's anti-money laundering and counter terrorism financing regime effective?' *De Rebus* 1 May 2018, available at *https://www.derebus.org.za/is-south-africas-anti-money-laundering-and-counter-terrorism-financing-regime-effective/*, accessed on 20 April 2022.

[212] Tatiana Tropina 'Fighting money laundering in the age of online banking, virtual currencies and internet gambling' (2014) *ERA Forum* 72.

[213] Ibid.

[214] Raiborn et al op cit note 133 at 39.

[215] Strauss op cit note 205 3.

[216] Tropina op cit note 212 70.

[217] Dr. Nathalie RÉBÉ 'Cyber-Laundering' (2022) IX *Proceedings of the International Conference on Cybersecurity and Cybercrime* 78-79.

co-operation.[218] The European Union ('EU') has been instrumental in bringing attention to the need to regulate cybercrimes in various ways. The first was the establishment of the European Cybercrime Centre in 2013 which purpose is to support law enforcement bodies in the EU and outside of the EU.[219] The second was the enactment of the 2015/849/EU directive which seeks to prevent ML activities which occur via the internet by stating that the directive also applies to entities which operate on the internet.[220]

In Australia, the Australian Transactions Reports Centre ('AUSTRAC') instituted civil proceedings against the Commonwealth Bank of Australia in 2017 for failing to comply with AML laws, its own AML internal procedures and not assessing AML risks of its machinery.[221] In an effort to mitigate risks of ML and cyberlaundering in SA, regulators and institutional bodies should look at policy, investigative, and prosecutorial methods of mature economies to address such risk. Any regulatory gaps which exist can be closed through co-ordination and co-operation between countries.[222]

(b) Revising the CDD principle

Although the FICA has statutorily required an AI to implement the enhanced CDD process the FIC has not provided guidelines to identify low, medium and high-risk customers nor guidelines on the application of the CDD process on differing circumstances and for different customers.[223] Applying a blanket approach to CDD has exposed an AI, especially financial institutions to transactions using 'illicit currency exchanges, shell companies and smurfing in

[218] John Hunt 'The new frontier of money laundering: how terrorist organizations use cyberlaundering to fund their activities, and how governments are trying to stop them' (2011) 20(2) *Information & Communications Technology Law* 142.

[219] Yuriy Yu. Nizovtsev and Oleg A. Parfylo, Olha O. Barabash, Sergij G. Kyrenko and Nataliia V. Smetanina 'Mechanisms of money laundering obtained from cybercrime: the legal aspect' (2022) 25(2) *Journal of Money Laundering Control* 301.

[220] Ibid.

[221] Harry Dixon, Nicole S. Healy, Karen Van Essen, Alexander S. Birkhold, Francesca, Lulgjuraj, Paige Mason, Jung Pak, and Christina Robertson 'International Anti-Money Laundering' (2018) 52 *The Year in Review International Law* 408.

[222] RÉBÉ op cit note 217 79 – 80; Strauss op cit note 205 3.

[223] Chitimira and Munedzi op cit note 20 53.

South Africa.'[224] In addition, the risk-based approach should be applied consistently to both low and high-risk customers throughout the business relationship so as to not overlook ML activities which could occur by any customer regardless of the risk rating.[225] The CDD process should also be revised to protect the online environment from being exploited by cyberlaunders. In this regard, SA regulators should develop policies to regulate the use of electronic systems in electronic KYC/CDD processes as per the guidelines issued by FATF on digital identities.[226]

(c) Emphasising the importance of STRs

To the same degree which the CDD process has been enforced, the detection and reporting of suspicious and unusual transactions should also be given sufficient attention. An additional burden should be placed on the FIC to enforce this provision through penalties[227] as the FICA has created an offence for the failure to lodge STRs.[228] The FIC should also afford an AI with the requisite authority to suspend transactions immediately which are suspicious or unusual until investigations have been completed.[229]

In the USA, the Financial Crimes Enforcement Network ('FinCEN') had in 2016 addressed cybercrimes by requiring that cyber activities be subjected to the suspicious activity reporting requirement. [230] FinCEN further encouraged financial institutions in line with the BSA to share ML information and extend the information to include events occurring online with one another.[231] In addition, financial institutions were also encouraged to open the lines of

[224] Ibid.

