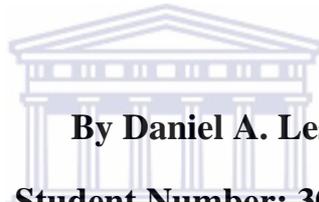


**ANTI-CYBERLAUNDERING REGULATION AND CONTROL**

**Submitted in partial fulfilment of the requirements of the LLM degree  
Transnational Criminal Justice and Crime Prevention – An  
International and African Perspective**

**University of the Western Cape**



**By Daniel A. Leslie**

**Student Number: 3006651**

**UNIVERSITY of the  
WESTERN CAPE**

**Prepared under the supervision of**

**Professor (Dr) Lovell Fernandez**

**Faculty of Law, University of the Western Cape, Cape Town, South  
Africa**

## TABLE OF CONTENTS

<i>Declaration</i>	vi
<i>Dedication</i>	vii
<i>Acknowledgement</i>	viii
<i>Abstract</i>	x
<i>Key words</i>	xi
<i>List of abbreviations</i>	xii
<b>CHAPTER 1: MAPPING THE TERRAIN</b>	1
1.1 INTRODUCTION	1
1.2 THE PROBLEM OF CYBERLAUNDERING: SIGNIFICANCE OF RESEARCH	2
1.3 RESEARCH QUESTIONS	4
1.4 SCOPE OF RESEARCH	5
1.5 LITERATURE REVIEW	5
1.6 METHODOLOGY	7
<b>CHAPTER 2: A BACKGROUND ON MONEY LAUNDERING: THE PRE-INTERNET ERA</b>	8
2.1 GENERAL	8
2.2 THE CONCEPT OF MONEY LAUNDERING	8
2.2.1 Defining money laundering	8

2.2.2 A brief history of money laundering	9
2.2.3 The money laundering process	11
2.2.4 Conventional money laundering methods	12
<b>2.3 WIRE TRANSFERS:</b>	
<b>A SHIFT FROM THE HARD CASH SYSTEM</b>	13
2.3.1 General	13
2.3.2 The meaning of wire transfers	13
2.3.3 The problem with wire transfers	14
2.3.4 A bridge between wire transfers and cyberlaundering	15
<b>CHAPTER 3: CYBERLAUNDERING</b>	17
3.1 GENERAL	17
3.2 THE CONCEPT OF CYBERLAUNDERING	17
3.2.1 The meaning of cyberlaundering	17
3.2.2 E-money	17
3.2.2.1 <i>Smart cards</i>	19
3.2.3 Models of cyber space payments systems	21
3.2.3.1 <i>The Merchant-Issuer model</i>	21
3.2.3.2 <i>The Bank-Issuer model</i>	22
3.2.3.3 <i>The Non-Bank-Issuer model</i>	22
3.2.3.4 <i>The Peer-to-Peer model</i>	23
3.3 THE CYBERLAUNDERING CYCLE	24
3.3.1 General	24

3.3.2 Placement	24
3.3.3 Layering	25
3.3.4 Integration	26
<b>3.4 CYBERLAUNDERING METHODS AND TECHNIQUES</b>	<b>26</b>
3.4.1 General	26
3.4.2 Online banking	27
3.4.2.1 <i>Online banking: A hypothetical scenario</i>	29
3.4.3 Online auctions	30
3.4.3.1 <i>Online auctions: A hypothetical scenario</i>	31
3.4.4 Online gambling	32
3.4.4.1 <i>Online gambling: A hypothetical scenario</i>	34
3.4.5 Digital payments systems	35
3.4.5.1 <i>Digital payments systems: A hypothetical scenario</i>	37
3.4.6 Virtual communities	38
3.4.6.1 <i>Reasons why SL can be used for money laundering</i>	40
3.4.6.2 <i>Second Life: A hypothetical scenario</i>	42
<b>CHAPTER FOUR: REGULATING CYBERLAUNDERING: POSSIBILITIES AND PRACTICALITIES</b>	<b>44</b>
4.1 GENERAL	44
4.2 CURRENT AML MEASURES AND CYBERLAUNDERING	45
4.3 EFFORTS BY ANTI-MONEY LAUNDERING AGENCIES	47
4.3.1 Governmental agencies	47

4.3.1.1 <i>The Drug Enforcement Administration</i>	47
4.3.1.2 <i>The Federal Bureau of investigation</i>	49
4.3.1.3 <i>National Accountability Bureau</i>	50
4.3.1.4 <i>Serious Crime Agencies</i>	51
4.3.1.5 <i>Immigration and Customs Enforcement</i>	51
4.3.2 Financial agencies	52
4.3.2.1 <i>Financial Action Task Force</i>	52
4.3.2.2 <i>Financial Crimes Enforcement Network</i>	54
4.3.2.3 <i>The World Bank</i>	55
4.4 GENERAL PREVENTIVE MEASURES FOR CYBERLAUNDERING	57
4.5 SPECIFIC PREVENTIVE MEASURES: CHOKES POINTS OF CYBERLAUNDERING	58
4.5.1 Safeguarding online banking	58
4.5.1.1 <i>Modifying the KYC principle</i>	58
4.5.1.2 <i>Adopting new wire transfer models</i>	61
4.5.2 Tighter measures for cyber payment systems	63
4.5.2.1 <i>Smart cards regulation</i>	63
4.5.2.2 <i>Protected cryptography</i>	64
4.5.2.3 <i>Better detection mechanisms</i>	65
4.5.3 Blocking the lacunae in e-gaming	67
4.5.3.1 <i>Regulation and virtual communities</i>	67
4.5.3.2 <i>Regulation and online gambling</i>	68

4.6 PROSECUTING CYBERLAUNDERING	69
4.6.1 General	69
4.6.2 Privacy concerns	70
4.6.3 The question of jurisdiction	72
<b>CHAPTER FIVE: EVALUATION</b>	<b>75</b>
5.1 THE PRESENT: AN OVERVIEW	75
5.2 THE FUTURE: A PROGNOSTIC SURVEY	76
5.3 RECOMMENDATIONS	79
5.3.1 Bringing cyberlaundering to the centre stage	79
5.3.2 Better policing	80
5.3.3 Extending the FATF's term to 2012	81
5.4 CONCLUSION	82
<b>LIST OF REFERENCES</b>	<b>84</b>
<b>ANNEXURE</b>	<b>101</b>



## DECLARATION

I, Daniel A. Leslie, hereby declare that this dissertation is original. It has never been presented to any other university or institution. Where other people's ideas have been used, proper references have been provided. Where other people's words have been used, they have been quoted and duly acknowledged.

Student: Daniel A. Leslie

Signature: \_\_\_\_\_

Date: \_\_\_\_\_



Supervisor: Prof (Dr) Lovell Fernandez

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

## DEDICATION

To my late father, Sunday Idowu Leslie, who remains my greatest inspiration.



## ACKNOWLEDGEMENT

First and foremost, I would like to thank my heavenly father for putting me in this humbling position, and for the mental prowess, agility and strength to undertake this research, which is nothing short of a manifestation of His divine help and providence.

I would also like to thank Professor (Dr) Lovell Fernandez. He is, unquestionably, a positive instigator and an inspiration to me. His impeccable reasoning, sound guidance and insatiable wisdom make him an excellent supervisor, and any student would be fortunate to be under his supervision. I have jealously drawn from his wealth of knowledge and experience in “moulding” this research. For this I am truly grateful.

My heart goes out to the entire co-ordinators of the Transitional Criminal Justice and Crime Prevention programme at the University of the Western Cape and the partners at Humboldt Universitat zu Berlin. These persons include Professor (Dr) Gerhard Werle, Dr Raymond Koen, Dr Moritz Vormbaum and Paul Bornkamm, to name just a few. In the first place, to have been considered for this wonderful programme is a blessing. This has afforded me the opportunity to embark on this journey.

Last but certainly not least, I am grateful to my family. It is often said that no man is an island. I am in this position today because I have wonderful, loving, caring and supportive family. I am eternally grateful to my mother Margaret Modupe Leslie for her constant prayers and undying love for me. I am also grateful to my late father, Hon. Justice (Dr) Sunday Idowu Leslie who was nothing short a wonderful father and an exceptional role model. I thank my siblings Kayode, Tayo, Yetunde, Bimbo, Vera,

Kenneth, Buki and Bolanle Leslie for always being a shoulder to lean on. You all will always have a special place in my heart.



## ABSTRACT

This paper is inspired by the ills borne out of the internet. The internet has become a modern day tool for criminals seeking to conceal the proceeds derived from their crime, hence the problematic notion of cyberlaundering. This paper journeys through the world of cyberlaundering by looking into the structure of the crime in great depth. It explores various possibilities, and tries to hatch out viable solutions to the dilemma.



## KEY WORDS

Cyberlaundering

Cyber crime

E-payments

E-money

Electronic Payment Technologies (EPT)

Financial Action Task Force (FATF)

Information Communication Technology (ICT)

Internet

Money laundering

Non-Compliant Countries and Territories (NCCTs)



**LIST OF ABBREVIATIONS**

AML	Anti-Money Laundering
DEA	Drug Enforcement Agency
EPS	Electronic Payment Systems
EPT	Electronic Payment Technologies
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FinCEN	Financial Crimes Enforcement Network
ICE	Immigration and Customs Enforcement
ISPs	Internet Service Providers
NAB	National Accountability Bureau
NCCTs	Non-Compliant Countries and Territories
SL	Second Life
SOCA	Serious Organised Crime Agency

## CHAPTER 1

### MAPPING THE TERRAIN

#### 1.1 INTRODUCTION

The advent of the internet could be rightly deemed a miracle. The ease at which everyday life is run can be majorly ascribed to this specie of technology which has been engrained in our lives. With its rising availability, the internet is steadily becoming a common luxury for all.<sup>1</sup> Be it personal or business, the internet has formed an indispensable tool upon which most organizations (whether public or private) are built. However, the wonder of the internet has yielded a new breed of vices in the society. Cyberlaundering is sadly one of such. The term cyberlaundering refers to how illegal proceeds of crime are laundered using the internet in order to make such illegal proceeds appear “clean.” This very novel form of cyber crime is characterised by evasiveness. As it is an untrodden path, not much research has been done on it. This paper thus seeks to investigate the structure of this crime, with a view to finding effective regulatory and control mechanisms.

At the G-7 summit on 14 July 1989 in Paris, the Financial Action Task Force (FATF)<sup>2</sup> was established. The FATF issued Forty Recommendations amongst which is

---

<sup>1</sup> In 2009, it was reported that about 70% of all households in the United Kingdom had internet at home compared to a miserly 54% in 2006. See <<http://www.statistics.gov.uk/CCI/nugget.asp?ID=8&Pos=1&ColRank=1&Rank=192>> [accessed on the 15<sup>th</sup> of March, 2010].

<sup>2</sup> The FATF is an inter-governmental body with the purpose of combating money laundering and terrorist financing. See paragraph 4.3.2.1.

the appeal to expand the coverage of the Anti-Money Laundering (AML) regime to lawyers, auditors, accountants and other legal structures that are sometimes used to disguise the beneficial owners of assets.<sup>3</sup> This fact is premised on the reality that the AML regime had previously been the task of economists and the like. As an impetus for undertaking this research, it becomes imperative within the global pandemonium caused by the advent of cyberlaundering to explore the measures that can be taken against cyberlaundering from both a practical and a legal standpoint.

## **1.2 THE PROBLEM OF CYBERLAUNDERING: SIGNIFICANCE OF RESEARCH**

This paper is inspired by the ugly reality of cyberlaundering facing the modern world. While most societal ills result from very glaring incidents, cyberlaundering - the inconceivable specie of money laundering, is apparently doing more damage than one can physically envisage. The answer to the frequently asked question – “just how much money is annually laundered in the world today?” appears to be a riddle of some sought. Till date no one knows precisely. It has been estimated that about \$3 trillion is laundered annually.<sup>4</sup> This figure is not only realistic, but is likely to triple with the fast spread of cyberlaundering practices. In 1999, the FATF indicated in its report that the internet

---

<sup>3</sup> See recommendations 12 and 16, Financial Action Task Force (2003: 15).

<sup>4</sup> See Lilley (2006: 40) and Robinson (1998: 16). As at 1998 the amount of money that is laundered annually was estimated to be about \$300 billion. See Robinson (1998: 16). Also see Singh (2009: 3) where it is indicated that the average amount of money laundered in the world could be between two and five per cent of the world's gross domestic product.

poses a threat, and might very well fuel money laundering activities.<sup>5</sup> We are currently witnessing the dawn of this reality.

Also, considering the rampant nature of this crime, particularly in most of the poor countries, there is a crippling effect on the economy. It is sad to note that most of the monetary aid given to these countries by charity organizations and governments of the western world, never actually see the light of day.<sup>6</sup> Due to the poor technological framework in these countries, there is poor accountability for these funds. One might ask, where do all the funds go? The answer lies in the reality of money laundering, which invariably links with the issue of poor governance.<sup>7</sup> With the growing awareness of the internet's capabilities, the sky is the limit for criminals seeking to conceal their illegal proceeds.<sup>8</sup> Given the fact that cyberlaundering has a potentially detrimental effect on the economy, the investigation of this new kind of crime becomes of paramount importance.

What is more, cyberlaundering is a lucrative enterprise for terrorist financing. The attacks by Al-Qaeda in New York City, on September 11 2001, spawned this reality.<sup>9</sup> After the attacks, the United States government and financial organisations have been forced to conduct intense investigations about the medium adopted by terrorists to finance their operations. The internet has been constantly identified as the most plausible medium.<sup>10</sup>

---

<sup>5</sup> Financial Action Task Force (2002: 23).

<sup>6</sup> See <[http://www.fact-finder.com/file/money\\_laundering/](http://www.fact-finder.com/file/money_laundering/)> [accessed on 31 July 2010].

<sup>7</sup> Blunden (2001: 29).

<sup>8</sup> Blunden(2001: 30).

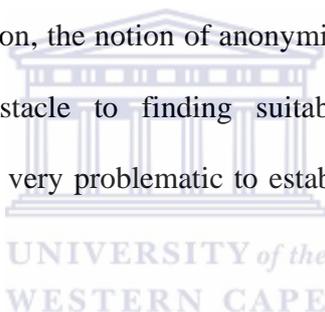
<sup>9</sup> Financial Action Task Force (2010A: 32).

<sup>10</sup> Kellerman (2004: 4).

This paper thus has an overall purpose of shedding light on this very grey area of the law. It also serves an educational purpose by highlighting the principal challenges which cyberlaundering practices present.

### 1.3 RESEARCH QUESTIONS

Cyberlaundering has proven to be a safe haven for money launderers. In lieu of the novel nature of this crime, it becomes crucial to first understand the kind of devil one is dealing with. An understanding of this crime is thus the first wall that this paper attempts to scale. In addition, the notion of anonymity, which is the very nucleus of the internet, is a major obstacle to finding suitable remedies to the problem of cyberlaundering. It is also very problematic to establish jurisdiction in the event that a cyberlaunderer is caught.

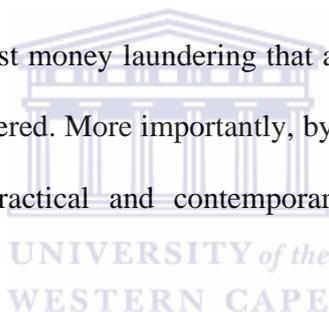


Therefore, based on these very glaring problems, this paper seeks answers to the following questions:

- I. What is cyberlaundering and what does the phenomenon entail?
- II. Are there possible remedies to the cyberlaundering problem?
- III. Who would have prosecutorial jurisdiction in the event that a cyberlaunderer is caught?

