JOURNAL OF ANTI-CORRUPTION LAW

2018 Volume 2 Number 2 Pages 214 - 233

CYBERLAUNDERING AND THE FUTURE OF CORRUPTION IN AFRICA

Sagwadi Mabunda *

ABSTRACT

Corruption has been given considerable attention as one of the major causes of the socio-economic ills that plague Africa. Statistics reveal that staggering amounts of money are lost annually to corruption. Many discussions about corruption focus on its meaning, its causes and its impact but one pertinent issue goes unexamined: what happens to the money? The answer is money laundering. And while we are trying to grapple with the challenges of today, it is imperative that we consider the troubles that await. This paper discusses the relationship between corruption and money laundering, with a focus on the technique of cyberlaundering. It recommends that regional research units be created to address the issues raised.

1 INTRODUCTION

This paper argues that the future of corruption is inextricably linked to money laundering. Corruption is a contentious subject which has been given considerable attention as one of the major causes of the socio-economic ills that plague Africa. It is a serious hindrance to her progress as a continent, as the statistics reveal that staggering amounts of money are lost annually to corruption. It goes without saying that Africa is facing a major crisis. Corruption is probably one of the most discussed topics at all levels of society, from top government officials to the lowest and most marginalised groups. The harm that corruption has done to this resource rich continent has become common knowledge.

Many discussions focus on the meaning of corruption, the causes of corruption and the impact of corruption, but one pertinent issue goes

* LLB (Wits), LLM (UWC), PhD Candidate (UWC). Email: Sagwadi.mabunda@gmail.com.
The author would like to express her gratitude to the National Research Foundation of South Africa for its generous support.

unconsidered: what happens to the money? Sometimes, perpetrators of grand corruption will flaunt their lavish lifestyles, showing off their luxury homes, expensive vehicles and designer clothes but it should be noted that these people are not representative of the community of corrupt individuals with whom Africa has to contend. The question that is often overlooked is: What do those who do not engage in ostentatious behaviour do with the proceeds of their corruption? What about those who commit corruption in the private sector with the intention of using some of the proceeds for the company itself? How do they manage to hide their corrupt activities and use the dirty money? The answer is money laundering.

This paper considers the future of corruption in Africa. It does so, not by focusing upon corruption directly but upon its enabler, money laundering through the technique of cyberlaundering. The reason for this approach is two-fold. Firstly, there is plenty of discussion of both corruption and money laundering in their respective fields. However, seldom does one find discussion that builds a bridge connecting the two crimes. Secondly, this attempt to connect the two considers them not only in their present form but also in their future manifestation in cyberspace.

The next section will discuss the relationship between corruption and money laundering. The third section will turn the focus to money laundering, highlighting what it is and what regulatory frameworks govern it. The fourth section will look at the three phases of money laundering, namely, placement, layering and integration. It will explain these phases from a cyberlaundering perspective and by way of a fictitious scenario on how the proceeds of corruption may be laundered. Thereafter, some recommendations will be offered, including the creation of regional research units dedicated to conducting research which will inform policy and legislation.

2 RELATIONSHIP BETWEEN CORRUPTION AND MONEY LAUNDERING

There has been a dearth of academic scholarship on the relationship between corruption and money laundering. Although recent years have seen a call for it to be considered carefully, that call has not been answered adequately. One of the reasons for the scant attention that has been paid to this topic is the relative novelty of corruption and money laundering as international policy priorities. Both came into prominence only in the 1990s. There also is the problem that agencies charged with combating economic crimes have created an artificial separation between corruption and money laundering, with one agency focusing on

corruption and the other on money laundering.[1] International actors, such as the World Bank, the United Nations and the Asian Development Bank, have each called for the adoption of an integrated approach to combating corruption and money laundering.[2]

Corruption covers an array of activities which range from public sector bribery to private sector insider trading and everything in between. Two definitions of corruption are used regularly. The first is provided by Transparency International, according to which corruption is "the abuse of public office for private gain".[3] This definition usually is criticised for focusing only on corruption in the public sector and ignoring private sector corruption. A second definition was proposed and adopted by some international organisations in 2006. These included the International Monetary Fund, the Asian Development Bank and the World Bank. For them, corruption is "the offering, giving and receiving, soliciting, directly or indirectly, of anything of value to influence improperly the actions of another party".[4] This definition is broad and somewhat ambiguous. It leaves ample leeway for individual interpretation, which can result in it being abused or rendered ineffective.