[225] Ibid 58.

[226] Ahmad Ghozi 'The Urgency of Electronic Know Your Customer (e-KYC): How Electronic Customer Identification Works to Prevent Money Laundering in The Fintech Industry' (2022) 7(1) *Diponegoro Law Review* 37.

[227] Chitimira and Munedzi op cit note 20 61.

[228] FICA s52.

[229] Chitimira and Munedzi op cit note 20 61.

[230] Dixon et al op cit note 221 397-98.

[231] Ibid.

communication between its AML and cyber security departments as a means of expanding its AML efforts.[232]

Likewise, the EU introduced the Fifth Anti-Money Laundering Directive which recognises that ML can be committed through online gambling and virtual currencies and averred that the ML tools of filing suspicious reports and following KYC procedures are to be applied on a stricter basis by these industries.[233] Having regard to international policy developments, currently an obligation rests on the FIC to enforce strict compliance with the CDD process and lodging of STRs at a sectoral level through various risk assessments.[234] Once a sectoral standard is developed to combat ML, the enhancement of business activities through technology, likely to increase ML activities can also be effectively detected and deterred.[235]

(d) Utilising technology to detect cyberlaundering

It has been argued that the KYC/CDD processes will not be strong enough to detect ML activities which take place electronically.[236] As a result it has been suggested that robust AML technology systems be developed to combat cyberlaundering.[237] One such type of technology is the purchase of software to enable data mining functions. The benefit of this is to analyse large amounts of data for patterns associated with ML methods on all transactions of a customer.[238] A benefit of implementing new AML technology, requires all role players to keep abreast of new technologies, identify new typologies of cyberlaundering and develop new investigative techniques to combat cyberlaundering.[239]

---

[232] Ibid.

[233] Christoph Wronka '"Cyber-laundering": the change of money laundering in the digital age' (2022) 25(2) *Journal of Money Laundering Control* 335.

[234] FIC op cit note 15 at 1.

[235] Ibid.

[236] Raiborn et al op cit note 133 37.

[237] Chitimira and Munedzi op cit note 20 46.

[238] Raiborn et al op cit note 133 38.

[239] Mabunda op cit note 11 232.

IV CONCLUSION

The pre-internet era saw money launderers engaging in multiple transactions and using several platforms to hide illicit funds and criminal activity.[240] The internet era and technological developments are rapidly improving, permitting money launderers to take advantage of the speed, anonymity and remoteness which the internet provides to commit crimes.[241] Money launderers and cyberlaunders benefit from relaxed laws, regulations, weak enforcement methods[242] and inefficiencies in compliance and reporting structures.[243] With this in mind FATF has scrutinised current SA AML legislative, regulatory and enforcement frameworks developed to combat ML and has identified shortcomings in the AML regime. These shortcomings frustrate better detection, prosecution and conviction rates of ML activities.[244]

Therefore, the current AML regime needs to be strengthened and the scope extended to include activities conducted on the internet. This can be achieved through revising CDD and STRs processes, implementing technology and international co-operation and co-ordination. Through this exercise post internet ML activities can be tackled head on by legislators, institutional, investigative, prosecutorial authorities and sectors of the economy who adopt a technological mindset to predict a money launderers tactics and implement strategies to effectively combat future ML methods committed on any platform.[245]

[240] Ibid 218.

[241] Turner op cit note 132 1407; Raiborn et al op cit note 133 37-8.

[242] Moshi op cit note 9 2.

[243] RÉBÉ op cit note 217 78.

[244] Chitimira and Munedzi op cit note 20 61.

[245] Mabunda op cit note 11 232.

BIBLIOGRAPHY

Journal articles

Boles, Jeffrey R. 'Anti-Money Laundering Initiatives for the South African Real Estate Market' (2017) 1 *Journal of Comparative Urban Law and Policy* 197.

Chitimira, Howard and Munedzi, Sharon 'Selected Challenges Associated With The Reliance On Customer Due Diligence Measures To Curb Money Laundering In South African Banks And Related Financial Institutions' (2021) 8(1) *Journal of Comparative Law in Africa* 42.

Daley, Madelyn J. 'Effectiveness of United States and International Efforts to Combat International Money Laundering' (2000) 2000 *Saint Louis-Warsaw Transatlantic Law Journal* 175.