## 1.4 SCOPE OF RESEARCH

The concept of cyberlaundering is evolving fast. It appears as if certain countries that are fully compliant with the recommendations of the FATF might be able to deter its spread as a result of their seemingly effective anti-money laundering (AML) regimes.<sup>11</sup> The problem of cyberlaundering is, however, intensified in most countries with very poor AML regimes. These are mostly countries formerly deemed as non-compliant countries and territories (NCCTs) by the FATF.<sup>12</sup> Thus, the scope of this research covers cyberlaundering activities in the latter category of countries, together with certain fully compliant countries with effective AML regimes. The relevant regulatory measures against money laundering that are in place in the latter category of countries would be considered. More importantly, by identifying the various contours of cyberlaundering, some practical and contemporary regulatory measures would be considered.



## 1.6 LITERATURE REVIEW

As a basic foundation, some international instruments are crucial to this paper's enquiry.<sup>13</sup> These international instruments have been analysed. Although the concept of

---

<sup>11</sup> For a list of these countries see the Financial Action Task Force (2002: 11). Also see Lilley (2006: 121).

<sup>12</sup> Although as of 13 October 2006, the FATF reports that there are no more NCCTs, most of the delisted countries from the list of NCCTs are still closely monitored by the FATF. Some of these countries include Cook Islands; The Dominican Republic; Egypt; Grenada; Guatemala; Indonesia; Marshall Islands; Myanmar; Nauru; Nigeria; Niue; Philippines; Russia; St. Vincent and the Grenadines; and Ukraine. See Financial Action Task Force (2002: 7).

<sup>13</sup> These are: The UN Convention against the illicit Traffic in Narcotic Drugs and Psychotropic Substances, signed on 20 December 1988 and came into force on 1 November 1990. The Warsaw Convention: Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, 16.V, (May, 2005); The EU Convention on Cybercrimes 23.XI, adopted on 12 April 2001 and came into force on July 2004; the United Nations

money laundering as a crime itself is relatively new, unlike cyberlaundering, there have been several publications on the subject. Some of these have also been considered.<sup>14</sup> Several commentary articles on cyberlaundering have also been examined.<sup>15</sup>

There has not been a reported case law dealing explicitly with cyberlaundering. For this reason, factual accounts of cyberlaundering activities, as available on the internet and other media outlets have been studied. Some highly informative internet materials have been consulted as well.<sup>16</sup>

Thus, this research stems from the principles of money laundering as generally understood, and it basically builds on existing knowledge of cyberlaundering as proffered in some publications.

---

Convention against Transnational Organized Crime, Resolution 55/25, (adopted on 15 November 2000, and came into force on 23 September 2003) and the Financial Action Task Force “40 Recommendations, plus Nine Special Recommendations” which was issued on 23 June 2003 (available at <[http://www.fatf-gafi.org/forty\\_recom/pdf](http://www.fatf-gafi.org/forty_recom/pdf)> [accessed on the 5<sup>th</sup> of March, 2010].

<sup>14</sup>See Beare, ME (2005) *Critical Reflections on Transnational Organized Crime, Money Laundering and Corruption* University of Toronto Press: Toronto; Hinsterseer, K (1997) “An Economic Analysis of Money Laundering” *Journal of Money Laundering Control* 1, 154; Lilley, P (2006) *Dirty Dealing, The Untold Truth About Global Money Laundering, International Crime and Terrorism* (3<sup>rd</sup>), London: Kogan Page; Madinger, J (2006) “Basic Money Laundering Schemes” in Madinger, J *Money Laundering: A Guide for Criminal Investigators* (2nd ed) Taylor and Francis: Boca Raton; Reuter P and Truman, (2004) *EM Chasing Dirty Money: The Fight Against Money Laundering* Peterson Institute for International Economics: Washington DC; Richards, JR (1999) “An Introduction to Money Laundering” in Richards JR *Transnational Criminal Organizations, Cybercrime, and Money Laundering* CRC Press: Boca Raton, and Shams, H (2004) “Money Laundering Law: History and Scope” in Shams, H *Legal Globalization: Money Laundering Law and Other Cases* British Institute of International and Comparative law: London.

<sup>15</sup> See *inter alia*: Bortner, M (1996) “Cyberlaundering: Anonymous Digital Cash and Money Laundering” <<http://osaka.law.miami.edu/~froomkin/seminar/papers/bortner.htm>> [accessed on 12 April 2010]; Grabosky, P and Smith, R (1998) *Crime in the Digital Age, Controlling Telecommunications and Cyberspace Illegalities* The Federation Press: Sydney; Marshall, CE et al (2005) “Computer Crime in Brave New World” in Reichel, P *Handbook of Transnational Crime and Justice* Sage: Los Angeles; Philipson, S (2001) “The Dangers of New Technology - Laundering on the Internet” 5(1) *Journal of Money Laundering Control Thomason* 89; Ping (2004) “New Trends in Money Laundering – From the Real World to Cyberspace” 1(5) *Journal of Money Laundering Control* 50 and Thomason, CV (2009) “How has the establishment of the internet changed the way offenders launder their dirty money?” *Internet Journal of Criminology* <<http://www.internetjournalofcriminology.com>> [accessed on 16 March 2010].

<sup>16</sup> These include: eHow (2009) “How to Launder Money” <[http://www.ehow.com/how\\_2049841\\_launder-money.html](http://www.ehow.com/how_2049841_launder-money.html)> [accessed on 5 March 2010], Financial Action Task Force (1997) “1996-1997 Report on Money Laundering Typologies” <<http://www.fatf-gafi.org/dataoecd/31/29/34043795.pdf>> [accessed on 5 March 2010], and Financial Action Task Force (2002) “FATF Annual Report for 2001-2002 Released” <<http://www.fatf-gafi.org/dataoecd/43/53/34949558.pdf>> [accessed on 5 March 2010].

## 1.7 METHODOLOGY

This research has been conducted pragmatically, on the basis of available resources. Primary and secondary sources have been used.<sup>17</sup> The quantitative and qualitative secondary sources that have been considered are books, articles, journals, official publications and the internet, along with media articles.



---

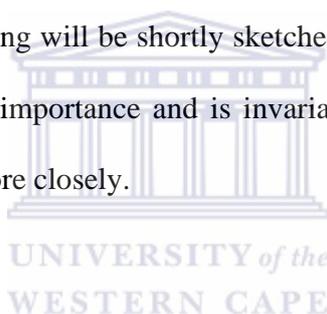
<sup>17</sup> See complete outline in the list of references.

## **CHAPTER 2**

### **A BACKGROUND ON MONEY LAUNDERING: THE PRE-INTERNET ERA**

#### **2.1 GENERAL**

Although the principal focus of this paper is cyberlaundering, it is important to understand the concept of money laundering which forms the foundation upon which cyberlaundering (as it's subset) is built. A brief history of money laundering and the process of money laundering will be shortly sketched. However, because the concept of wire transfers is of great importance and is invariably linked to cyberlaundering, this chapter will focus on it more closely.



#### **2.2 THE CONCEPT OF MONEY LAUNDERING**

##### **2.2.1 Defining money laundering**

There are several ways in which money laundering can be defined. Sometimes money laundering is defined as it pertains to the legal jurisdiction or the relevant context within which one operates. This has caused great disparities with its precise definition.<sup>18</sup>

---

<sup>18</sup> For instance, in the United States, money laundering is generally defined as the practice of disguising illegally obtained funds so that they seem legal. See Lilley (2006: 10). On the other hand, in the United Kingdom, it refers to any financial transaction which generates an asset or value as the result of an illegal act like tax evasion, or false bookkeeping (therefore a predicate offence). See Hinterseer (1997: 154). In India, it is any process connected with the proceeds of crime and projecting it as untainted property. See Pillai & Julian (2008: 6).

An encompassing definition by the Organisation for Economic Cooperation and Development (OECD) is as follows:

‘Money laundering is the attempt to conceal or disguise the ownership or source of the proceeds of criminal activity and to integrate them into legitimate financial systems in such a way that they cannot be distinguished from assets by legitimate means. Typically, this involves the conversion of cash-based proceeds to account-based proceeds.’<sup>19</sup>

The underlying purpose of money laundering is to reduce the risk of confiscating illegal proceeds, so that the launderer can spend and enjoy the profits easily. This rationale is key to the concept of cyberlaundering. This fact is further elucidated by the FATF’s definition of money laundering. It defines it as the processing of criminal proceeds to disguise their illegal origin.<sup>20</sup> From this basis, the meaning of cyberlaundering can be deduced. Cyberlaundering, in simple terms, means using the mechanism of the internet to launder “dirty money.” A better understanding of cyberlaundering and how it operates is provided in the following chapter.

### **2.2.2 A brief history of money laundering**

The history of money laundering has long been associated with certain individuals like Al Capone, Meyer Lansky and Frank Abegnale, amongst a slew of other notorious

---

<sup>19</sup> See the Organisation of Economic Cooperation and Development (2002) “Glossary of statistical terms” <<http://www.bis.org/publ/cpssoob.pdf>> [accessed on 23 March 2010].

<sup>20</sup> Organisation of Economic Cooperation and Development (2001: 2).

fraudsters in the 20<sup>th</sup> century.<sup>21</sup> However, these individuals were not exactly charged with money laundering. The term “money laundering” was first used during the Watergate scandal in the United States which led to the impeachment of President Richard Nixon.<sup>22</sup> However, the advent of money laundering as a crime can be traced back to the Bank Secrecy Act,<sup>23</sup> which was enacted in the United States. The Bank Secrecy Act is significant because it introduced the “Know Your Customer” (KYC) principle, in terms of which financial institutions are required to scrutinize their customers and keep records of their transactions.<sup>24</sup> Also, certain reporting requirements were enshrined in the Act, like the reporting of all transactions exceeding \$10,000 and transfer of value exceeding \$5000.<sup>25</sup>

Another significant legislative enactment is the Money Laundering Control Act of 1986,<sup>26</sup> which was adopted in the US as a response to the shortcomings of the Bank Secrecy Act. The unfortunate consequence that resulted from the stringent provisions of the Bank Secrecy Act was the act of smurfing.<sup>27</sup> In terms of the Money Laundering

---

<sup>21</sup> Al Capone was prosecuted by the United States government for tax evasion and fraud in the 1940s. Meyer Lansky, or the so-called “mob’s accountant,” was notorious for siphoning funds with Swiss Bank accounts in the 1960s and 1970s. Frank Abagnale was the so-called “gangster-turned-saint” whose very fraudulent and evasive ways in the 1970s and 1980s later became a valuable asset for the FBI, for which he later worked. See Madinger (2006: 43) and Robinson (1998:12).

<sup>22</sup> The Guardian newspaper, which reported on the scandal, used the word “laundering” to refer to how President Nixon and the members of his campaign team moved money from the United States to Mexico. See <[http://www.wikipedia.com/money\\_laundering/](http://www.wikipedia.com/money_laundering/)> [accessed on 20 August 2010].

<sup>23</sup> Act 31 of 1970, C.F.R.

<sup>24</sup> See section 100 of the Act.

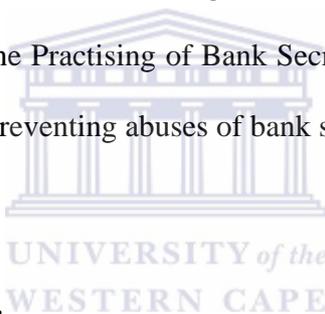
<sup>25</sup> See sections 101 and 221 of the Act. At the time, the constitutionality of the Act was contested in the case of *California Bankers Association v Schultz*, 39 L Ed 2d 812 (1974). However, the Act was later upheld as constitutional in the decision of the US Supreme Court (416 US. 21 1974). See Bortner (1996: 2).

<sup>26</sup> Act 18 of 1986, U.S.C.

<sup>27</sup> The term smurfing refers to a structured deposit system in terms of which a launderer (or “smurf”) deliberately deposits money below the reportable threshold into various accounts. This is purposely done to evade suspicion, because deposits of that precise amount or above would require the filing of a cash transaction report (CTR). There could be either one or multiple smurfs involved in this operation. Filipkowski (2008: 6).

Control Act, failure to comply with the reporting requirements laid down by the Bank Secrecy Act is criminalised.<sup>28</sup> This legislation also adopted the filing of currency transaction report (CTR) by banks. The Act is still very relevant today.

Several other legislative landmarks are important to the evolution of the anti-money laundering (AML) regime. In May 1973, a treaty called the U.S.–Switzerland Mutual Legal Assistance on Criminal Matters,<sup>29</sup> was concluded. It catapulted money laundering into the international arena, even though only to limited extent, by creating the necessary awareness of procedural terms for dealing with it at law. In July 1977, Swiss Banks in Switzerland concluded the “Agreement on the Observance of Care and Accepting Funds and on the Practising of Bank Secrecy,” which secured the expanding Swiss financial sector by preventing abuses of bank secrecy.<sup>30</sup>



### **2.2.3 The money laundering process**

Money laundering could be deemed to be a theatre of disguise involving various actors, roles and sequences. Some find the act of money laundering very synonymous with the process of laundering dirty clothes; the washing, drying and ironing stages.<sup>31</sup> Its complexity has often led to its division into the placement, layering and integration stages.<sup>32</sup> The next chapter looks at these stages in greater detail, because cyberlaundering also follows the same pattern.

---

<sup>28</sup> See Section 103(2).

<sup>29</sup> The treaty was enacted on May 25 1973 and came into force on January 23 1977.

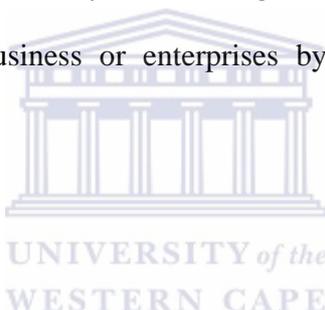
<sup>30</sup> See Articles 3-7 of the agreement.

<sup>31</sup> Singh (2009: 6).

<sup>32</sup> See Hinterseer (1997: 154).

The placement stage refers to the initial stage where funds derived from illegal activities are moved to a place (usually a traditional or non-traditional financial institution) convenient for the launderer and less suspicious to law enforcement agencies.<sup>33</sup> The layering stage refers to the process whereby the money is separated from its true origin to feign legitimacy. The criminal usually disguises the ownership of the funds by scattering these proceeds across the commercial sphere. The layering process is especially crucial to the cyberlaundering process.<sup>34</sup>

Otherwise known as the final process in the money laundering cycle when the clean clothes are taken out of the dryer, the integration phase entails converting illegal proceeds to legitimate business or enterprises by way of financial or commercial operations.<sup>35</sup>



#### **2.2.4 Conventional money laundering mechanisms**

The concept of money laundering is a constantly evolving phenomenon, and criminals constantly seek out avenues to hide the proceeds of crime from law enforcement agencies. The most recent avenue, which is cyberlaundering, is the subject of this paper. Prior to the internet era, criminals commonly used shell companies,<sup>36</sup> cash

---

<sup>33</sup> Financial Action Task Force (2010B: 23).

<sup>34</sup> See paragraph 3.3.3 below.

<sup>35</sup> See Shams (2004: 23) and Hinterseer (1997: 91).