Chapter III of The United Nations Convention against Corruption (UNCAC) provides for criminalisation of and law enforcement against corruption. Articles 15 to 22 include active and passive bribery, the embezzlement or diversion, trading in influence, illicit enrichment by a public official and the like. These provisions cover corruption in both the public sector and the private sector. As an international convention, UNCAC provides the necessary guidance for signatories to be able to implement its provisions domestically. The parameters set by UNCAC therefore will inform what conduct is considered corrupt when determining whether an act constitutes a predicate offence for money laundering.[5]

Money laundering is defined as "the processing of … criminal proceeds to disguise their illegal origin".[6] This definition is provided by the Financial Action Task Force (FATF), which is the international inter-governmental body that sets the anti-

1 See Chaikin D & Sharman JC (2009) *Corruption and Money Laundering: A Symbiotic Relationship* New York: Palgrave Macmillan at 3.
2 Chaiken & Sharman (2009) at 3.
3 Transparency International "How to Define Corruption" at 1, available at https://www.transparency.org/what-is-corruption (visited 18 March 2019).
4 Asian Development Bank (2006) *Anticorruption Policy: Harmonised Definitions of Corrupt and Fraudulent Practices* Manilla: Asian Development Bank at 3.
5 A predicate offence is a crime that gives rise to money laundering.
6 FATF "What is Money Laundering?" at 1, available at http://www.fatf-gafi.org/faq/moneylaundering/#d.en.11223 (visited 18 March 2019).

money laundering standards worldwide. The FATF's definition of money laundering is less contentious than the definitions of corruption.

Money laundering manifests itself either through simple transactions where the illicit proceeds are relatively small amounts or through complicated multi-layered transactions for larger amounts. Furthermore, it can be done by an individual or involve the participation of many persons.[7] And, more recently, it has shifted its area of operation from the terrestrial to cyberspace.

The illicit proceeds do not have to be in the form of cash always. They can be in the form of any assets, such as precious metals and minerals (for example, gold and diamonds), credit card receipts, stocks and bonds, rare coins and money orders. The aim of the launderer is to conceal the origins of the illicit proceeds and to do this it is necessary to commingle the "dirty" funds with "clean" funds to make them indistinguishable from each other and confuse the investigation authorities.

In most jurisdictions, corruption is a predicate offence for money laundering and this is one of the factors which helps to create intersection between the two crimes. Moreover, for money laundering to thrive it depends heavily on corrupt government officials, business executives and dishonest banks. Such uninhibited economic delinquency within the financial sector, in which financial institutions are complicit, ultimately leads to the eroding of the economic growth of a country.[8]

Chaiken & Sharman contend that corruption and money laundering have a symbiotic relationship, not only in the sense that they tend to occur together but, more importantly, in that the occurrence of the one tends to result in the creation of the other. In short, they reinforce each other incident-wise.[9] The same authors suggest that the failure of anti-money laundering and anti-corruption strategies is due largely to the fact that the problems relating to corruption and money laundering have been studied in isolation.[10] This is worrisome, particularly in African countries, for the simple reason that the combating of corruption and money laundering is stymied by a lack of local "ownership". In turn, this means that whatever anti-money laundering and anti-corruption policies may be in existence, dealing with the two crimes separately results in gaps that can be exploited by those who are the supposed guardians and keepers of these policies.

---

7 Hamman AJ (2015) *The Impact of Anti-Money Laundering Legislation on the Legal Profession in South Africa* (PhD Thesis: University of the Western Cape) at 9.

8 Van Jaarsveld IL (2004) "Following the Money across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet" 16 *South African Mercantile Law Journal* 685-694 at 688.

9 Chaiken & Sharman (2009) at 1.

10 Chaiken & Sharman (2009) at 2.

There may be instances where corrupt officials may launder their dirty funds and then undermine the measures designed to detect, prevent and punish such misconduct.[11] Studies show that anti-corruption and anti-money laundering policies are not priorities in many developing countries.[12] This could be attributable to a perception amongst these countries that anti-money laundering and anti-corruption policies have been foisted upon them by outsiders who have little or no understanding of the more pressing problems besetting their economies. As a result, the law enforcement agencies are maintained only symbolically, to pay lip service to international and regional oversight bodies.[13]

Of course, these problems are not unique to Africa. But the continent faces exceptional challenges when it comes to corruption, which makes it all the more necessary not to regard corruption in isolation from money laundering. Certainly, one cannot be solved without an understanding of the other. This paper discusses the problem of corruption from the vantage point of money laundering, particularly cyberlaundering in an effort to provide a new perspective. For purposes of this discussion, corruption will be considered only insofar as it is a predicate offence for money laundering.

3 MONEY LAUNDERING

There are several techniques which a launderer can adopt to hide the origin of illicit funds. The most common way to do this is by depositing money into a bank or into the trust account of a designated non-financial business, such as a law firm or a real estate agent. Essentially, the launderer wants to create as much distance between the proceeds of the crime and the crime itself. The idea is to engage in a number of financial transactions with the dirty money — which may involve international transactions — all for the purpose of concealing its illegal origins. The so-called "layered" money then is introduced into the legitimate economy to make it appear as lawful money. After this has taken place, the money launderer is free to do whatever he or she desires to do with the money. Often, the money is used to purchase luxury items.