De Koker, Louis 'Client identification and money laundering control: Perspectives on the Financial Intelligence Centre Act 38 of 2001' (2004) 4 *TSAR* 715.

Dixon, Harry, Healy, Nicole S., Van Essen, Karen, Birkhold, Alexander S., Lulgjuraj, Francesca, Mason, Paige, Pak, Jung and Robertson, Christina 'International Anti-Money Laundering' (2018) 52 *The Year in Review International Law* 397.

Filipkowski, Wojciech 'Cyber Laundering: An Analysis of Typology and Techniques' (2008) 3(1) *International Journal of Criminal Justice Sciences* 15.

Ghozi, Ahmad 'The Urgency of Electronic Know Your Customer (e-KYC): How Electronic Customer Identification Works to Prevent Money Laundering in The Fintech Industry' (2022) 7(1) *Diponegoro Law Review* 34.

Hugo, Charl and Spruyt, Wynand 'Money laundering, terrorist financing and financial sanctions: South Africa's response by means of the Financial Intelligence Centre Amendment Act 1 of 2017' (2018) *TSAR* 227.

Hunt, John ‘The new frontier of money laundering: how terrorist organizations use cyberlaundering to fund their activities, and how governments are trying to stop them’ (2011) 20(2) *Information & Communications Technology Law* 133.

Mabunda, Sagwadi ‘Cyberlaundering and the Future of Corruption in Africa’ (2018) 2(2) *Journal of Anti-Corruption Law* 214.

Moshi, Humphrey P B ‘Fighting money laundering: The challenges in Africa’ (2007) *Institute for Security Studies* 1.

Nizovtsev, Yuriy Yu. and Parfylo, Oleg A., Barabash, Olha O., Kyrenko, Sergij G. and Smetanina, Nataliia V. ‘Mechanisms of money laundering obtained from cybercrime: the legal aspect’ (2022) 25(2) *Journal of Money Laundering Control* 297.

Raiborn, Cecily, Schorg, Chandra and Bubrig, Christie ‘Guarding Against E-Laundering of Dirty Money’ (2003) 18(1) *Commercial Lending Review* 36.

RÉBÉ, Dr. Nathalie ‘Cyber-Laundering’ (2022) IX *Proceedings of the International Conference on Cybersecurity and Cybercrime* 77.

Saxena, Rajeev ‘Cyberlaundering: The Next Step for Money Launderers?’ (1998) 10(3) *St. Thomas Law Review* 685.

Snail, Sizwe Lindelo ‘Online Gambling in South Africa’ (2007) 15(3) *Juta’s Business Law* 114.

Tropina, Tatiana ‘Fighting money laundering in the age of online banking, virtual currencies and internet gambling’ (2014) *ERA Forum* 69.

Tuba, David ‘Prosecuting Money Laundering The FATF Way: An Analysis of Gaps and Challenges In South African Legislation From a Comparative Perspective’ (2012) *South African Journal of Criminology* 103.

Turner, Shawn 'U.S. Anti-Money Laundering Regulations: An Economic Approach To Cyberlaundering' (2004) 54(4) *Case Western Law Review* 1389.

Weaver, Stephen Jeffery 'Modern Day Money Laundering: Does the Solution Exist in an Expansive System of Monitoring and Record Keeping Regulations?' (2005) 24 *Annual Review of Banking & Financial Law* 443.

Wronka, Christoph '"Cyber-laundering": the change of money laundering in the digital age' (2022) 25(2) *Journal of Money Laundering Control* 330.

Wu, Yen-Te 'FinTech Innovation and Anti-Money Laundering Compliance' (2017) 12(2) *National Taiwan University Law Review* 201.

Internet references

BusinessTech 'How to reduce money laundering in 2020' 23 January 2020, available at *https://businesstech.co.za/news/industry-news/367824/how-to-reduce-money-laundering-in-2020/*, accessed on 12 January 2022.

Chen, James 'Money Laundering What It Is and How to Prevent It' *Investopedia*, available at *https://www.investopedia.com/terms/m/moneylaundering.asp*, accessed on 13 January 2021.

FATF 'What is Money Laundering' available at *https://www.fatf-gafi.org/faq/moneylaundering/*, accessed on 9 April 2022.