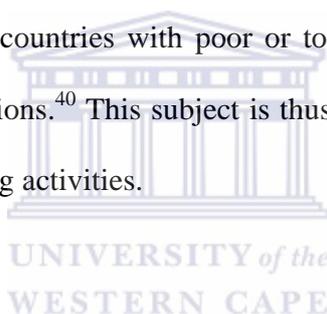
<sup>36</sup> Shell companies operate under the guise of corporate entities conducting legitimate businesses, while in reality they have no assets and are inoperative. However, some of these companies do partly conduct legitimate businesses. Money launderers hide the proceeds of their crimes under these front companies, which are now rampant on the internet. See Madinger (2008: 65).

smuggling,<sup>37</sup> illicit third party influences,<sup>38</sup> and smurfing,<sup>39</sup> amongst several other methods.

## **2.3 WIRE TRANSFERS: A SHIFT FROM THE HARD CASH SYSTEM**

### **2.3.1 General**

What is better known as the second milestone in the development of money laundering is the wire transfer system, which is the intermediate between the typical hard cash system and the internet-based system. Wire transfers are especially important for most underdeveloped countries with poor or totally non-existent internet facilities crucial for banking operations.<sup>40</sup> This subject is thus vital to the issue of regulating and controlling cyberlaundering activities.



### **2.3.2 The meaning of wire transfers**

Due to the advancement of technology, wire transfers originated in the 1970s and 1980s from banking institutions which sought the luxury and convenience of transferring funds without having to handle the cash physically. The wire transfer of money refers to the electronic transfer of funds (albeit its value) at the request of a

---

<sup>37</sup> This is arguably the oldest and simplest form of money laundering. It is a placement system in terms of which bulk cash is shipped across the border via either a cargo or other means. See Reuters and Truman (2006: 49).

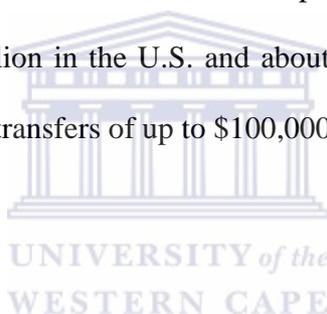
<sup>38</sup> A typical example is the so-called "hawala" system. This is common in most European and Asian countries. In terms of this system, a person (who is usually not a citizen of the country where he is resident) sends out money internationally to persons in another country. Instead of the traditional banking avenue, an intermediary is used who physically gives the money to the recipient at a lower commission to that which a bank would charge. See Singh (2009: 6).

<sup>39</sup> See footnote 25 supra.

<sup>40</sup> See Zeldin and Florio (2007: 187) for more details.

customer from one bank account to a beneficiary account, which is usually another bank. A wire transfer can either be effected locally or internationally.<sup>41</sup> Since the transferred funds are electronic in nature, only the actual value of the funds is transferred.

In the past, wire transfers were effected by cable. Today banks do this electronically. The popular method by which funds are electronically transferred (internationally) is through an electronic funds messaging service called the Society for Worldwide Interbank Financial Telecommunications (SWIFT).<sup>42</sup> SWIFT is primarily used to process significantly high transactions. For example, SWIFT is used to process credit payments of up to \$2 million in the U.S. and about R5 million in South Africa.<sup>43</sup> It is also used to process debit transfers of up to \$100,000 in the U.S. and R500, 000 in South Africa.<sup>44</sup>



### **2.3.3 The problem with wire transfers**

Money launderers have found a loophole in the SWIFT messaging system. When filing the forms, banks are generally required to fill out certain mandatory fields on the form with certain basic information of the originator (person giving the instruction) such as the account number, the originator's name and address, and beneficiary details. Herein lies the problem. Although the wire transfer will be rejected if these mandatory

---

<sup>41</sup> Pillai and Julian (2008: 219). Also see Reuter and Truman (2006: 34).

<sup>42</sup> Although other electronic funds message service exists, SWIFT is the most popular. About 2,600 banks throughout the world, in over 65 countries, are part of the SWIFT service. See eHow "How SWIFT wires funds" <<http://www.ehow.com/swift/>> [accessed on 4 June 2010].

<sup>43</sup> Pillai and Julian (2008: 219).

<sup>44</sup> Pillai and Julian (2008: 220). See also Financial Crimes Enforcement Network (2009: 43).

fields are not populated, should the mandatory fields be filled in with any type of characters, the wire transfer would succeed. This helps money launderers because they can easily provide false information. Verification of this data is in many instances not done, or poorly done, thereby frustrating the work of law enforcement agencies in the process. This situation is further compounded by the fact that many countries have still not reached the acceptable standard of compliance in terms recommendations 10 (record keeping) and 11 (unusual transactions) of the FATF's "40 Recommendations."<sup>45</sup>

#### **2.3.4 A bridge between wire transfers and cyberlaundering**

The mechanisms available to individual countries for regulating illicit financial dealings are ultimately decisive. It is for this reason that the FATF was established in 1989. There is no doubt that several distinct problems and challenges inherent in various countries are stumbling blocks to the creation of a comprehensive and stringent anti-money laundering (AML) regime. In most democratic countries, money launderers take advantage of the highly revered privacy rights which they use to circumvent the reporting and information requirements stipulated by numerous AML laws. In this respect, cyberlaundering bears a great similarity to wire transfers because they both share a similar challenge. The only difference is the fact that cyberlaundering is causing far greater damage compared to wire transfers. With the rapid growth of technology and

---

<sup>45</sup> See the Financial Action Task Force (2003: 20). South Africa is a good example. Regardless of the stringent laws enacted by the South African government against laundering activities, the FATF still deems the South African government partially compliant with its recommendations. See E-Standard Forum (2009: 12). Very few countries such as the U.S. and Germany are considered to be fully compliant with those recommendations.

the internet in most underdeveloped countries, money launderers who are using the avenue of wire transfers are upgrading to the channel of cyberlaundering.



## **CHAPTER 3**

### **CYBERLAUNDERING**

#### **3.1 GENERAL**

This chapter sets out to unravel the structure of cyberlaundering. In doing this, it will contribute to a better understanding of how cyberlaundering works.

#### **3.2 THE CONCEPT OF CYBERLAUNDERING**

##### **3.2.1 The meaning of cyberlaundering**

Cyberlaundering is a system in terms of which the mechanism of the internet is used to hide funds derived from illegal activities in order to make such funds less traceable and less suspicious to law enforcement agencies. This new breed of money laundering was heralded by the exponential increase of electronic finance (e-finance) since the late 1990s.<sup>46</sup>

##### **3.2.2 E- money**

Although the notion of cyberlaundering is a concept that stems from the advent of the internet, the very root of the problem is the reality of electronic money. Electronic money (otherwise called e-money) refers to an internet based system of legal tender

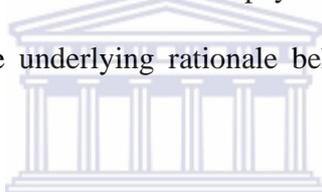
---

<sup>46</sup> Kellerman (2004: 2).

which does not take the form of currency notes, but instead takes the form of certain electronic impulses of 1s and 0s (also referred to as digital bits).<sup>47</sup> One might ask, why e-money? For a cyberlaunderer, several reasons exist why e-money is advantageous:<sup>48</sup>

1. E-money is faster to transfer.
2. E-money is faster to circulate from one geographical account to another.
3. It is easier to hide from law enforcement agencies.
4. It is easier to invest in illegitimate businesses.

According to the Financial Crimes Enforcement Network (FinCEN),<sup>49</sup> e-money is advanced through various different electronic payment mediums (or Electronic Payment Technologies- EPTs). The underlying rationale behind the use of EPTs is explained thus:<sup>50</sup>



‘The common element is that these systems are designed to provide the transacting party with immediate, convenient, secure and potentially anonymous means by which to transfer financial value. When fully implemented, this technology will impact users world-wide and provide readily apparent benefits to legitimate commerce; however, it may also have the potential to facilitate the international movement of illicit funds.’

---

<sup>47</sup> See Ask “E-Payments” <[http://www.ask.com/what is e-money?/ files/e\\_payment\\_methods/](http://www.ask.com/what%20is%20e-money?/files/e_payment_methods/)> [accessed on 8 June 2010]. See also Molander, et al (1998: 2).

<sup>48</sup> Pillai and Julian (2008: 99).

<sup>49</sup> This is the financial intelligence centre of the US Department of Treasury. It is one of the major enforcement agencies put in place by the US government to regulate and control financial crimes. See the Financial Crimes Enforcement Network (2009: 20).

<sup>50</sup> Financial Crimes Enforcement Network (an undated website document) “Money in Cyberspace” <<http://www.fincen.org/resource-moneyincyberspace/1212>> [accessed on 17 June 2010].

### 3.2.2.1 *Smart cards*

Today, when transacting on the internet, various internet service providers (ISPs) use different EPT systems for making payments. However, of these various types, smart cards are clearly the most efficient and common means of obtaining electronic cash. Smart cards are generally easy to use. One can credit the card with funds and then use it as either a debit card or a credit card, depending on the purpose the user has in mind.<sup>51</sup> A better explanation is the following:

‘A smart card looks much like a credit card. Consumers purchase smart cards and load them with electronic money at a vending machine, bank, Automated Teller Machine, personal computer (over the Internet), or through a specially equipped telephone. Once the e-cash is loaded on the card, the money can then be spent over the Internet or through other communication devices.’<sup>52</sup>

The main cause of concern with smart cards is primarily the method by which money is transferred onto the card. Generally speaking, a smart card can be loaded telephonically, or at an ATM machine, or by a direct online transfer from one’s bank account, or from the hard drive of one’s computer, or from cyberspace (in which case, the money is usually stolen),<sup>53</sup> or either by some form of electronic wallet (e-wallet) via which funds can be moved from one card to another.<sup>54</sup> This is where the popular MONDEX card, which is part of MasterCard International, has an advantage, for it

---

<sup>51</sup> See Reuter and Truman (2006: 123).

<sup>52</sup> The United States Government Accounting Office (2009: 78).

<sup>53</sup> An example would be where a criminal acquires monetary value by stealing another’s details like a credit card or account number. This is called identity theft.

<sup>54</sup> The United States Government Accounting Office (2009: 78).

permits the free and easy transfer of funds from one person to another, doing away with the complexity of other smart cards that require transactions to be reported to a central computer system.<sup>55</sup> This very fact strikes at the heart of cyberlaundering.<sup>56</sup>

Also, the PayPal card is another kind of smart card which opens up an avenue for money laundering because, just as with most other kinds of smart cards, it does not require one to have a bank account. Persons with false identities can therefore possess it. Interestingly, gift cards, which are often used by most departmental stores, are now being used by cyberlaunderers, because it is just another form of smart card.

The use of smart cards, just like other electronic cash systems which facilitates e-money, often circumvents the Know Your Customer (KYC) procedures, because majority of internet service providers (ISPs) are unscrupulous about their customers. Most online applications by customers for an e-money account, which usually requires the customer to provide certain personal information, are not verified by these ISPs. For example, the Freedom Eagle Cash Card, which is predominant in the United Kingdom, does not require any kind of identification from potential customers. New customers can thus purchase it online within minutes. Also, this kind of smart card can be recharged repeatedly, with no actual limit on the value stored on the card.<sup>57</sup> A cyberlaunderer could not be more content with such an unfettered payment system.

---

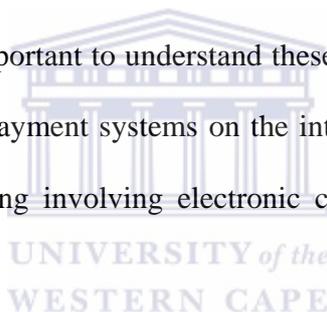
<sup>55</sup> See <<http://www.mondexcard.com/about/file838/>> [accessed on 17 June 2010].

<sup>56</sup> This was noted by Stanley Morris (the director of FinCEN) in his 1995 speech to the Congress Banking committee, available at <<http://www.fincen.org/resource>> [accessed on 17 June 2010].

<sup>57</sup> For more details see <<http://www.freedom-card.co.uk/>> [accessed on 2 September 2010].

### 3.2.3 Models of cyberspace payment systems

The business of a cyberlaunderer flourishes due to the anonymity feature of e-money. The mere fact that money is represented in digital bits makes the identity of the launderer undetectable. Since the internet facilitates cyberspace payments, another key consequence of the anonymity feature is the fact that it defies jurisdictional barriers. Funds can be moved from one jurisdiction to another without regulation and interception. The World Bank identifies four concrete cyber-based payment systems promoting money laundering capabilities.<sup>58</sup> These are the Merchant-Issuer model, the Bank-Issuer model, the Non-Bank and Peer-to-Peer models. The latter two models are most problematic. It is important to understand these models because they represent the different possibilities of payment systems on the internet. They consequently represent the core of cyberlaundering involving electronic cash (or e-cash). These models are briefly discussed below.



#### 3.2.3.1 *The Merchant-Issuer Model*

This model entails a scenario where both the issuer of a smart card, or pre-paid card, and the seller of goods are the same. Good examples are the Oyster card<sup>59</sup> used by the Transport of London, Barclaycard,<sup>60</sup> Visa card<sup>61</sup> and the Octopus card<sup>62</sup> used by the

---

<sup>58</sup> Kellerman (2004: 3).

<sup>59</sup> See <<http://www.tfl.gov.uk/oyster/>> [accessed on 12 September 2010].

<sup>60</sup> See <<http://www.barclaycard.co.uk/>> [accessed on 1 August 2010].

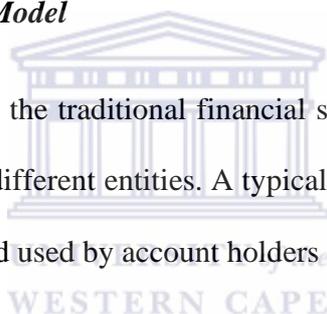
<sup>61</sup> See <<http://www.visa.com/>> [accessed on 19 August 2010].

<sup>62</sup> See <<http://www.octopuscards.com/>> [accessed on 24 August 2010].

Hong Kong transit system.<sup>63</sup> However, some merchants under this category could also be the operators of illegitimate businesses. For example, these merchants could be an organized crime syndicate, or might be operating a business online which conducts criminal activities. These merchants often try to conceal their identities from law enforcement officers. Research has shown that the majority of these companies are registered in certain strategic locations such as Costa Rica, Curacao, Antigua and Cyprus.<sup>64</sup>

### ***3.2.3.2 The Bank-Issuer Model***

This model is based on the traditional financial system where the issuers and sellers or merchants are entirely different entities. A typical case is the common bank-customer relationship. The debit card used by account holders of banks is a very good example.



### ***3.2.3.3 The Non-Bank Issuer Model***

This model is very problematic because it is factually common place among cyberlaunderers. In this case, users purchase e-cash from issuers using traditional cash. These users then proceed to conclude transactions with participating merchants who accept e-cash. The merchants would then redeem the traditional cash equivalent of the e-

---

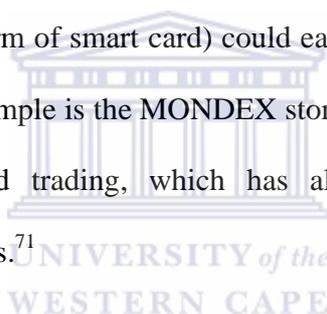
<sup>63</sup> Jamali (2009: 14).