Whatever techniques are used in any given case, the money laundering process consists of three phases, namely, the placement stage, the layering stage and the integration stage. Cyberlaundering is a technique which has to be considered together with the archetypal money laundering techniques, since it is unlikely that 100 per cent of the money laundering process can occur outside

11 Chaiken & Sharman (2009) at 8.
12 Chaiken & Sharman (2009) at 22.
13 Chaiken & Sharman (2009) at 21.

cyberspace. The fact of the matter is that the cyberlaunderer may have to re-surface from cyberspace at some point, particularly when he or she has to commingle with or introduce the illicit funds into the lawful terrestrial economy.

Africa's technological capabilities are growing at exponential rates. Gone are the days when corrupt officials and other criminals would smuggle money from one jurisdiction to another in big suitcases via porous borders. Nowadays cyberspace affords corrupt individuals fast, cheap, safe and easy avenues to launder their ill-gotten gains. And whilst we can theorise about the many ways to commit corruption, at the end of the day the only thing that matters is where the money goes and how to retrieve it. Understanding the new ways in which corrupt individuals launder criminal proceeds will help dispossess them of their dirty money and deter them from further corrupt activities, because the risk of exposure will become greater than the rewards of the criminal act. Combating cyberlaundering will give the citizenry confidence that the regulators are forward thinking in their attempts to stop corruption, thereby making it possible to retrieve at least some of the stolen money.

In 2001, Morris-Cotterill observed that there is a popular notion that the internet provides a new and undetectable method of money laundering. He argued that the internet is merely an updated cheque system or a more secure, efficient and cheaper means of moving money.[14] He claimed also that the publicity surrounding cyberlaundering was due simply to efforts to introduce more stringent regulations for the internet. These would result in raising barriers for poorer nations, a proposition which he regarded as "dubious".[15] Morris-Cotterill concluded that the notion that the internet makes money laundering easier is an erroneous one, not deserving of any consideration of the interface between money laundering and technology.[16] It is submitted that, nowadays at least, such views cannot be correct because they are based on the false assumption that banks are at the centre of all transactions and that the information that is associated with all transactions is kept with the transaction, in the sense that it is present at every point of the transaction via whatever messaging system is being used. Today, unlike 2001, the internet does deserve serious consideration in relation to money laundering because it does pose serious threats in this regard.

14 Morris-Cotterill N (2001) "Money Laundering" *Global Policy Forum*, available at https://www.globalpolicy.org/component/content/article/172/30048.html (visited 21 March 2019).

15 Morris-Cotterill (2001).

16 Morris-Cotterill (2001).

Money laundering evolves as criminals discover new capabilities to clean their dirty money. Cyberlaundering is not a new form of money laundering. On the contrary, it adopts the tried and tested structure of money laundering, in the form of placement, layering and integration, but elevates it to a new level. It is merely a new technique applied to the traditional three-tiered money laundering process.

3.1 Regulating Money Laundering

There are several international instruments which regulate money laundering.[17] Anti-money laundering efforts are dependent not only on hard law in the form of international conventions, but also are grounded in soft law which is embodied in the 40 + 9 Recommendations of the FATF. Even though the FATF Recommendations are not binding legally, they play a very significant role in anti-money laundering efforts, as they have been adopted and implemented by many countries to signify their commitment and political will to combating money laundering.[18]

In every region of the world, the work of the FATF is supported by FATF-style bodies. These bodies ensure that the Member States in the respective regions are compliant with the FATF.[19] In Africa alone, there are four FATF-style bodies, namely, the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), the Middle East and North Africa Financial Action Task Force (MENAFATF), the West Africa Money Laundering Group (GIABA) and the Central Africa Anti-Money Laundering Group (GABAC). This means that every corner of Africa is covered by anti-money laundering laws.

The soft anti-money laundering law is not only limited to the 40+9 FATF Recommendations. It is found also in several guidelines, codes and best practices of

17 These are the 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention); the 2001 UN Convention against Transnational Organised Crime (Palermo Convention); and the UN Convention against Corruption (UNCAC). It bears noting that the Vienna Convention has the more African signatories and states parties than the other conventions. See Fernandez L (2017) "Corruption (Article 28I) and Money Laundering (Article 28Ibis)" in Werle G & Vormbaum M (eds) *The African Criminal Court: A Commentary on the Malabo Protocol* Dordrecht: Asser Press at 101.

18 Fernandez (2017) at 101.

19 There are nine FATF-style regional bodies in the world. They are: (1) Asia/Pacific Group on Money Laundering (APG) based in Sydney, Australia; (2) Caribbean Financial Action Task Force (CFATF) based in Port of Spain, Trinidad and Tobago; (3) Eurasian Group (EAG) based in Moscow, Russia; (4) Eastern & Southern Africa Anti-Money Laundering Group (ESAAMLG) based in Dar es Salaam, Tanzania; (5) Central Africa Anti-Money Laundering Group (GABAC) based in Libreville, Gabon; (6) Latin America Anti-Money Laundering Group (GAFILAT) based in Buenos Aires, Argentina; (7) West Africa Money Laundering Group (GIABA) based in Dakar, Senegal; (8) Middle East and North Africa Financial Action Task Force (MENAFATF) based in Manama, Bahrain; (9) Council of Europe Anti-Money Laundering Group (MONEYVAL) based in Strasbourg, France. See Fernandez (2017) at 102.

a host of international and intergovernmental supervisory bodies and organisations. For example, the Basel Committee on Banking Supervision aims to improve the supervision of banking internationally. The Wolfsberg Group is a key contributor to the formulation of guidelines to deal with financial crime risks. It is an association of 13 banks worldwide[20] which enforces guidance relating to the application of customer due diligence rules, anti-money laundering and counter-terrorist financing policies.