Goredema, Charles 'Chapter 4: Confronting money laundering in South Africa: An overview of challenges and milestones' available at *https://issafrica.org/topics/organised-crime/01-may-2007-monograph-no-132-confronting-the-proceeds-of-crime-in-southern-africa-an-introspection-edited-by-charles-goredema/chapter-4-confronting-money-laundering-in-south-africa-an-overview-of-challenges-and-milestones*, accessed on 10 January 2022.

KYC-Chain 'The History of Money Laundering' 25 April 2019, available at *https://kyc-chain.com/the-history-of-money-laundering/*, accessed on 4 January 2022.

Mthembu- Salter, Gregory 'Chapter 2: Money Laundering in the South African real estate market today' June 2006, available at *https://issafrica.org/chapter-2-money-laundering-in-the-south-african-real-estate-market-today*, accessed on 10 January 2022.

Murphy, Gary 'Preventing money laundering in the age of Covid' *Allsop* 9 December 2020*,* available at *https://www.allsop.co.uk/media/preventing-money-laundering-in-the-age-of-covid/,* accessed on 8 April 2022.

National Gambling Board South Africa 'Frequently asked Questions' available at *https://www.ngb.org.za/faqs.aspx,* accessed on 11 March 2022.

Nkhwashu, Nkateko 'Is South Africa's anti-money laundering and counter terrorism financing regime effective?' *De Rebus* 1 May 2018, available at *https://www.derebus.org.za/is-south-africas-anti-money-laundering-and-counter-terrorism-financing-regime-effective/*, accessed on 20 April 2022.

PWC 'Effectively meet your regulatory obligations – Anti-Money Laundering in the Casino and Gaming Industry' available at *https://www.pwc.co.za/en/assets/pdf/anti-money-laundering-july-2011.pdf,* accessed on 14 February 2022.

Seth, Shobhit 'How the SWIFT Banking System Works' *Investopedia 28 February 2022,* available at *https://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp#toc-swift-for-electronic-funds-transfers,* accessed on 9 March 2022.

Strauss, Kilian 'How can we effectively combat the use of the internet for money laundering' available at *www.academia.edu*, accessed on 10 July 2022.

United Nations Office on Drugs and Crime 'Money Laundering' available at *https://www.unodc.org/unodc/en/money-laundering/overview.html*, accessed on 9 April 2022.

Worthington, Rebecca 'South Africa Publishes More About Money Laundering Vulnerabilities' Squire Patton Boggs – The Anticorruption Blog 17 April 2019, available at *https://www.anticorruptionblog.com/africa/south-africa-publishes-more-money-laundering-vulnerabilities/*, accessed on 10 January 2022.

Legislation

The Cybercrimes Act 19 of 2020.

The Financial Intelligence Centre Act 38 of 2001.

The Financial Intelligence Centre Amendment Act 1 of 2017.

The Prevention of Organised Crime Act 121 of 1998.

The Protection of Personal Information Act 4 of 2013.

Guidance Notes

FIC Guidance Note 7 on the Implementation of Various Aspects of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001).

FIC Guidance Note 4 on Suspicious Transaction Reporting.

National Reports

FIC Anti-Money Laundering and Counter-Terrorism Financing Legislation (2018).

FIC Assessment of the inherent money laundering and terrorist financing risks – Gambling Sector (2022).

FIC Report released on risks of money laundering facing the gambling sector (2022).

FIC Typologies and Case Studies (2019).

International Reports

FATF International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations (2021).

FATF Mutual Evaluation Report: Anti-Money Laundering and Combating the Financing of Terrorism: South Africa (2009).

FATF Mutual Evaluation Report: Anti-Money Laundering and counter-terrorist financing measures (2021).

FATF Report – Vulnerabilities of Casinos and Gaming Sector (2009).

International Monetary Fund (IMF) Country Report No. 21/227 Detailed Assessment Report on Anti-Money Laundering and Combating the Financing of Terrorism (2021).

Book Chapters

Papadopoulos, Sylvia 'Chapter 1: An introduction to cyberlaw' in Papadopoulos @ Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 1 – 8.

Papadopoulos, Sylvia 'Chapter 5: Online consumer protection' in Papadopoulos @ Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 63 – 93.

Watney, Murdoch 'Chapter 15: Cybercrime and the investigation of cybercrime' in Papadopoulos @ Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 333 – 351.