<sup>64</sup> Reuter and Truman (2006: 124).

cash from the original issuers.<sup>65</sup> Examples of this sort are the electronic coin product of Cybercash,<sup>66</sup> the Virgin Card<sup>67</sup> and the Freedom Eagle Card.<sup>68</sup>

### 3.2.3.4 Peer-to-Peer Model

This is a more flexible payment system in terms of which e-cash is transferable between users, regardless of whether or not a bank or non-bank issued the e-cash. Because the e-card is transferable, the point of contact with payment via traditional cash is only when the e-cash is issued and when it is redeemed.<sup>69</sup> Therefore, a person who has an e-wallet (which is a form of smart card) could easily transfer funds to another friend who has the same. An example is the MONDEX stored value card.<sup>70</sup> A trendier example of this system is e-gold trading, which has also become a fertile ground for cyberlaundering operations.<sup>71</sup>



The dilemma which this system creates, as identified above, is basically that a money launderer could easily transfer funds from his or her e-wallet to an associate in a totally different jurisdiction who has the same. This appears fascinating because the transaction would reflect that it originates from another e-wallet provider company, and not from the issuer bank if originally issued by a bank.<sup>72</sup> A very complex trail could as well be

---

<sup>65</sup> Kellerman (2004: 3).

<sup>66</sup> See <<http://www.cybercash.com/about/file/>> [accessed on 9 June 2010].

<sup>67</sup> The Virgin pre-paid cards are especially popular in the USA, South Africa, UK and other parts of Europe. See <<http://www.virgin.co.uk/pre-paidcards/>> [accessed on 9 June 2010].

<sup>68</sup> See <<http://www.freedom eagle.com>> [accessed on 9 June 2010].

<sup>69</sup> Jamali (2009: 14).

<sup>70</sup> See <<http://www.mondex.com/about/>> [accessed on 9 June 2010]. Another very similar example is the PayPal funds transfer services. See <<http://www.paypal.com>> [accessed on 9 June 2010].

<sup>71</sup> See paragraph 3.4.5 below.

<sup>72</sup> See Reuter and Truman (2006: 125).

created where the initial launderer sends or transfers money to different e-wallets at different times.

### **3.3 THE CYBERLAUNDERING CYCLE**

#### **3.3.1 General**

Just as one would commonly find with the conventional system of money laundering, the cyberlaundering practice assumes a three-stage process which includes the placement, layering and integration stages.



#### **3.3.2 Placement**

The placement stage is an example of how e-money is often used. In this instance, the proceeds of crime in the form of e-money can be used to buy foreign currency or goods for the purpose of re-selling them.<sup>73</sup> E-money can also be exchanged from one person to another without an intermediary involved. This system is fostered by the feature of anonymity, which is the bedrock upon which cyberlaundering operations thrive. Thus, ‘e-money may be used to place dirty money without having to smuggle cash or conduct face-to-face transactions.’<sup>74</sup>

“Dirty money” can be placed using various techniques of cyberlaundering, primarily by way of using online casinos.<sup>75</sup> When a person gambles, or buys casino chips with

---

<sup>73</sup> Philippsohn (2001: 489).

<sup>74</sup> Philippsohn (2001: 490). Also see Jamali (2009: 14).

<sup>75</sup> See paragraph 3.4.4 below.

dirty money and wins, the casino refunds such a person in cash, thus legitimating the money. Also, e-gold appears to be a very lucrative avenue for placing dirty money.<sup>76</sup> Other methods of placement include transfers done from an ATM, transfers of values stored in one's hard-drive or email account, or sometimes telephonically.<sup>77</sup>

### 3.3.3 Layering

This stage represents the cyberlaunderer's attempt at an ultimate disguise. The money is separated from its true origin and spread or "layered" through different techniques. Online banking would be the most applicable cyberlaundering technique for this purpose. This stage also gives a clear example of how wired transfers bear relevance to cyberlaundering. As mentioned earlier,<sup>78</sup> the loophole that the wire transfer system creates is the poor CTR and other reporting requirements, which are evident. The result is that a person can use an online bank to open an account without providing his or her true personal information and without the bank authenticating such person's proof of identity.<sup>79</sup> A cyberlaunderer is thus able to open different bank accounts online with a false identity. Consequently, through this process, audit trails are not created as compared to the physical transfer of funds from one jurisdiction to another.

---

<sup>76</sup> See paragraph 3.4.5 below.

<sup>77</sup> As an example, an existing customer of a smart card company could call the company to reload an exhausted smart card.

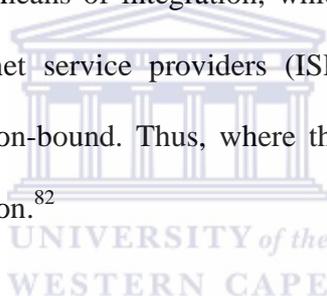
<sup>78</sup> See paragraph 2.3.3 supra.

<sup>79</sup> Jamali (2009: 14).

### 3.3.4 Integration

Here, the cyberlaunderer seeks to make the proceeds of crime legitimate by integrating them into the broad commercial market. The cyberlaunderer accomplishes this mainly by opening shell companies which ostensibly render different services. The company is called a “shell company” because services need not be rendered in that company as the company is created merely as a camouflage.<sup>80</sup> It would thus seem as though the payments that have been made are for services provided. Online casinos are good examples of this.<sup>81</sup>

Unlike the traditional means of integration, which primarily entail the use of false invoices of goods, internet service providers (ISPs) record more profits and their services are not jurisdiction-bound. Thus, where the funds are transferred by foreign banks, there is less suspicion.<sup>82</sup>



## 3.4 CYBERLAUNDERING METHODS AND TECHNIQUES

### 3.4.1 General

Although there are numerous avenues adopted and utilized for cyberlaundering purposes, it would be wise to confine one’s study to those techniques which are currently most prevalent. For this reason, this aspect focuses primarily on online

---

<sup>80</sup> Hinterseer (1997: 160).

<sup>81</sup> Filipkowski (2008: 6).

<sup>82</sup> See Jamali (2009: 14), and <[http://www.apacs.org.uk/resources\\_publications/card\\_facts\\_figurese.html](http://www.apacs.org.uk/resources_publications/card_facts_figurese.html)> [accessed 12 June 2010].

banking, digital payment methods, online casinos, online auction sites, online gambling and virtual communities.

### 3.4.2 Online banking

Online banking enables a customer of an internet-based bank to perform regular banking activities like account inquiries, payment of bills and transfer of funds, using the internet. With the click of a mouse and from the comfort of one's home, a customer can conclude certain transactions without being physically present at the bank. The advantages of banking online are amongst the numerous rewards that come with the advent of the internet. A recent study has shown that 97.7% of all the banks in the world today, regardless of where they are located, are now internet-based.<sup>83</sup> The world has clearly become a cyber hub.

The intricacies typical with online banking have caused it to be a "safe vehicle" for cyberlaunderers. Cyberlaunderers are having a fine ride with this technique. Online banking can be used to aid cyberlaundering in primarily two ways. Firstly, the ease at which an account can be opened on the internet at an internet-based bank is the first invitation to cyberlaunderers. The main catch here is that there is no authentic verification of the potential customer's identity. Therefore, the face-to-face check conducted when one banks in the conventional way is not performed. The true identity of the criminal seated at the other end of the computer remains unknown, and whatever information is provided for the opening of his or her account is the only evidence seen

---

<sup>83</sup> See <<http://www.wisegeek.com/what-is-online-banking92338/>> [accessed on 12 June 2010].

by the bank. Secondly, online banking is advantageous to the cyberlaunderer because it is the perfect avenue for smurfing. The layering stage of the cyberlaundering cycle can therefore be completed when the smurfs disperse the ill-derived funds to various other accounts by means of online banking.<sup>84</sup> The other twin tool that accords with this method is the use of smart cards. By way of the peer-to-peer payment system, and using an online bank, a criminal can move e-money from one card to another card in the possession of another person in cahoots with him. This is actually possible, given that the conventional banking “Know Your Customer” (KYC) principle, which requires banks to report suspicious transactions to law enforcement agencies, does not directly apply to online banks.<sup>85</sup>

Jurisdiction is the main reason why online banking cannot be easily regulated. The place where an online bank’s website is registered does not fall within the limits of any international standard regulating it.<sup>86</sup> It is still unclear which country would have jurisdiction where the website of an online bank is registered in a place different from where the customer operates.<sup>87</sup> Since such international norm is lacking, the gaping lacuna that exists as a result of online banking is made wider. To compound the situation, most countries still refuse to cooperate with one another in sharing intelligence on the matter.<sup>88</sup>

Furthermore, online banking is rendered prone to cyberlaunderers because of the complex encryption methods currently used by hackers on the internet. Hackers can

---

<sup>84</sup> See paragraph 2.2.4 supra.

<sup>85</sup> For more details see Filipkowski (2008: 6).

<sup>86</sup> Jamali (2009: 18).

<sup>87</sup> See discussion in paragraph 4.6.3 below.

<sup>88</sup> Filipkowski (2008: 9).

encrypt certain programs to transfer funds electronically from one bank account to another without leaving a trail behind for law enforcement agencies.<sup>89</sup> Furthermore, these hackers make use of special information retrieving viruses to steal the bank details of other bank customers such as their credit card numbers. This is termed identity theft. A cyberlaunderer could use the stolen information when conducting certain banking operations online.<sup>90</sup> The current trend is for criminals to purchase fake identities from hackers for the purpose of opening a bank account online which would eventually secure the placement and layering stages of cyberlaundering.<sup>91</sup>

#### **3.4.2.1 Online banking: A hypothetical scenario**

A hypothetical scenario of a way (amongst several others) in which cyberlaunderer operates using online banking is given below:

Mr Adams, a student with little means of livelihood, is very conversant with the internet. He constantly browses job websites like [www.gumtree.com](http://www.gumtree.com) and [www.jobangels.com](http://www.jobangels.com) in search of job opportunities. Mr Brice, on the other hand, is a fraudster who runs a fake charity organization on the internet called [www.HelpHaitiNow.com](http://www.HelpHaitiNow.com) (a shell company) amongst several illegal activities he operates. Mr Brice has opened a special bank account online for this charity organization under the name Help Haiti Now. By means of a cash-in-hand

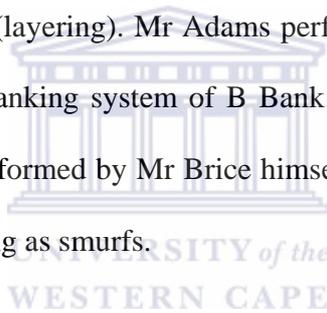
---

<sup>89</sup> Marshall et al (2005: 115).

<sup>90</sup> Marshall et al (2005: 115).

<sup>91</sup> Jamali (2009: 18). Another method by way of which one's identity can be stolen online is the use of spoof websites. These websites make certain attractive offers to the visitors with the condition that they provide certain personal details of theirs. See Atta-Asamoah (2009: 109).

arrangement (as could also be by way of “common purpose”) Mr Adams and Mr Brice cross paths (as guests to these job sites) and eventually reach an agreement. Mr Brice aims to siphon his illegally derived funds onto the mainstream commercial sector. He deposits a portion of his ill-derived funds into his savings account in B Bank (placement). Mr Brice then loads several smart cards and gift cards with the remaining funds, at different times. He then gives some of these cards to Mr Adams (the smurf) with the instruction to visit the charity organization and to make deposits under different identities to the bank account of the charity organization as well as his own personal bank accounts at strategic intervals (layering). Mr Adams performs all these operations online by using the online banking system of B Bank. Note: The work of the smurf, Mr Adams, can be performed by Mr Brice himself and can as well be performed by several others acting as smurfs.



### **3.4.3 Online auctions**

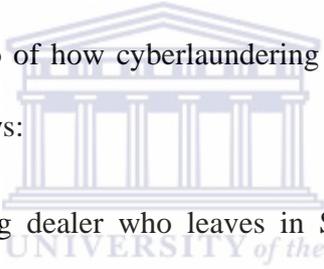
Online auctioning is currently a booming industry on the internet. However, it also has a loophole for cyberlaundering purposes. An online auction website allows persons registered on such site to put up items for sale on the site. Other persons registered on that very site can bid for such an item, and just as is the case with a typical auction sale, the item is sold to the person with the highest bid. Once this is done, the buyer sends the agreed amount to the company’s bank account whilst the seller directly sends the item or

product to the buyer. The company would then eventually pay the seller and charge its own commission if the buyer finds the product acceptable as advertised.<sup>92</sup>

The threat level with this system does not appear high because, in the ordinary course of events, the company is a legitimate one. The loophole is in the bidding process. A smurf could exploit this avenue by continuously bidding higher and higher, because in an auction sale without reserve, there is no limit to the bid made by a buyer.

#### **3.4.3.1 *Online auctions: A hypothetical scenario***

A hypothetical scenario of how cyberlaundering could work through the avenue of online auctions is as follows:



Mr Brice is a drug dealer who lives in Sydney. He wishes to convert the proceeds of his crime to legitimate wealth. He is registered on the auction site called Auction Express ([www.AuctionExpress.com](http://www.AuctionExpress.com)). In cahoots with Mr Adams (his smurf, who lives in Israel and is also registered on the same auction site), he agrees to put a painting up for sale on the same auction site at a specific time. He purchases a smart card which he loads with the proceeds of his illegal earnings. He sends the encryptions of the smart card to the email address of Mr Adams, who thereafter decrypts it and extracts the value in the smart card. At the agreed time, the painting is put up on the auction site. Mr Adams bids the highest for the painting, and the painting is consequently sold to him. Mr Adams then pays the money to the bank account of Auction Express, and Mr Brice sends the painting

---

<sup>92</sup> See Filipkowski (2008: 10).

to Mr Adams. After the necessary verifications have been made, Auction Express then pays the money to Mr Brice (which then takes the form of clean legitimate money). Note: This activity could be done simultaneously, as it is possible for Mr Brice to use multiple smurfs.

#### 3.4.4 Online gambling

Online gambling has been defined as “the provision of opportunities to play games of chance or obtain access to sports or race bookmaking via computer networks.”<sup>93</sup> Generally speaking, conventional casinos are often used to launder money. This is why various countries have very strict laws in place to govern the operations of casinos. The primary difference between online gambling and the traditional casino is the fact that one in every five persons who visits an online gambling site is deemed to be a pathological gambler in comparison to the same ratio of persons who visit a traditional casino.<sup>94</sup> This fact is justified by several factors. Firstly, online casinos, just like any other internet based activity, is very convenient to use from the comfort of one’s home. Also, in light of the fact that there are thousands of online gambling sites on the internet,<sup>95</sup> most online gambling sites entice customers to gamble for free for a stipulated number of minutes or hours, or at a very low discounted rate. This is hardly the case with traditional casinos.

---

<sup>93</sup> Musimanga (1998: 53). See the Financial Action Task Force (2008: 44). Also see annexure.

<sup>94</sup> See <<http://www.timesonline.co.uk/tol/news/politics/article620834.ece>> [accessed on 21 July, 2010].

<sup>95</sup> As of 2009, it was reported that a total number of 1,800 online gambling sites exist on the internet, and this number continues to grow. See The United States Government Accounting Office (2009: 41).

Cyberlaundering via the avenue of online gambling can follow two major routes. A cyberlaunderer could either exploit a very legitimate web-based online gambling service for laundering purposes, or could set up an online gambling service for the purpose of cleaning “dirty” money.<sup>96</sup> The first method is not common because of its inherent risks for cyberlaunderers. Usually, with a legitimate web-based system, a cyberlaunderer lacks actual control over the gaming activities and stands the chance of either winning or losing real money. The second scenario involving the establishment of an online casino, primarily for money laundering, is a more common form, because of its putative nature. The real danger of online gambling lies in this latter form.