Africa also has continental and regional co-operation initiatives. The then Organisation of African Union Convention on Preventing and Combating of Terrorism of 1999 (Algiers Convention) and the 2002 Plan of Action of the African Union High-Level Intergovernmental Meeting on the Prevention and Combating of Terrorism in Africa are notable anti-money laundering documents. The Plan of Action includes measures such as the enactment of national laws to criminalise money laundering and financing of terrorism, the setting up of financial intelligence units, training personnel on fighting and preventing money laundering and regulating co-operation with international financial institutions. All these measures are efforts to curb terrorist financing.[21]

Some have argued that ordinary money laundering efforts are cumbersome and should be discarded.[22] They hold that the stringent policies that are being imposed by the anti-money laundering authorities place an unbearable strain on the financial services of small countries[23] and contribute to undermining the financial wellbeing of those countries because of the increased administrative and financial commitments required to implement them.[24] However, whereas they may be cumbersome, they are necessary, because the negative impact that money laundering has on national income and output, fiscal policies, exchange rates and terms of international trade[25] far outweighs the burden of enforcement mechanisms.

Money laundering distorts the prices of imports and exports by increasing the former and decreasing the latter, which leads to weakening of the economic

20 The 13 banks are Banco Santander, Bank of America, Bank of Tokyo-Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JP Morgan Chase, Société Générale, Standard Chartered Bank and UBS.

21 Fernandez (2017) at 101 note 38.

22 See, for example, Rahn RW (2002) "Taxation, Money laundering and Liberty" 9(4) *Journal of Financial Crime* 341-346.

23 Rahn (2002) at 344.

24 Stessens G (2000) *Money Laundering: A New International Law Enforcement Model* Cambridge: Cambridge University Press at 165.

25 Bartlett BL (2002) *The Negative Effects of Money Laundering on Economic Development* Asian Development Bank Regional Technical Assistance Project No 5967 at 1.

position of the affected country. It also leads to the decrease of creditability in the eyes of foreign direct investors. Money laundering also has the added disadvantage of being exploited for terrorist activities, although one should add that the money used by terrorists need not be sourced from a crime, but can be clean money from a very legitimate source.

3.2 Customer Due Diligence

Section D of the FATF Recommendations provides for preventive money laundering measures. These are the measures that ought to be taken by financial institutions and designated non-financial businesses and professions to prevent money laundering. In terms of Recommendation 9 countries should make sure that the financial institution secrecy laws within their jurisdiction do not inhibit the implementation of any of the FATF recommendations. Recommendations 10 and 11 provide for customer due diligence and record-keeping respectively.

Customer due diligence (CDD) is part of the risk-based approach to the application of anti-money laundering mechanisms. This approach is meant to be the foundation of efficient allocation of resources across the anti-money laundering and countering of terrorist financing efforts. Under the risk-based approach, countries should require their financial institutions and designated non-financial businesses and professions to identify, assess and take effective action to mitigate their support of money laundering and terrorist financing.[26]

Recommendation 10 requires financial institutions to undertake CDD measures when establishing business relations; when carrying out occasional transactions which either are above the designated threshold of USD/EUR 15 000 or are wire transfers; where there is a suspicion of money laundering or terrorist financing; or where the financial institution has any doubts about the veracity or adequacy of customer identification data previously obtained.[27] This implies that CDD is not a once-off exercise. The Interpretive Note to Recommendation 10 states that financial institutions are not required repeatedly to verify the identity of the customer for each and every transaction. They can rely on the information supplied in the first instance, unless there is a suspicion by that there may be something amiss.[28] For example, a suspicion of money laundering related to a customer's account or substantial changes in the customer's account which are

26 FATF Recommendations (2016) at 11.
27 FATF Recommendation 10.
28 FATF Recommendation 10.

inconsistent with the customer's business profile constitute circumstances that may warrant a further verification.[29]

CDD entails the following measures. Firstly, it is necessary to establish and verify the customer's identity through reliable and independent source documents, data or information. The information can be verified through a certificate of incorporation, a certificate of good standing, a deed of trust or any other independently verifiable source which can prove the name, form and the current existence of the customer. It is also important to verify the address of the customer's residence or, in the case of a legal person, the address of the registered office and, if different, its principal place of business.[30] Secondly, where a corporate vehicle, such as a trust, is created it is of utmost importance that the identity of the beneficial owner be disclosed, as well as that of the beneficiary. This is a matter that has become all the more urgent following the publication of the Panama Papers.[31] Thirdly, financial institutions need to understand and, where necessary, obtain information on the purpose and intended nature of the business relationship. This might involve analysing the economic logic of a transaction. In other words, given say, the bank's knowledge of the customer's income and account activity, does it make any sense for the customer to set up an offshore company in a country known for its strict bank secrecy and lax anti-money laundering legislation. Fourthly, it is required of financial institutions and all accounting entities to conduct ongoing due diligence in the business relationship and to scrutinise transactions that occur during the business relationship. The aim is to ensure that the institution's knowledge of the customer, the business and the risk profile of the customer and, where necessary, the customer's source of funds are consistent with the transactions made by the customer.

Where the financial institution is unable to verify the identity of the customer and the beneficial owners of accounts or it is unable to comply with the requirements from the FATF Recommendations, then it should refrain from opening an account, commencing with the business relationship or completing the transaction. In some cases, it may be necessary to terminate the business relationship altogether. Financial institutions are urged to consider submitting a suspicious transaction report (STR) about the customer to the designated financial intelligence unit.[32] This report, when submitted, must be anonymous. Hence,

29 Interpretive Note to FATF Recommendation 10.

30 FATF Recommendation 10.

31 International Consortium of Investigative Journalists (2017) "Leaders, Criminals and Celebrities" at 1, available at https://www.icij.org/investigations/panama-papers/ (visited 18 March 2019).

32 FATF Recommendation 10.

according to Recommendation 21, financial institutions (their directors, employees and officers) are prohibited from disclosing to the customer the fact that a STR has been forwarded to the financial intelligence unit.[33]

4 CYBERLAUNDERING TECHNIQUES

4.1 Placement

Placement is the first phase of laundering money. It involves the launderer performing the first act of distancing the proceeds from the actual crime. Depending on the crime perpetrated, the difficulty of placing the money can vary. When one is dealing with a cash intensive criminal enterprise, such as an unlawful narcotics peddling business, the proceeds typically are returned to the kingpin in bulky hard cash. Bulky cash is difficult to hide and even harder to deposit into a bank without raising suspicion. Some of the safeguards put in place by anti-money laundering initiatives include setting reporting thresholds to which banks must adhere. If, for example, a country has decided that its banks must record any cash deposits above the threshold of USD/EUR 15 000, then the bank receiving such a deposit would be required to collect personal identifying information about the account holder as part of its customer due diligence as per FATF Recommendation 10.

In terms of conventional money laundering, as opposed to cyberlaundering, the launderer would put the money into a legitimate cash intensive small business, such as a jewellery store or a pizzeria, which would act as a front to conceal the criminal activity. This kind of front business renders the money less suspicious when it eventually is injected into the lawful economy during the integration phase.[34] The placement phase is probably the hardest phase for launderers in the laundering cycle because it lends itself to easy detection, especially when large amounts of money are deposited in a financial institution.

In order to circumvent deposits that ordinarily would trigger an STR, money launderers typically make use of process of “smurfing” or “structuring”. What this means is that the launderer breaks up the pool of money into smaller bundles which fall below the reporting threshold. Then several “smurfs” are employed to deposit the money under separate names in the same bank or different banks, without attracting suspicion. An even easier way would be to work in cahoots with corrupt bank officials who turn a blind eye to the deposit of reportable amounts in

33 FATF Recommendation 10.

34 De Kock L (2003) “Money Laundering Trends in South Africa” 6(1) *Journal of Money Laundering Control* 27-41 at 36.

exchange for a fee. Given the rampant poverty in Africa, it is not hard to imagine that the prospect of earning something on the side would be seductive to many corruptible bank tellers or other officials charged with responsibility of conducting due diligence procedures.

Terrestrial money laundering tends to be very risky because it involves a large network of people, and not all of them can be trusted. Taking money laundering into cyberspace makes the exercise easier and more efficient. Below is a hypothetical[35] which takes money laundering as far into cyberspace as possible. This narrative will traverse all three phases of the money laundering cycle, highlighting the process as it evolves.

Basani is the owner of the trendy and exclusive Burgundy Country Club. Membership of and entrance into this exclusive club is by invitation only, and her clientele includes some very influential corporate executives and government officials. On the face of it, the club is merely a networking platform for the elite, but in reality it is a nest of corrupt activities. This is where corrupt deals are made and sealed. The club's exclusivity is its key to success, because it guarantees secrecy and Basani provides the best money laundering services corrupt money can buy.

Basani is exceptionally skilled in technology and she provides various cyberlaundering services to her clients. In return, she is guaranteed protection from criminal investigative and prosecution, as well as several other privileges and benefits. In the placement phase of her cyberlaundering schemes, Basani must ensure that she has a front business that will obscure some of the illicit funds to be laundered. The Burgundy Country Club is registered as a legitimate business, which allows it to meet the minimum requirements for CDD as recommended by the FATF.