The act of smurfing is commonly adopted by criminals using online gambling as a bedrock for their money laundering operations. Smurfs can be given cash by a criminal to play games on such a criminal’s online casino (in light of the second form highlighted above). This excludes the commission which the criminal pays them. Whether these smurfs eventually win or lose, either way, the criminal wins because the proceeds revert to him or her. This system is also called “the drumming up business scenario.”<sup>97</sup>

Cyberlaunderers could not be more content because of the “jurisdictional freedom” central to online casinos. This is typical with most cyber crimes. The borderless nature of the internet makes it nearly impossible to effectively regulate and control online casinos. This is a big problem whether or not a country has chosen to legalize internet

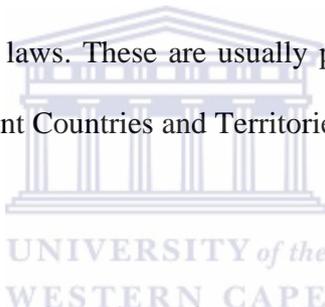
---

<sup>96</sup> Bumeter (2001: 2). There is usually a third form of online gambling which is called live-based gambling, which enables players to interact with one another online while playing, but is of little significance compared to the other two forms.

<sup>97</sup> See Bumeter (2001: 7) and Jamali (2009: 28).

gambling. Currently, in about 50 countries, internet gambling is legalized.<sup>98</sup> Only in very few countries like India<sup>99</sup> is internet gambling illegal. In the United States (US), although internet gambling is not per se considered illegal, in terms of the Wire Act,<sup>100</sup> the electronic transmission of betting and wagering activities is illegal.

The feature of anonymity is also a constant denominator in cases where criminals use online casinos to launder money, just as we see with respect to other cyberlaundering avenues. On a full-blown scale of money laundering via online gambling, criminals who own online casinos try to avoid the registration of their internet provider (IP) addresses. They do this by situating these sites in places with weak anti-money laundering (AML) laws. These are usually places that are formerly deemed by the FATF as Non-Compliant Countries and Territories (NCCTs).



#### **3.4.4.1 Online gambling: An hypothetical scenario**

As indicated earlier, the “drumming up business scenario” appears to be the most popular method by which money can be laundered using online casinos. A practical assessment of this is illustrated below.

Mr Brice is a drug dealer who resides in the state of Massachusetts in the US (a country which has an effective AML regime). His aim is to convert the proceeds of his crime to legitimate wealth. Mr Adams and several other

---

<sup>98</sup> This is evident in most European countries and some parts of the Caribbean. In Africa, only South Africa has express provisions legalizing internet gambling, although subject to certain regulations in terms of its National Gambling Act 7 of 2004.

<sup>99</sup> See Part 1 of the Bombay Wager Act IV of 1887.

<sup>100</sup> The Federal Wire Act 87 of 1961, U.S.C.

people like him run online casinos in Pakistan, a country with a poor AML regime. Mr Brice gets in touch with Mr Adams for the sake of cooperating and solidifying ties with him and several other online casino owners in Pakistan. Mr Brice uses Mr Adams and the others as an army of smurfs for his operations. He obtains their e-mail addresses, and purchases smart cards which he loads with equal financial values. Mr Brice then sends the details of these cards to the smurfs in Pakistan, using encrypted software. These smurfs then decrypt the details of the smart cards, and consequently register at Mr Adams's casino. The smurfs afterwards use the value of the smart cards to play and deliberately lose all the funds to Mr Adams' casino. This excludes the commission which they are individually given. The proceeds then revert to Mr Brice in the form of monthly instalments from either Mr Adams or (strategically) each smurf involved. On the flipside, should the smurfs win, the proceeds are again forwarded to Mr Brice also in the form of monthly instalments. Note: This could be only a slice of the pie, because Mr Brice can simultaneously make a similar arrangement with smurfs in various other countries.

### **3.4.5 Digital Payment Systems**

According to the FATF, the rationale behind establishing digital payment systems arises from the fact that it helps with certain key transactions on the internet without

regard to traditional currencies, or foreign exchange concerns.<sup>101</sup> The most accepted form of digital payments is the e-gold system, and this would be analyzed in greater detail.

E-gold is a form of electronic currency created for the World Wide Web. It is issued by e-gold Ltd, a Nevis corporation which is backed 100% by gold bullion in allocated storage.<sup>102</sup> The uniqueness of this form of electronic currency exists in how it is totally unrelated to traditional national currencies like the US dollar or the Japanese yen. E-gold operates by virtue of an account-based system in terms of which e-gold account holders can spend specified weights of gold to other e-gold account holders.<sup>103</sup> Consequently, e-gold can only be traded with someone with another e-gold account. Only ownership is exchanged. The e-gold system is created to suit international transactions considering the fact that it is borderless in nature. Traders using this system can trade this currency with other persons in several other countries. Although the term e-gold is the most common, other electronic metals (e-metals) such as e-silver, e-palladium and e-platinum are also used in a similar fashion.<sup>104</sup>

There are several reasons why a cyberlaunderer would thrive on this system. Firstly, it is not regulated. Unlike what is required of financial institutions, no CTRs are filed out. The customer due diligence (CDD) standards which most financial institutions are obliged to comply with are circumvented. Also, the recurring issue of anonymity comes up again. The fact that one's account can only be accessed via the internet renders it impossible for the identity of e-gold traders to be verified. Another reason

---

<sup>101</sup> Financial Action Task Force (2006: 12).

<sup>102</sup> See <<http://www.e-gold.com/unsecure/qanda.html>> [accessed on 14 July 2010].

<sup>103</sup> See <<http://www.e-gold.com/unsecure/qanda.html>> [accessed on 14 July 2010].

<sup>104</sup> See <<http://www.e-gold.com/unsecure/qanda.html>> [accessed on 14 July 2010].

why this system appears attractive is that most corporations of this nature are inclined to play on the vulnerability of nations with little or no effective AML regime. It is no wonder that e-gold Ltd has its server in Luxemburg.<sup>105</sup> This method of cyberlaundering is very relevant to the placement, layering and integration stages of money laundering. As indicated earlier, this is a non-bank peer-to-peer issuer model,<sup>106</sup> and the problems identified with this model are part of the general problems of online payment systems.

#### **3.4.5.1 Digital payment systems: A hypothetical scenario**

A brief account of how it is possible for a cyberlaunderer to launder money using this method is briefly explained below:

Mr Brice is a drug dealer who leaves in Cambodia. He has acquired incredibly huge proceeds of about \$1 million from his illicit activities within the past 3 months. He finds it very risky to deposit this money directly into his account in B Bank. He therefore goes online (www.e-gold.com) and opens an account with e-gold Ltd. He uses his entire illicit proceeds to acquire \$1 million worth of e-gold (placement). Mr Brice spends this much because he realises that he can easily dispense with the CTR requirements of most financial institutions. With this done, he begins to make numerous purchases of assets online from various companies situated in Australia and New Zealand, which accept e-gold as a

---

<sup>105</sup> See Phil Osborne's quoted commentary in Kellerman (2004: 4).

<sup>106</sup> See paragraph 3.2.3.3 supra.

viable payment system (layering).<sup>107</sup> Note: Mr Brice could, alternatively, have more than one e-gold account to which he could deposit parts of the illegal proceeds in feigning legitimacy.

### 3.4.6 Virtual communities

The subject of cyberlaundering would not be completely explored without a concise insight into virtual communities, as this is one of the most problematic techniques of cyberlaundering. A virtual community (otherwise called Massively Multiplayer Online Role-Playing Games or “MMORPG” in short) is an internet-based game/social network which allows participants or players to live a life very much akin to everyday life on such a website. The virtual world or community is a part of the online community in the form of a computer-based simulated environment.<sup>108</sup> The virtual community enable its users, who are represented in the form of avatars,<sup>109</sup> to live another life in a virtual environment that completely mirrors real life. This is currently the trendiest version of online gaming. There are several examples of virtual communities, such as Second Life, Entropia Universe, IMVU, Active Worlds, World of Warcraft and Kaneva. In 2008, it was estimated that the size of an average virtual economy grew to about \$450 million from \$350 million in 2007.<sup>110</sup> The current size of Second Life’s virtual economy stands

---

<sup>107</sup> This example is a real-life account of cyberlaundering involving e-gold Ltd. See Grow (2006: 10) and Kellerman (2004: 16).

<sup>108</sup> For more details see <<http://www.en.wikipedia.org/wilg/virtual-world/>> [accessed on 22 July 2010].

<sup>109</sup> An avatar is a digital representation of a person on the web. In simple terms, it means the “cartoonized” version of a person in a virtual environment.

<sup>110</sup> See Drug Enforcement Administration (2007) “National Money laundering Strategy” <<http://www.treas.gov/press/releases/docs/nmls.pdf>> [accessed on 29 July 2010].

well above \$500 million.<sup>111</sup> Given the popularity of Second Life, which has about 18 million users,<sup>112</sup> it would be discussed as a sample case.

In 2003, Second Life (SL) was developed by Linden Labs in the United States. In this virtual world, users (who are called “residents”, and through their avatars) can ‘explore, meet other residents, socialize, participate in individual and group activities; create and trade virtual property and services with one another or travel throughout the world.’<sup>113</sup> The residents in SL also have the ability to create things (or virtual objects) in the virtual world. SL has its own currency called Linden Dollars (L\$) which residents spend for commerce and other purposes. Residents can make real profits from their inworld transactions. Although residents receive a weekly stipend of L\$300, they are not restricted to this amount because a resident can convert real money into L\$ using SL’s money exchange service called “Xstreet,” which operates like a money exchange service in the real world.

It is very hard to classify virtual communities as game sites because these communities transcend the virtual world into real life, resulting in dire consequences which take a heavy toll on the real world. At this juncture, one might ask, how can a virtual reality site like SL be used for cyberlaundering? There are several reasons for this.

---

<sup>111</sup> See Drug Enforcement Administration (2007) “National Money laundering Strategy” <<http://www.treas.gov/press/releases/docs/nmls.pdf>> [accessed on 29 July 2010].

<sup>112</sup> See <<http://www.en.wikipedia.org/wilg/virtual-world/>> [accessed on 22 July 2010].

<sup>113</sup> See Jamali (2009: 32).

### 3.4.6.1 *Reasons why SL can be used for money laundering*

(i.) SL is a world with very little regulations or laws that control individual relations. Consequently, there are no AML laws. It is therefore the most conducive environment for money launderers. Where a society exists which does not prescribe laws controlling money laundering, such an act would not be deemed a crime and consequently, there can be no “criminals” in this respect. Even though SL has laws which govern the activities of residents by way of its Terms of Service provisions, this, however, only pertains to the residents’ protection from harassment, disclosure, indecency, intolerance and assault.<sup>114</sup>

Also, SL’s economy is not as controlled as in the real world, even though it operates like the one in the real world. For example, the Linden Exchange Service (Xstreet) enables residents to change real money to L\$ for use in SL. Also, L\$ can be changed back to real money to be used in the real world. The catch here is that Xstreet, not being a real financial institution, is not under any obligation to comply with the reporting obligations, nor is it required to provide information about clients as is expected from real-life traditional financial institutions.<sup>115</sup>

(ii.) SL is also a haven for tax evaders. The tax implication for residents in SL is a very dicey one. The principle followed is this: Only residents who

---

<sup>114</sup> See <[http://www.secondlife.com/terms\\_of\\_service/](http://www.secondlife.com/terms_of_service/)> [accessed on 22 July 2010]. Also see Jamali (2009: 41).

<sup>115</sup> The few regulatory mechanisms put in place by SL are considered in paragraph 4.5.3.1 below.

live in the European Union are charged value added tax (VAT). This is chargeable for anything for which a resident pays Linden Lab.<sup>116</sup> However, VAT is not charged on transactions in Linden Dollars (L\$) between residents. The real risk it creates with respect to tax evasion, and consequently cyberlaundering, is that the resident-to-resident transactions are not subject to taxation, and residents are under no obligation to disclose their source of income. Therefore, criminals can hide their income from the tax authorities by transacting in different forms of goods and services in the virtual world.<sup>117</sup>

(iii.) Also, SL forms a perfect environment for smurfing. There are certain features which are very ideal for smurfing activities. A simple example is where an army of smurfs (living in different regions of the world) purchase L\$ as residents in SL. They can each trade with themselves or do whatever they wish with the money.<sup>118</sup> At the end of the process, a smurf can convert the proceeds of his or her trade back from L\$ to his/her local currency. At this stage, the proceeds appear legitimate, and anything can be done with the money.

(iv.) Further, SL thrives on anonymity. The notion of a “resident” in SL is itself very vague. All that fellow residents in the virtual community know

---

<sup>116</sup> This includes premium account registration, purchases from the land store, land use fees (tier), private region fees, land auctions and LindeX transactions. See <<http://www.secondlife.com/corporate/vat.php>> [accessed on 23 July 2010].

<sup>117</sup> Jamali (2009: 45).

<sup>118</sup> Jamali (2009: 45).

about each other are each other's names, and a bit of each other's profile. Therefore, the resident could be anybody, and the details given in the profile do not necessarily have to be correct, as it is nearly impossible to conduct a verification of a resident's true identity on SL. Identity theft could easily occur in such an environment. Also, the dangers of online banking, as earlier identified,<sup>119</sup> gets compounded even more in SL because a resident can open a legitimate account in a "virtual bank," without providing a correct identification. Given that the basic banking laws that apply in the real world are nearly non-existent in SL, this opens up opportunities for money laundering, with devastating consequences for the real-life economy.



#### **3.4.6.2 *Second Life: A hypothetical scenario***

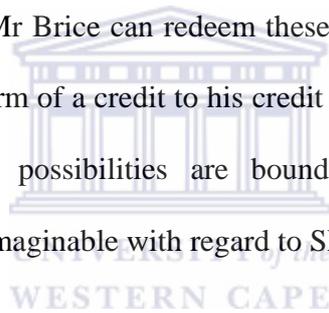
In Second Life (SL), as well as in other virtual communities, there are complex sets of circumstances illustrating how money can be laundered. A basic example is the following:

Mr Brice is a drug dealer living in South Africa. He wishes to convert the proceeds of his illegal activities to legitimate wealth. He becomes a resident of SL. He buys land in SL, and builds a big entertainment company which provides all forms of social activities such as night clubs, strip clubs and an exclusive 5 star club, membership of which is strictly

---

<sup>119</sup> See paragraph 3.4.2 supra.

by invitation. Mr Adams is a smurf, along with about 50 others who live across parts of Asia, South America, Europe and Africa. They are also residents of SL. Mr Brice loads different smart cards with equal financial value with the proceeds of his illegal activities. He sends those cards electronically to the various smurfs. On SL, Mr Brice invites the smurfs to be the only exclusive members of his 5-star club. The membership fee he charges is equivalent to the value represented in each smart card, which is paid to him in L\$. Mr Brice could automatically convert this back to real money or could further trade with the other smurfs with these proceeds. Mr Brice can redeem these proceeds using the ATM machine, either in form of a credit to his credit card account or his PayPal account. Note: The possibilities are boundless, given the infinite complex scenarios imaginable with regard to SL.



## CHAPTER 4

### REGULATING CYBERLAUNDERRING: POSSIBILITIES AND PRACTICALITIES

#### 4.1 GENERAL

At this stage, it should be quite clear that the concept of cyberlaundering, because of its novelty, is not properly mapped out and does not have well defined elements. Although the general notion is still the fact that cyberlaundering is an internet-based form of money laundering, its parameters are not as yet defined. It becomes extremely difficult for one to distinguish properly and set out effective control mechanisms for the crime. As a result, a piecemeal approach needs to be followed in exploring and identifying ways to fill up the loopholes that exist in cyberspace which enable criminals to thrive on cyberlaundering.