As her first line of defence, Basani operates a no-cash policy for all transactions associated with the Burgundy Country Club, legal or otherwise. She keeps track of all her business in encrypted files to which only she has access to. This scheme allows her to avoid bulk cash transactions that would raise the suspicion of banks. The Burgundy Country Club offers an array of services to its members and they are encouraged to set up accounts with the club in order to gain access those services. The exclusivity of the Burgundy Country Club also means that the admission fees are exceptionally high, the idea being that investigators are

35 Names, characters, businesses, places, events and incidents are either the products of the author's imagination. Any resemblance to actual persons, living or dead, or actual events is purely coincidental.

not astonished when they come across financial transactions involving large sums. The steep membership fees are indeed a prelude to the types and magnitude of the transactions that are processed by the Burgundy Country Club.

With the legal transactions out of the way, Basani sets out on her criminal enterprise. To begin with, she requires that the members pay an exorbitant monthly loyalty fee. These loyalty fees are recorded formally as such, but only as a disguise. In reality, they are laundered and then re-paid to members at the end of the year as part of the Burgundy Country Club's "cash-back incentive programme". The membership fees, loyalty fees and other ancillary costs are processed through the accounts of the Burgundy Country Club to promote the impression of its being a legitimate business.

The second step is for Basani to set up various bank accounts for the members of the Burgundy Country Club under false identities. These false identities would have been purchased, at shockingly low prices, from black market merchants found in the deep web. One does not have to go to the deep web to acquire fake identities because they can be obtained just as easily on the surface web or even from conventional criminal syndicate.[36] The deep web merely provides greater anonymity than the other routes.

The purchase of false identities on the internet does three things for Basani. Firstly, it ensures that the members of the Burgundy Country Club can put distance between themselves and the laundered assets. Secondly, it ensures that they can create as many bank accounts as they wish, which is particularly helpful at the layering stage of the money laundering. Such multiple accounts mean that they do not have to depend on third-party bank accounts. All they need do is move the money around amongst themselves as members of the club or amongst their own bank accounts for added security. Thirdly, multiple false identities also mean that the members do not have to be limited to one jurisdiction or one set of even biometric data. In an ideal situation, a money launderer would use at least one jurisdiction with strict bank secrecy laws while exploiting loopholes in other legal systems and international co-operation to facilitate her criminal activities. When using cyberspace, this becomes easy to accomplish because there are no virtual jurisdictional borders with which to contend. For instance, today John Smith can

36 In May 2018, Chriselda Lewis, an investigative journalist for SABC News, did an exposé which revealed that one can buy a fake payslip, three months' bank statements and a fake identity in an internet café in downtown Johannesburg for less than R600. This is risky, though, as one can be identified easily when one enters and exits the cafe. See Lewis C (2018) "SABC News Exposes Fake Payslips, Bank statements" *SABC News* at 1, available at http://www.sabcnews.com/sabcnews/sabc-news-exposes-fake-payslips-bank-statements/ (visited 18 March 2019).

be a 30-year-old South African male, residing in Johannesburg and tomorrow he can be a 45-year-old Zambian female resident in Lusaka with property in Malawi, Uganda and Tanzania. Online transactions have the added benefit of not having facial recognition opportunities. False identities also mean that if one should assume the "citizenship" of a particular jurisdiction, one can skirt some of the tedious verification practices usually imposed upon foreigners, particularly in countries with lax anti-money laundering practices or strong bank secrecy laws. Furthermore, Basani can ensure that the club members use prepaid cards for some transactions so that they will not leave the same kind of trail that credit cards would.

4.2 Layering

The next step in money laundering is layering. This phase seeks to create a smokescreen to befuddle investigators in search of the paper trail.[37] Layering creates a multitude of transactions which can span across several locations as well as over numerous jurisdictions.[38] Cyberspace has made the world smaller and has rendered national borders almost redundant. It also has the added benefit of providing near instantaneous transactions.

The key in the layering phase is to ensure that the illegal funds are indistinguishable from legitimate funds. The most common way of doing this is through wire transfers. FATF Recommendation 16 deals with wire transfers, which is very helpful in relation to the problem of cyberlaundering. The Recommendation is intended to prevent terrorists and other criminal organisations from having unrestricted access to wire transfers to further their illegal enterprises. It main purpose is to keep track of the basic information associated with the originator and the beneficiary whilst ensuring that the information is available readily when needed.[39] The information needs to be accessible to law enforcement agencies and/or prosecutorial services to aid them in investigations and prosecutions of criminals and terrorists. It also is important for the prevention of money laundering because it may allow for the detection of criminal or terrorist activities. Additionally, the information needs to be available to financial intelligence units which may use it to identify and analyse any suspicious or unusual activity. Finally, it may be useful in instances where financial institutions have to freeze a customer's account.[40]

37 Hamman (2015) at 13.
38 Madinger 2012) at 260.
39 Interpretive Note to FATF Recommendation 16.
40 Interpretive Note to FATF Recommendation 16.

In essence, the Recommendation provides that when financial institutions are dealing with wire transfers and related messages, they must ensure that they obtain accurate originator and beneficiary information in respect of the transactions. Thereafter, they must ensure that the acquired information regarding the wire transfer remain with the transaction throughout the payment chain.[41] This would not be problematic in the deep web.

Briefly, the deep web, the dark web or the hidden web refers to the unindexed portion of the internet. The unindexed portion is a collection of thousands upon thousands of websites which can be accessed only via special tools such as Tor and I2P. The dark web is most notorious for being the site where all nefarious activities occur in cyberspace. It is known for black market drug sales, assassins for hire and child pornography.[42] It is used also as a safe-haven for whistle-blowers from oppressive regimes because it provides almost absolute anonymity. It is a tool which can be used for good or bad, depending on the user's inclination. The dark web's real seductiveness lies in the anonymity it provides by hiding the IP addresses of the servers that run them, making it is hard to establish where and by whom they are hosted.[43] The dark web can be an important tool for a cyberlaunderers because it creates the perfect smokescreen for most of the transactions.

Countries are required to ensure that their financial institutions monitor transactions with the intention of detecting those which do not have the required originator and/or beneficiary information. Thereafter, the financial institutions must take appropriate defensive measures, which may include freezing non-compliant accounts. Further, countries should forbid transactions involving designated persons and entities identified in the relevant United Nations Security Council resolutions which aim to prevent and suppress terrorism and terrorist financing.[44]

The FATF recommends that countries set a monitoring threshold which is lower than the one imposed by CDD measures. Countries also may apply a minimum threshold for cross-border wire transfers not higher than USD/EUR 1 000. Terrorist groups can further their agendas with relatively small wire transfer amounts. Therefore, if the threshold is too high, many of the transactions would

41 FATF Recommendation 16.

42 Greenberg A (19 November 2004) "Hacker Lexicon: What is the Dark Web?" *Wired* at 1, available at https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/ (visited 18 March 2019).

43 Greenberg (19 November 2004) at 1.

44 FATF Recommendation 16.

be undetectable.[45] However, when the thresholds are reduced, they must not be too low because they would overburden financial institutions with too many transactions to track. Since countries are expected to trace all wire transfer activities, it is imperative that an appropriate balance be struck.

The scope of the Recommendation 16 is applicable to both domestic and cross-border wire transfers. Both cross-border transfers and domestic transfers always should contain the name of the originator and of the beneficiary, the originator and beneficiary account number, and the originator's address or national identity number and further personal details.[46] Person-to-person wire transactions fall within the ambit of Recommendation 16.

Recommendation 16 does not cover all online transactions. Transactions completed with credit, debit or prepaid cards for the purchase of goods and services are exempt from its requirements if the credit, debit or prepaid card numbers accompany all the transactions which flow from the respective cards. This means that if one can create a platform which provides goods and services, such as an online merchant, one can skirt the requirements of Recommendation 16. Although it might be possible for the initial transactions to be recorded when the client makes the first payment with her credit, debit or prepaid card, the originator and beneficiary information does not have to be attached to all the transactions thereafter. Furthermore, given that one can use false identities, even if the information is captured in the beginning it may not have as big an impact as the investigators may hope because it may not lead to the true identity of the suspect. Moreover, even if there is some information recorded, such as the transaction not including payment for a good or service, an interruption in the chain of transactions may pose an obstacle to investigators.

It is time to return to the Burgundy Country Club hypothetical. Basani is aware of the opportunities for money laundering on the internet, with her favourite platform being online gambling. The Burgundy Country Club offers an online gambling platform which is licensed so that it can meet the CDD tests imposed by financial institutions and other regulators. Basani decides not to confine the online gambling platform to members of the Burgundy Country Club. Her rationale for this decision is that the platform have as many users as possible, thus making sure that one cannot determine whether it is used solely for the pleasure of gambling or as a conduit for money laundering. It creates the perfect smokescreen as it becomes impossible to distinguish between criminal and lawful

45 Interpretive Note to FATF Recommendation 16.
46 Interpretive Note to FATF Recommendation 16.

funds. The astronomical fee which she charges for access to the gambling platform is meant to filter the participating players, so that her politician and business clients do not attract suspicion if they play with large amounts of money. Some of the money that was entrusted to Basani by her clients is used to fund the account of an online casino which is used to wager up the amounts that are played in the games.[47]

Burgundy Country Club members may elect to use their personal computers to enter the platform or they may choose to enter via the heavily encrypted computers available at the club and which will assist technologically challenged members to cover their tracks. The computers at Burgundy Country Club are routed through the Tor network which allows the users access to the dark web.

Most internet gambling sites require players to register onto the site and to provide basic identifying information.[48] Basani makes this a requirement for every player who is not a member of the Burgundy Country Club to ensure that when law enforcement agencies investigate the gambling platform, it can be shown to be a legitimate business. Burgundy Country Club members, as part of the loyalty rewards programme, can "register" with the linked false identity accounts to expand the layering of the proceeds.