The current anti-money laundering (AML) regime is primarily based on enforcement mechanisms against money laundering operations. This follows the order of listing the predicate crimes that form the basis of money laundering; investigations, prosecutions, trials, convictions, punishment and confiscation.<sup>120</sup> While preventive mechanisms exist in certain instances,<sup>121</sup> the enforcement strategies, however, remain central to the AML regime. It is from this premise that the ensuing discussion regarding the AML regime on cyberlaundering sets out.

---

<sup>120</sup> Marshall et al (2005: 5).

<sup>121</sup> This basically entails reporting, regulations and supervisions, including ensuring customer due diligence. See Marshall et al (2005: 7).

## 4.2 CURRENT AML MEASURES AND CYBERLAUNDERING

The general preventive AML measures can be quickly summarised as follows: We have the reporting provisions on the one hand, and the record-keeping provisions on the other.<sup>122</sup> The model legislation which has been generally followed is the Bank Secrecy Act, which requires financial institutions to report all transactions above the value of \$10, 000, and which also requires financial institutions to maintain records of all transactions for a period of five years after such transaction has been concluded.<sup>123</sup> Similarly, most telecommunication services and internet service providers (ISPs) are required to observe and maintain user data for a period of one year in order to assist law enforcement bodies with investigations and prosecutions of cyber-related crimes.<sup>124</sup>

Whilst these reporting and recording requirements are more suited for certain tangible or physical transactions, they are not entirely viable solutions to the problem of cyberlaundering. The cyberlaundering dilemma scales past these measures. The following are reasons for this fact.

Firstly, by virtue of the nature of online transactions, one need not be physically present at the relevant place or site where transactions are conducted. This strikes at the problem of anonymity. The problem here is not whether certain ISPs, including some online financial institutions, can adhere to these reporting and record-keeping requirements, but the viability or truth of the information provided by the customer or

---

<sup>122</sup> Many local laws have followed the trend set by the Bank Secrecy Act.

<sup>123</sup> See sections 101 to 113 of the Act.

<sup>124</sup> See Jamali (2009: 67). The following local enactments are clear examples of this position: The US Telecommunications Act 56 of 1996, U.S.C. (sections 706-709); the South African Electronic Telecommunications Act 103 of 2006 (sections 3 and 4); and with regard to the European Council, the EC Directive 2002/22/EC (adopted on 7 March 2002) bears relevance.

user, which they (as ISPs) might be required to keep or report. This appears to be a common feature of most of the cyberlaundering mechanisms identified earlier.<sup>125</sup> For this reason, it is also problematic to enforce the “Know Your Customer” (KYC) principle directly.<sup>126</sup>

Secondly, the internet totally alleviates “the process chain” of things. Time and space as we conceive of them are shrunk into an immeasurable unit due to the speed at which the internet operates. The result is that it is highly unlikely (especially for hackers) to leave a trail behind, evidencing certain online transactions. The intangible nature of the internet makes it extremely easy for internet users to bypass certain processes or steps in a transaction process, which would otherwise be required ordinarily.<sup>127</sup> Closer monitoring by law enforcement agencies becomes very difficult as a result. In addition, one must remember that there are millions of transactions conducted per second on the internet. This creates some technical difficulty with respect to maintaining and closely scrutinizing each transaction.<sup>128</sup> Also, the internet is constantly exposed to different threats of viruses with very destructive capabilities. These viruses range from those which are designed to steal data, to others which are designed to hide or conceal data in order to render it inaccessible. Certain viruses also have the capability of shutting down websites completely.<sup>129</sup>

---

<sup>125</sup> See paragraph 3.4 supra.

<sup>126</sup> See a discussion on this at 4.5.1.1 below.

<sup>127</sup> For example, when one is opening a bank account at a physical bank, there is what is initially called the verification stage where one shows the consultant one’s identity book and other relevant documents in order to ascertain that the documents presented match the person in question. This verification process is not the same when one needs to open an account online. As stated earlier in paragraph 3.4.2 supra, the risk that inheres is that the information which is provided by the person wishing to open an account need not be true, in order for an online account to be open.

<sup>128</sup> See Jamali (2009: 50).

<sup>129</sup> A new breed of Trojan viruses known as the MX Trojans has these capability.

Given all these dangers that result of the nature and numerous features of the internet, it becomes extremely difficult to effectively apply the reporting and record keeping requirements as a preventive solution to cyberlaundering.

### **4.3 EFFORTS BY ANTI-MONEY LAUNDERING AGENCIES**

With respect to the general AML regime, there are several enforcement measures which have been put in place by certain agencies and institutions to fight money laundering. Given that cyberlaundering has not been really put into perspective, the general AML regime does not have measures that specifically deal with the issue of cyberlaundering. Nevertheless, some governmental agencies and financial organisations have adopted measures which are geared towards fighting cyberlaundering. This section gives a broad overview of these governmental agencies and financial organisations, and how they are responding to the emergence of cyberlaundering.

#### **4.3.1 Governmental agencies**

##### ***4.3.1.1 The Drug Enforcement Administration***

The Drug Enforcement Administration (DEA) was established by the United States (US) government to control the sale and distribution of illegal drugs in the US.<sup>130</sup> Illicit drug trade has been a steadily growing business globally. Recent studies have shown

---

<sup>130</sup> The DEA has an international reach with about 86 offices in over 62 countries.

that about \$65 billion are being spent on illegal drugs annually in the US alone.<sup>131</sup> For this reason, the DEA has been very active in the enforcement of money laundering laws in the US, as it is the key prosecutorial agency for drug related crimes in the country.<sup>132</sup>

In a recent report, the DEA identified New York City as one of the main financial hubs in the US where the threat of cyberlaundering operations relating to the proceeds of illegal drugs is menacing.<sup>133</sup> One of the DEA's focus areas is the e-payment system.<sup>134</sup> Nowadays, hard cash is hardly used to pay for drugs. Payments are now done online. To come to grips with this phenomenon, the DEA manages a special unit called the National Drug Intelligence Centre (NDIC) which is tasked with uncovering this practice.<sup>135</sup>

The DEA has examined the scenario where a law enforcement officer catches a drug dealer who has certain smart cards or pre-paid cards in his or her possession. In this regard, the question that arises is whether the seizure of the pre-paid cards consequently hinders the business of the suspect in custody. This would not be an issue where law enforcement bodies seize hard cash proceeds of crime. The NDIC arm of the DEA has been looking into this, and the outcome of the first investigation it has conducted shows that it is futile to stop electronic payments by seizing pre-paid cards. This is because pre-paid cards can be accessed by both the card holder and other third parties who are usually linked to the card. Thus, the funds that are stored in a pre-paid card, which might be in the possession of a law enforcement officer, can still be transferred from that card

---

<sup>131</sup> See <<http://www.justice.gov/dea/programs/money.html>> [accessed on 30 July 2010].

<sup>132</sup> See Jamali (2009: 42).

<sup>133</sup> See <<http://www.justice.gov/dea/programs/money.html>> [accessed on 30 July 2010].

<sup>134</sup> See paragraph 3.2 above.

<sup>135</sup> See <<http://www.justice.gov/dea/programs/money.html>> [accessed on 30 July 2010].

by the same suspect once released on bail, or by a co-conspirator or third party who need not be physically in the presence of the accused.<sup>136</sup>

For a problem of this nature, the only likely remedy would be a legislative one. The State of Nevada is the only state in the US with a possible solution to the problem. In Nevada, a new law was enacted called the SB-82,<sup>137</sup> which came into effect on 1 July 2009. This law authorizes law enforcement officers to investigate suspicious pre-paid card transactions and fraud cases that occur each year. Thus, with a warrant, the relevant authority can freeze funds on the pre-paid card for up to 10 days. This inevitably prevents criminals, as well as third parties, from removing the funds from the pre-paid card within that period. In certain instances, the SB-82 allows authorities to seize funds loaded onto a pre-paid card without a warrant.<sup>138</sup>

Whether or not this solution has been viable has not been assessed yet. We shall revert to the SB-82 in the discussion on pre-paid cards below.<sup>139</sup> For now, in sum, credit is due to the DEA for inspiring this legislative initiative.

#### ***4.3.1.2 The Federal Bureau of Investigation***

The Federal Bureau of Investigation (FBI) is a multi-tasked law enforcement agency in the US. It is a special intelligence unit for certain high profile crimes, including money laundering.

---

<sup>136</sup> Such third parties or co-conspirators are mostly smurfs who are not usually in the same territory or country as the accused. See the National Drug Intelligence Program (2010: 55).

<sup>137</sup> NV Senate Bill 82-75<sup>th</sup> (BDR 14-266).

<sup>138</sup> See the National Drug Intelligence Program (2010: 61).

<sup>139</sup> See paragraph 4.5.2.1 below.

However, with regard to cyberlaundering, the FBI currently works in conjunction with other agencies like the Internet Fraud Complaint Centre (IFCC) and the National White Collar Crime Centre (NWC3). The FBI has not published a concrete report on its various investigatory surveys on cyberlaundering, neither has it published a report on cyberlaundering cases. But on a much broader note, it has identified the online casinos as a major hub for money laundering activities.<sup>140</sup>

#### **4.3.1.3 National Accountability Bureau**

The National Accountability Bureau (NAB) of Pakistan is the country's own initiative to fight the rampant incidence of corruption and money laundering in the country.<sup>141</sup> The cash flow in Pakistan is largely unregulated. A clear example of this is the country's currency exchange services which use the banking remittance system.<sup>142</sup> The growth of technology in Pakistan has compounded these problems. It has therefore turned out to be a hot spot for cyberlaundering operations.

In a factual sense, the NAB has not been entirely successful in combating the numerous cyberlaundering activities in the country. This is due to the problematic financial system in the country. Pakistan was previously blacklisted by the Financial Action Task Force (FATF) as a Non-Compliant Country and Territory (NCCT),<sup>143</sup>

---

<sup>140</sup> International Finance Corporation (2009: 3). Also see Jamali (2009: 41).

<sup>141</sup> The agency was established in terms of the National Accountability Ordinance 1999. See <<http://www.nab.gov.pk/>> [accessed on 08 August 2010].

<sup>142</sup> Jamali (2009: 43). The remittance system allows for less scrutiny of persons seeking to exchange currencies regardless of such person's nationality and the amount he wishes to change.

<sup>143</sup> See <<http://www.fatf-gafi.org/info/191432/>> [accessed on 08 August 2010].

because it was seen as a risk to the ‘international financial system.’<sup>144</sup> Although the NAB lays out plans to tackle the ‘electronic money laundering problem,’<sup>145</sup> as it calls it, there has not been any enforcement or any actual step taken towards this end.

#### **4.3.1.4 *Serious Organized Crime Agency***

The Serious Organized Crime Agency (SOCA) is the United Kingdom’s incentive to effect a proper regulation of illegal drugs, human trafficking, fraud, gun crimes, computer crimes and money laundering.<sup>146</sup> With regard to anti-money laundering activities, the SOCA deals primarily with suspicious activity reports, and acts in accordance with the Proceeds of Crime Act<sup>147</sup> and the Computer Misuse Act.<sup>148</sup>

Similar to the FBI, the SOCA is yet to issue a concrete report on its numerous investigations of cyberlaundering activities in the United Kingdom.

#### **4.3.1.5 *Immigration and Customs Enforcement***

The Immigration and Customer Enforcement (ICE) is an investigative agency in the US Department of Homeland Security. As part of its vast array of programmes, the ICE seeks to prevent and investigate criminal operations along the US border. This inevitably includes money laundering.

---

<sup>144</sup> See <<http://www.fatf-gafi.org/03343/html>> [accessed on 08 August 2010].

<sup>145</sup> See <<http://www.nab.gov.pk/>> [accessed on 08 August 2010].

<sup>146</sup> See <<http://www.soca.gov.uk/about-soca/>> [accessed on 08 August 2010].

<sup>147</sup> 2002, c.29.

<sup>148</sup> 1990, c.18. Whilst the Proceeds of Crime Act deals with aspects of civil recovery of criminal proceeds, the Computer Misuse Act deals with basic violations of computer technology laws.

Recently, the ICE's cybercrime centre established the Operation Cornerstone Investigation initiative.<sup>149</sup> This initiative has the primary purpose of attacking the roots of money laundering activities, including cyberlaundering, by enlisting the cooperation of the private sector. Just like the DEA, the ICE has also identified the e-payment systems as being problematic. Its own strategy is more holistic in nature. The ICE has delegated special agents to liaise with certain private sectors, mostly financial institutions, in order to assist it in identifying weaknesses in the financial system. By identifying these weaknesses, it would be much easier to find an effective and practical solution. Currently, in each of the ICE's 25 different field offices across the US, a special agent has been appointed to exercise this function.<sup>150</sup>



### **4.3.2 Financial Agencies**

#### **4.3.2.1 *The Financial Action Task Force***

The Financial Action Task Force (FATF) is an inter-governmental agency which was established by the G-7 summit in Paris in 1989. It plays a policy-making role in the fight against money laundering. Primarily, the FATF 'sets international standards to combat money laundering and terrorist financing; it assesses and monitors compliance with the FATF standards; it conducts typologies studies of money laundering and terrorist financing methods; trends and techniques, and responds to new and emerging threats such as proliferation financing.'<sup>151</sup> The FATF's "40 plus 9 Recommendations"<sup>152</sup> are a

---

<sup>149</sup> Kellerman (2004: 3).

<sup>150</sup> Kellerman (2004: 4).

<sup>151</sup> See <<http://www.fatf-gafi.org/info/191432/>> [accessed on 08 August 2010].

clear reflection of its aims. Other than the basic formulation of these policies, the FATF also seeks to stir up political will amongst countries to make the fight against money laundering their top priority. As of March 2010, the FATF had about 35 member states.<sup>153</sup>

The FATF has played a big role in the fight against cyberlaundering because it has identified certain key threat areas. In 2007, the FATF identified certain new (online) payment methods which make the electronic cash system a potential threat to the fight against money laundering.<sup>154</sup> Sadly, this prediction by the FATF is now a reality. The FATF has also identified and issued a report on the aspect of online gambling.<sup>155</sup> Certain of its proposals in this regard are considered below.<sup>156</sup>

Furthermore, the FATF Special Recommendation VII<sup>157</sup> (SR VII) seeks to prevent money laundering and terrorist financing possibilities by way of wire transfers. In this light, the FATF has proposed that the originator information should be made available to the relevant law enforcement or prosecutorial body in order to aid investigations and prosecutions. The originator information would also help financial intelligence units and the beneficiary financial institution to identify and report these suspicious transactions and their existent risks.<sup>158</sup>

---

<sup>152</sup> Financial Action Task Force (2003: 78).

<sup>153</sup> See <<http://www.fatf-gafi.org/info/191432/>> [accessed on 08 August 2010].

<sup>154</sup> Financial Action Task Force (2010C: 56). Also, see paragraph 3.2 supra.

<sup>155</sup> Financial Action Task Force (2008: 77). See annexure.

<sup>156</sup> See paragraph 4.5.3.2 below.

<sup>157</sup> Financial Action Task Force (2003: 23). Also see the Financial Action Task Force (2004B: 31).

<sup>158</sup> Financial Action Task Force (2004B: 14).

The FATF generally stresses the importance of political will in the fight against money laundering. The enforcement of these FATF recommendations and proposals by countries is equally crucial.

#### **4.3.2.2 *The Financial Crimes Enforcement Network***

The Financial Crimes Enforcement Network (FinCEN) is a law enforcement branch of the US Department of Treasury. It was established in 1990 to provide a broader government-based form of financial intelligence. The FinCEN is directly responsible for the regulatory measures flowing from the Bank Secrecy Act. Thus, the FinCEN oversees the reporting and recording keeping stipulations required by most financial institutions in the US.<sup>159</sup> In essence, this agency seeks to enforce the control measures currently in place to curb money laundering activities. Also, the Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism Act of 2001 (US PATRIOT Act)<sup>160</sup> widened the duties of the FinCEN to include terrorist financing initiatives related to money laundering activities.