Basani also makes use of algorithms that allow a player to gamble against himself to create a complex web of transactions in the game. This technique operates as follows. John wishes to play Black Jack online but he is an amateur at the game, which means he can enter the platform as Player A. The idea behind this is to minimise risk. If John relies on another real player, Player B, to enter the game and play against him, he runs the risk of losing some money if Player B is better than he and they do not have a prior agreement with each other. In order to safeguard against this, the game is rigged with a computer algorithm that will allow John to play against himself as both Player A and Player B. This would work in the same way as if he were playing against a computer in a single player mode, except that this time the computer can generate as many players as needed, which means that John can play against Players B, C, D, E, F and G at the same time, with him being the only human player at the table. Given that all this is happening online, investigators do not have the visual clues that "humans" have been substituted with algorithms.[49]

47 Cabot A (2001) *The Internet Gambling Report IV* Las Vegas: Trace Publications at 5-12.

48 National Gambling Impact Study Commission (1999) *Final Report* at 5.

49 This example is informed by episode 10 of season 1 of *CSI: Cyber*, titled "Click Your Poison", air date 6 May 2015.

What is more, to further the pretence of a real game, Basani rigs things to allow John, as Player A, to win some hands and lose others. Basani can determine for how long she wants the games to last, be it single games, which see John winning the final game, or be it multiple-day games in tournament style. The latter form of play will allow John to win some games and lose others without raising suspicion when he comes out as the ultimate winner.

The beauty of creating an algorithm to play these games is that Basani's clients can log in with their multiple false identities and accounts to participate. Also, she can use the accounts of her clients to play without their having to participate actively. This would work in a similar way to an investment banker making investments on behalf of her clients without their being concerned with the day-to-day activities of their investment portfolios.

Online gambling is just one of the ways of layering dirty money, but it is very effective because it is not regulated as heavily as terrestrial gambling. In addition, it involves complex technological innovations which are streets ahead of the run-of-the-mill criminal investigator.

4.3 Integration

The final phase of money laundering is the integration stage. This occurs when the money is returned into the lawful economy. This is also the stage at which the gamblers' winnings are paid back to them via cheques or credited to their legitimate bank account to be assimilated back into the lawful economy. At this stage, unless the money is has been converted into Bitcoins, the cyberlaundering cycle would be concluded.[50] Thereafter, transactions revert to the archetypal techniques, but if the other phases have been negotiated meticulously and without a hitch, all that is left for the criminal to do is to enjoy the laundered proceeds.

5 RECOMMENDATIONS

An essential element of legislative and policy change is consolidated academic research. In order to combat corruption and money laundering, it is proposed that regional research units be created. Every regional block in Africa ought to have an institutional research unit dedicated to researching the intersectionality of economic crimes and their future manifestations.

50 The use of cryptocurrency in cyberlaundering has been discussed by the author in Mabunda S (2018) "Cryptocurrency: The New Face of Cyber Money Laundering" in Proceedings of the *IEEE International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)* 1-6.

Take, for example, the Southern African Development Community (SADC). At least one of the universities in any of the SADC countries ought to house a UN-funded economic crime and cybercrime research unit. This research unit should not only do ordinary research but also run postgraduate academic programmes in the field. This would produce pure academic research which is not stifled by bureaucracy or corruption. Furthermore, if the research units are housed in universities and funded by the UN, it would ensure that there are both international oversight and internationally recognised academic standards in place.

Additionally, having the research unit be a regional effort and not country specific would allow for robust information sharing at a regional level and thereafter, via annual or bi-annual conferences, scholars of each unit can meet to discuss their findings. These finding can be published via the relevant AU and UN committees or agencies. This would allow academics and policy makers to observe the trends in each region and identify the points of convergence and divergence in order to formulate effective solutions.

Creating regional academic research units will ease the strain on individual governments which have talented and willing researchers but do not have the resources to give them research opportunities in their respective countries. This would lessen the burden on anti-corruption and anti-money laundering institutions to produce their own research, as they can co-operate with the research units and focus their resources on combating corruption and money laundering.

6 CONCLUSION

As corruption is a predicate for money laundering, it is important to consider the direction that both corruption and money laundering are going to take. The technique of cyberlaundering is the next logical step.

This paper has shown, through an extended hypothetical, what opportunities are available in cyberspace for launderers to hide and disguise their dirty money. The example of Basani's Burgundy Country Club represents only the tip of an enormous iceberg which requires the urgent attention of governments. It also highlights the way in which investigators need to think about cyberlaundering and how investigative techniques ought to be devised. Quite frankly, investigators must learn to think like launderers in order to anticipate their stratagems and counter them effectively.

Governments need to approach cyberlaundering not with trepidation but with a clear understanding that it is not a new crime against which they need to legislate afresh. Rather, it is a new technique that has been added to the arsenal of

techniques at the disposal of money launderers and which needs to be understood. Finally, cyberlaundering cannot be ignored in the vain hope that it will disappear. It will not because technology, including the technology of crime, is the future.