Ultimately, the FinCEN seeks to cover all money laundering threats, which includes the detection and deterrence of cyberlaundering.<sup>161</sup> This is stated in its Strategic Plan for the Fiscal Years of 2008-2012.<sup>162</sup> However, the FinCEN is yet to issue an actual report on the subject.

---

<sup>159</sup> <[http://www.fincen.gov/about\\_fincen/wwd/](http://www.fincen.gov/about_fincen/wwd/)> [accessed on 9 August 2010].

<sup>160</sup> 115 Stat. 272 (2001).

<sup>161</sup> See Jamali (2009: 59).

<sup>162</sup> Available at <[http://www.fincen.gov/about\\_fincen/wwd/](http://www.fincen.gov/about_fincen/wwd/)> [accessed on 9 August 2010].

#### 4.3.2.3 *The World Bank*

The World Bank's effort to regulate cyberlaundering is probably the most radical and aggressive compared to most other regulatory or policy-making organizations. The World Bank's fight against cyberlaundering is premised on the rationale that the internet, which is the very root of the problem, should be used to fight the crime.

The World Bank, in conjunction with the International Monetary Fund (IMF), has introduced the Financial Sector Assessment Program (FSAPs),<sup>163</sup> which is geared towards blocking certain loopholes in the cyber payment systems, especially with respect to the Non-Bank Issuer Model and the Peer-to-Peer Model.<sup>164</sup> The threats that emanate from these payment methods are identified as a result. However, there is yet to be a report issued on this.

Also, the World Bank has started a project called the Global Systems Mapping Project, which monitors the flow or movement of money in complex financial systems.<sup>165</sup> By identifying the various avenues or means through which money moves, it would be much easier for governments and policy makers to be able to forge better monetary policies in future.<sup>166</sup>

Furthermore, the World Bank proposes that a cyber-threat analysis centre should be created across all financial institutions. These threat centres could be like an international information sharing vehicle. Some financial institutions in the US already have this facility, generally called the Financial Services Information Sharing and

---

<sup>163</sup> See <<http://www.imf.org/about/projects/worldbank>> [accessed on 13 August 2010].

<sup>164</sup> See the discussion at paragraph 3.2.3.3. *supra*. Also, see Kellerman (2004: 3).

<sup>165</sup> Kellerman (2004: 16).

<sup>166</sup> Kellerman (2004: 16).

Analysis Centre (ISAC). The ISAC serves as an internet-based third party service provider which could provide alerts, and real time information sharing and notifications.<sup>167</sup> Along with detecting potential cyberlaundering transactions, the ISACs could detect other possible cyber threats like phishing.<sup>168</sup>

Moreover, better harmonisation and coordination of cyber entities would go a long way in curbing cyberlaundering. Ensuring a tighter entry barrier, such as licensing and registration, would further prevent certain websites such as e-gold.com (and the like) from being mechanisms for money laundering.<sup>169</sup>

Another proposal made by the World Bank relates to the 13<sup>th</sup> recommendation by the FATF, which deals with the Know Your Customer (KYC) principle. Basically, financial institutions are required to apply this principle as closely as they can to online transactions with customers. This is discussed in detail below.<sup>170</sup>

Lastly, it is suggested that electronic forensics should be promoted and given priority in financial institutions today.<sup>171</sup> In order for bank examiners and law enforcement agencies to investigate cyberlaundering operations, there must first be electronic evidence with which they can work.<sup>172</sup> However, electronic evidence would only exist if it is properly preserved by the financial institution. Therefore, in-house or external training of financial officers must be conducted in order to preserve the evidence effectively.

---

<sup>167</sup> Kellerman (2004: 18).

<sup>168</sup> Phishing is a form of identity theft in terms of which a criminal tries to acquire someone's details (like username, password, and credit card information) by masquerading as a legitimate entity.

<sup>169</sup> Kellerman (2004: 16).

<sup>170</sup> See paragraph 4.5.1.1 below.

<sup>171</sup> Kellerman (2004: 17).

<sup>172</sup> Kellerman (2004: 16).

#### 4.4 GENERAL PREVENTIVE MEASURES FOR CYBERLAUNDERING

General preventive measures can be taken to tackle cyberlaundering. One must not stray from the fact that the problematic aspects of cyberlaundering are invariably linked to the general problems identified within the broad sphere of money laundering.

Firstly, a primary area of focus should be countries which the FATF has removed from its list of Non-Compliant Countries and Territories (NCCTs), but are now subjected to close monitoring.<sup>173</sup> Although delisted, many of these countries still do not adequately police internet operations. They are thus fertile breeding grounds for cyberlaundering activities. This has a dire consequence on countries with effective AML regimes, because criminals who run internet sites in these former NCCTs are often not located in such countries. They are often located in fully compliant countries such as the United States and the United Kingdom. Consequently, these NCCTs are merely a tool or base point for the operations of a criminal, because of the lack of vigilant policing.

Another area of focus should be predicate offences. A crime must have been committed from which a criminal derives funds. The purpose of laundering the funds is eventually to disguise the proceeds of such crime in order to make them appear legal. This is the underlying rationale for money laundering. Just as there are predicate offences underlying the typical money laundering offence like theft and fraud, there are also predicate offences which are the basis of cyberlaundering. Some of these predicate offences are internet fraud, identity theft, internet piracy, and phishing, amongst a host

---

<sup>173</sup> Some of these countries are, namely, Cook Islands, The Dominican Republic, Angola, Antigua, Egypt, Grenada, Pakistan, Guatemala, Indonesia, Marshall Islands, Myanmar, Nauru, Nigeria, Niue, Philippines, Russia, St. Vincent, the Grenadines and Ukraine. See <<http://www.fatf-gafi.org/info/191432/>> [accessed on 08 August 2010].

of others. The logic is simply that by tackling these predicate crimes one is ripping out the roots of cyberlaundering. The effective combating of these predicate crimes depends on whether efficient policies exist to suppress them adequately.

#### **4.5 SPECIFIC PREVENTIVE MEASURES: CHOKES POINTS OF CYBERLAUNDERING**

Other than the general measures stated above, there are also specific deterrent measures that merit our focus. At this stage, it is important to reaffirm the fact that anonymity is the core of the cyberlaundering dilemma. Unfortunately, one cannot merely tackle the anonymity problem holistically. Rather, one must consider the most plausible regulatory means available for the core areas which stem from the anonymity feature. The identifiable areas, or choke points, are online banking, cyber payment systems and e-gaming. Regulatory possibilities for these various aspects are expounded upon below.

##### **4.5.1 Safeguarding online banking**

###### **4.5.1.1 *Modifying the KYC principle***

The FATF recommendation 13 simply states that all financial institutions must have basic knowledge of their transacting customers.<sup>174</sup> In recent times, this principle has

---

<sup>174</sup> Financial Action Task Force (2003: 62).

been further expounded by the Wolfsberg group of banks.<sup>175</sup> The financial institutions under the Wolfsberg group advocate what is known as the risk-based approach.<sup>176</sup> However, the KYC principle and its extended risk-based form are only preconditions laid down for a financial institution wishing to transact with a “new” customer. Seeing that the customer would be continually present, the same procedure is not usually conducted for future transactions. This precautionary framework does not cater directly for online transactions. As mentioned earlier, with respect to one of the problems with online banking, multiple actors can have access to an online bank account, as long as the information required for access is provided. The problem here is that there is currently no effective mechanism which can ascertain the true identity of the person seeking to open an account online. Hence, the same rigid KYC safeguards that would have been conducted for potential customers in the normal course of events cannot be similarly performed with respect to a prospective customer of an online bank.

The Electronic Banking Group of the Basel Committee on Banking Supervision has been battling with the quandary of how banks can apply the due diligence requirements, basically the KYC principle, to non-face-to-face customers. In its 2001 report on risk management principles,<sup>177</sup> the Committee proposed that banks should apply the same customer identification procedures to non-face-to-face customers as is done in the case of face-to-face customers who are subjected to an interview. Coupled with this, financial institutions are advised to mitigate higher risks by ensuring the ‘certification of documents presented; requisition of additional documents to complement those which

---

<sup>175</sup> See the Wolfsberg Group of Banks (2010: 40).

<sup>176</sup> The risk-based approach requires banks to look at the inherent risks involved in banking with a customer. This entails a more detailed analysis of the customers, their background and their respective personal circumstances.

<sup>177</sup> The Basel Committee on Banking Supervision (2001: 90).

are required for face-to-face transactions; independent contact with the customer of the bank; third party introduction, e.g. by an introducer [subject to any criteria] or requiring the first payment to be carried out through an account in the customer's name with another bank subject to similar customer due diligence standards.<sup>178</sup>

Even though the above measures are quite stringent, the problem is yet unsolved. For this reason, it would seem logical to require a potential customer who wishes to open an online account at a bank to be physically present in order to go through the normal interview process. In other words, subjecting a potential customer to the same face-to-face interview procedure might be the safest route to follow. After this process, such a customer can conduct subsequent banking transactions online. By so doing, the bank can conduct the necessary verifications and thus act in line with the required KYC principle. However, this would not completely eradicate the problem. For the other numerous transactions to be conducted subsequently online by the customer, better safeguards need to be adopted. To this end, a more complex system of identification needs to be introduced which would not merely require one to populate the required field in the application form with a name and password. In this regard, it has been suggested that in order to promote transparency of online transactions, a biometric and public key infrastructure must be installed.<sup>179</sup> This implies that one would always need to provide two kinds of information. Firstly, specific information about something which the customer knows, and second, some personal feature of his or her person would need to

---

<sup>178</sup> The Basel Committee on Banking Supervision (2001: 81).

<sup>179</sup> Kellerman, (2004: 16).

be authenticated.<sup>180</sup> What this exactly entails remains uncertain at this point. But adopting such a dual standard verification system is likely to guarantee the identity of persons who perform online transactions.

#### **4.5.1.2 Adopting new wire transfer models**

By way of rehashing what has been discussed earlier,<sup>181</sup> the notion of wire transfers refers to the electronic transfer of funds, albeit its value, at the request of a customer from one bank account to a beneficiary account, which is usually another bank. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) system is the main interbank messaging system which banks use to indicate monetary transfers internationally.<sup>182</sup> However, the loophole that exists relates to the wire transfers between a local bank and an international bank, with no relationship or connection with each other. The quote below details the vulnerability of the SWIFT system which criminals have since exploited.

‘When a bank wants to wire a customer’s money to another bank, one of the several types of SWIFT messages may be used as instructions for the transfer. This message is sent through SWIFT separately from the actual settlement of the funds. When a customer’s bank does not have a direct relationship with the ultimate receiving bank [especially with international transfers] banks may use either cover payments or serial payments to send money through one or more

---

<sup>180</sup> Kellerman, (2004: 16). This biometric system is currently used when one needs to draw money from an ATM machine, which requires the ATM card and a password. It is difficult to follow the same safeguard with regards to online transactions. Clearly, this aspect is one which merits some technological advancement. This should however not defy the reach of the modern world’s technological prowess.

<sup>181</sup> See paragraph 2.3 supra.

<sup>182</sup> See paragraph 2.3.1 supra.

intermediate banks. [In terms of cover payments]... two separate SWIFT messages [the MT103 and the MT 202] are sent... The MT 202 sent to the intermediary bank did not retain originator and beneficiary information [as the MT 103].<sup>183</sup>

In essence, a criminal has been able to disguise his or her identity in order to launder money by sending wire transfers through intermediary banks.<sup>184</sup> The upshot of this is that these intermediary banks are oblivious about the identity of the sender. The DEA has been effective in identifying this problem. As a result, a new type of SWIFT messaging system known as the MT 202 COV has been introduced.<sup>185</sup> The MT 202 COV covers the loopholes and enables the intermediary bank to retain both originator and beneficiary information on virtually all wire transfers. Therefore, it does not matter whether the intermediary bank is local or international, for the information is captured regardless of the link it might have with the originator bank. As a result of this new system, an intermediary bank can consequently conduct its own investigations on suspicious transactions as it would have had the requisite information to do so.<sup>186</sup>

While some financial institutions in the US are beginning to adopt this new system, most financial institutions are yet to adopt it fully. The banking regulatory laws therefore need to be amended to ensure that this new wire transfers system is made mandatory for all banks.

---

<sup>183</sup> The National Drug Intelligence Program (2010: 79).

<sup>184</sup> See paragraph 3.4.2.1 supra.

<sup>185</sup> The National Intelligence Program (which the DEA oversees) has been instrumental in this innovation. The system was launched on 21 November 2010.

<sup>186</sup> The National Drug Intelligence Program (2010: 79).

## 4.5.2 Tighter measures for cyber payment systems

### 4.5.2.1 *Smart cards regulation*

As a basis, it must be generally understood that most payments are made online through prepaid or smart cards.<sup>187</sup> The main issue that has been identified in this respect is that cyberlaunderers are using smart cards to store and transfer proceeds of illicit activities. The focus should therefore be on how the use of these smart cards can be regulated by the relevant authorities. We have seen above that the DEA has influenced the State of Nevada to adopt the SB-82 law, which would enable law enforcement authorities to investigate suspicious smart card transactions and freeze the stored value in these cards when a criminal is caught with them.<sup>188</sup> Governments should therefore take a cue from this by enacting similar legislation. This initiative might, however, be an up-hill battle for most countries which have been delisted from the NCCTs list, but are still subject to monitoring by the FATF. This is evidenced by the fact that majority of these countries are still battling to comply with certain basic FATF recommendations.

Furthermore, given the fact that certain smart card companies, like the Freedom Eagle Card,<sup>189</sup> do not put a cap on the amount that can be loaded onto their cards, smart cards should be regulated by limiting their functions and capacities.<sup>190</sup> This can be done by restricting the value in a smart card to a particular amount, by restricting its turnover limits and by limiting the number of smart cards per customer.<sup>191</sup> Although this might

---

<sup>187</sup> See the discussion on cyber payments in paragraph 3.2.2 supra.

<sup>188</sup> See paragraph 4.3.2.3 supra.

<sup>189</sup> See paragraph 3.2.2.1 supra. Also see <<http://www.freedom-card.co.uk/>> [accessed on 2 September 2010].

<sup>190</sup> See Ping (2004: 15) for a similar argument.

<sup>191</sup> Ping (2004: 16).

seem quite probable in lieu of regulation, such measures can still be circumvented in a world of smurfs. A cyberlaunderer could still easily use smurfs who individually have smart cards in their own names for his or her operations. Moreover, this is likely to cause an uproar amongst smart card companies who might see this as an obstacle to doing good business.

#### **4.5.2.2 Protected cryptography**

Messages (and other forms of communications via the internet) are not barely conveyed or “transported” around cyberspace. They take the form of encryptions. To understand how encryptions work, one invariably needs to delve into the roots and skeletal framework of online transactions, which is embedded in a technological mould. Certain suspicious communications between persons can go unchecked. An example is where a cyberlaunderer sends an encrypted code to a smurf via an email containing the details of certain prepaid cards.<sup>192</sup> Encryption is a technological term used to refer to a protected message. To get a clearer picture of how this works, when two persons communicate via the internet (from simple emails to online bank transactions) there are two public keys involved.<sup>193</sup> In a much broader sense, each communication (or “key”) is encrypted. However, in certain instances, and largely dependent on the government of

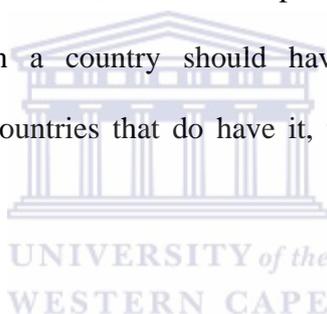
---

<sup>192</sup> See the concurrent privacy argument below in paragraph 4.6.2 below.

<sup>193</sup> For more information on what a public key entail see <[http://www.livinginternet.org/file\\_crypt](http://www.livinginternet.org/file_crypt)> [accessed on 16 August 2010].

the day, a “third party system” generally known as a key recovery system<sup>194</sup> is in place to intercept public keys and decrypt the relevant information that transpires.

In the US, the National Security Agency came up with what is known as “Clipper Chip” which is a key recovery system. This is a standard encryption method that would enable the government to track encryptions. Once a suspicious transaction is sensed, the government can decrypt messages in order to have a trail of the message. Where a “Clipper Chip” kind of system is not in place, a law enforcement agency would require a court order to decrypt such a message when there is sufficient proof of suspicious transactions occurring. However, this raises privacy concerns.<sup>195</sup> The information technology (IT) body in a country should have such a key recovery system. Unfortunately, for most countries that do have it, this key recovery system has been under utilized.



#### **4.5.2.3 Better detection mechanisms**

With respect to cyber payments, the issue of detection is crucial. The question that begs an answer is how law enforcement bodies are expected to detect suspicious transactions. Most electronic transactions possess certain digital signatures which entail ‘the identification of the user, location of the teller machine where it was used with the amount of transaction it holds, and the date/time stamp.’<sup>196</sup> It is usually a hassle for

---

<sup>194</sup> See <[http://www.livinginternet.org/file\\_crypt](http://www.livinginternet.org/file_crypt)> [accessed on 16 August 2010]. The key recovery system is also known as the key escrow agency system. See Straub (2002: 531).

<sup>195</sup> See paragraph 4.6.2 below.

<sup>196</sup> See Jamali (2009: 43).

authorities to monitor every digital signature closely for suspicious transactions. For this reason, oversights often occur.

Most financial institutions and companies are now taking cognisance of the detection problem. Some pre-paid card companies now use the services of some independent detection agencies to monitor the pre-paid card transactions by their customers. An example of such a company is Red Plc which offers the PRISM Merchant system<sup>197</sup> and which boasts successful detection of fraud and money laundering schemes. PRISM's operations are explained as follows:

'PRISM Merchant combines powerful neural network risk models with a flexible rules-based system for implementing expert merchant risk management strategies. PRISM's neural models utilize data feeds from your merchant processing system to score transactions from individual merchants. The models take into account a wide range of merchant information, including higher than normal incidence of charge-backs, variations in transaction volumes, numerous same-card transactions, average ticket amounts that exceed the norm for the merchant's line of business, large number of keyed-in transactions and significant increases in average ticket items for a credit sale.'<sup>198</sup>

The success of this system is yet to be ascertained. The mere fact that the detection of cyberlaundering activities is put in the hands of private entities is just another way of privatizing national security. This should not cause one to lose sight of the fact that law enforcement bodies bear the principal duty of detecting such

---

<sup>197</sup> For more information see <<http://www.redplc.com/about/>> [accessed on 16 August 2010].

<sup>198</sup> <<http://www.redplc.com/about/PRISM/>> [accessed on 16 August 2010].

suspicious transactions. Thus, it is nothing more than a reiteration of the fact that the bulk of the work rests with governments.

### **4.5.3 Blocking the lacunae in e-gaming**

#### **4.5.3.1 Regulation and virtual communities**

Virtual communities, as identified earlier,<sup>199</sup> are very problematic. Perhaps the most problematic features are the possibilities for participants to open a bank account in a “virtual bank” and transfer money within the virtual world as in the real world. For this reason, these virtual worlds are very attractive to the prying eyes of money launderers. One does not have to look into space to find the loophole, because internal control might seem to be the only viable solution. Some of these internal measures deserve some elaboration.

The most glaring problem which needs redress is the unregulated banking system in the virtual worlds. These so-called “virtual banks” should be made subject to the same regulations and control to which terrestrial banks are being subjected. It could, however, be quite challenging in reality to expect virtual banks to adhere to record-keeping and reporting requirements.<sup>200</sup> But an attempt would undeniably be the first step in addressing this vulnerability. Most virtual communities are now under pressure to operate their business in line with the standards of the real world. For example, in March 2009, Entropia Universe obtained permission from the Swedish Financial Authority to

---

<sup>199</sup>See paragraph 3.4.6 supra.

<sup>200</sup> This links back to the discussion on the intangibility of the internet, which aids cyberlaundering. See paragraph 4.2 supra.

conduct legitimate banking activities in its virtual community.<sup>201</sup> This has the implication that Entropia's virtual bank would be subject to the same recording-keeping and reporting requirements which terrestrial banks must comply with. Other virtual communities like Second Life (SL) are yet to obtain such a license. If these licenses are made mandatory for virtual communities, and they follow suit, the threats posed by virtual banks would be lessened.

SL does, however, have regulatory measures aimed at policing suspicious transactions in its virtual world. For instance, because most of the activities on its site are, in reality, based on its server, it is able to monitor the activities of each resident closely and keep a record of them. SL is also under an obligation to report to law enforcement agencies where suspicious transactions have been detected.<sup>202</sup> SL's money exchange service (X-street) is similarly monitored. However, the reality is that these measures are still constantly circumvented by residents. For this purpose, a third party regulatory body is required to keep a better watch.

#### ***4.5.3.2 Regulation and online gambling***

Online casinos are invariably informal financial organizations and they should be subject to the same strict regulatory measures as online banking.<sup>203</sup> In consequence, online casinos should be subject to the KYC principle. Such strict measures might,

---

<sup>201</sup> See Mindark (2009: 4).

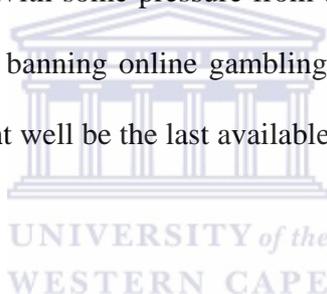
<sup>202</sup> Jamali (2009: 48).

<sup>203</sup> See paragraph 4.5.1 supra.

however, not be pleasing to operators of online gambling sites, as it could dissuade potential customers.

As indicated earlier,<sup>204</sup> the online gambling problem is compounded by the fact that most sites are registered in off shore countries with very weak AML laws.<sup>205</sup> As a result, the KYC procedures are not adhered to assiduously. This factor, by itself, hinders the possibility of finding an appropriate measure to control money laundering through online gambling.

Due to imminent dangers, the US has gone as far as banning online gambling (albeit only in certain respects). With some pressure from the FBI, in 2007, Linden Labs took an unprecedented step by banning online gambling in Second Life.<sup>206</sup> Banning online gambling completely might well be the last available solution, should the situation spiral out of control.



## **4.6 PROSECUTING CYBERLAUNDERING**

### **4.6.1 General**

In general, the prosecution of the crime of money laundering has been quite challenging. The problem of jurisdiction and investigations often arises. These problems are compounded further when it comes to cyberlaundering. There has been no reported case law on cyberlaundering. This aspect, much like the other aspects of

---

<sup>204</sup> See paragraph 3.4.4 supra.

<sup>205</sup> For example, Antigua is a territory where most online casinos sites are registered.

<sup>206</sup> This was done in terms of the Illegal Gambling Business Act 15 of 1970, U.S.C. and the Unlawful Internet Gambling Enforcement Act 4 of 2006, U.S.C. See Jamali (2009: 42).

cyberlaundering, is an untrodden path, which leaves one in the dark. One ought to remember that the cyberlaunderer could well be anybody, ranging from the criminal who siphons off funds from the crime he commits into cyberspace, to a juristic person or an internet service provider (ISP). The question as to whom to prosecute would depend solely on the merits of each case. What appears to be a bigger challenge, however, are the issues of privacy and jurisdiction. More light will be shed on these aspects.

#### 4.6.2 Privacy concerns

The right to privacy is a fundamental human right guaranteed in the constitutions of most democratic states. An ongoing debate has been whether the right law enforcement agencies have to pry into electronic communications of persons should supersede the individual's fundamental right to privacy. Undoubtedly, this is a major stumbling block for law enforcement officers when conducting investigations on suspicious transactions. This debate is particularly heated when it comes to the issue of cryptography. Many have argued that the key recovery system, which is like an "automatic store-house" where all encryptions are collected, is a direct violation of one's privacy.<sup>207</sup> This is because a law enforcement agency can easily gain access to such encryptions where they are able to prove a reasonable suspicion or make out a *prima facie* case. Consent by persons cannot play a role here because it involves prove of encryptions, and not hard files or records containing the identity of individuals.<sup>208</sup>

---

<sup>207</sup> See Straub (2002: 530).

<sup>208</sup> See <[http:// www.livinginternet.org/file\\_crypt](http://www.livinginternet.org/file_crypt)> [accessed on 16 August 2010].

The opposing argument here relates to national security and the interest of justice. There are many evil-minded people, such as terrorists, who constantly devise means of causing some kind of havoc. There are others who find the internet simply more convenient for committing all sorts of crimes, and these people use the internet concurrently as a useful tool to “wash” the proceeds derived from their respective crimes. The question is thus whether the need to prevent the activities of these persons is more fundamental than the need to protect an individual’s right to privacy.

To start with, every case must be judged on its own merits. Despite these arguments, it should be remembered that the domestic legislation dealing with electronic communications in the relevant country must first be studied. Some of these laws stipulate the situations where a law enforcement agency is allowed to access the electronic records and communications of persons. For example, in South Africa, the Electronic Communications and Transactions Act<sup>209</sup> (ECTA) lists instances where electronic communications may be intercepted.<sup>210</sup> A similar provision can be found in the Regulation of the Interception of Communication and the Provision of Related-Information Act<sup>211</sup> (RICA). Similarly, in the US, the Right to Financial Privacy Act<sup>212</sup> (RFPA) and the Electronic Communications Privacy Act<sup>213</sup> (ECPA) both regulate the interception of the one’s personal information. The RFPA specifically requires a law enforcement agency to have authorization before the financial records of a person can be

---

<sup>209</sup> Act 25 of 2002.

<sup>210</sup> See sections 51 and 52 of the Act.

<sup>211</sup> Act 70 of 2002. See sections 2 to 11.

<sup>212</sup> Act 12 of 1982, U.S.C. Sections 3401-3409.

<sup>213</sup> Act 18 of 1986, U.S.C. Section 2510(12).

obtained from a financial institution. The ECPA, on the other hand, prohibits internet service providers from dispensing the details of one's electronic communications.<sup>214</sup>

Therefore, as long as a particular action by a law enforcement agency is warranted – that is, where reasonable suspicion has been established, the privacy argument might not hold. On the other hand, where no reasonable suspicion exists, a law enforcement agency cannot go sniffing around one's private communications and successfully raise the interest of justice argument in defence.

#### **4.6.3 The question of jurisdiction**

The question of jurisdiction arises at the stage where a cyberlaunderer is apprehended. There is a need to ascertain where such criminal should be prosecuted. This yields several complications, considering the nature of cyberlaundering. Where a criminal operates a website to conduct his activities, it is uncertain whether jurisdiction would be established in the territory from which the suspect operates, or at the place where the website is registered, or the place where the conduct of the criminal is felt. Due to the novel nature of the cyberlaundering concept, it is yet to be adequately classified both, under international law and municipal law. Once this is settled, the relevant laws would have solved the riddle of jurisdiction.

Cyberlaundering falls under the category of cybercrimes, and for this reason, one must have recourse to cyber law as a starting point to determine jurisdiction. In South

---

<sup>214</sup>See sections 3401-3409 of the RFPA and sections 2510(12) of the ECPA.

Africa, for example, section 90 of the ECT Act<sup>215</sup> provides that a South African court would have jurisdiction over the prescribed cyber offences stipulated in the Act in terms of the territoriality principle, the effects principle, or the active personality principle. The ECT Act is a good example because it represents a blend of both UK and US legislations on cyber law.

In terms of the active personality principle, a person who has committed a cybercrime would be prosecuted in the country of which he is a national. In the case of cyberlaundering, it is likely that the criminal would be concurrently charged with the predicate offence which he committed. Since it is very difficult to physically apprehend a cyberlaunderer, the active personality principle might not be entirely suited for cyberlaundering purposes.

In terms of the effects principle, the effects of the crime must have been felt in the country seeking jurisdiction. However, with this principle, it is difficult to establish the actual effect in question because of the volatile nature of cyberlaundering. For example, in light of the typical online gambling scenario where a criminal uses smurfs to play on his online casino, the smurfs could play on such website from different countries around the world. It is almost inconceivable to determine the actual effect of such an operation.

The territoriality principle, therefore, merits consideration. According to this principle, the court will exercise jurisdiction where the offence is committed within the territory of the country seeking jurisdiction. One has to conceive of internet service providers as businesses. Just as a company's registered place of business is the place

---

<sup>215</sup> See footnote 209 supra.

where a summons is served on it in a pending criminal matter, the same principle should apply to websites. Thus, the place where a website is registered should be indicative of where jurisdiction lies in a cyberlaundering case.

The European Union Convention on Cybercrimes<sup>216</sup> also supports the territoriality principle with respect to other cybercrimes. In terms of the Convention's provisions, states parties must prosecute cyber offences in the light of either the territoriality principle or the active personality principle.

Therefore, a cyberlaunderer should be deemed to have committed the crime in the territory where the website he uses as a medium is duly registered. This is, however, not without challenges, especially in countries that are notorious for their poor AML laws. There are numerous websites which are not registered, and which freely operate in these countries. And as these activities go unchecked, cyberlaundering operations are easily fostered.

Overall, international instruments and national laws should be adapted to suit the cyberlaundering scenario. Where cyberlaundering is properly classified and framed, the question of jurisdiction would be properly defined and put in a better perspective.

---

<sup>216</sup> Budapest. 23.XI.2001. Adopted on 12 April 2001, and came into effect on 1 July 2004.

## CHAPTER 5

### EVALUATION

#### 5.1 THE PRESENT: AN OVERVIEW

The subject of cyberlaundering has sadly been constantly evaded.<sup>217</sup> This is probably due to its hybrid character, being a crossroad between law and technology. The aura of vagueness and uncertainty around it does not make it any easier to fit in a particular mould. Given the convolutedness of the problem, as set out above, this paper has sought to unveil the phenomenon of cyberlaundering. This is important because, by identifying and understanding the concept of cyberlaundering and how it operates, one takes the first step towards unravelling the problem. Although possible control mechanisms have been identified, these are merely tentative. By way of contrast, what is not at all tentative is the reality of cyberlaundering and its growing prevalence.

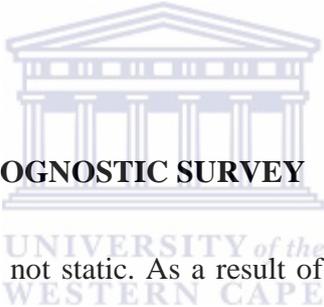
In truth, the gravity of this problem cannot be quantified because of the nature of the internet. The much reiterated feature of anonymity, which forms the root of the various choke points identified, makes it seem as though mere mortals are battling ghosts in the crusade against cyberlaundering. Ironically, because the internet defies the notion of boundaries and jurisdictions, it is extremely difficult to establish jurisdiction over the

---

<sup>217</sup> The fact that not much is known about cyberlaundering is the primary reason why the topic has constantly been avoided. For example, in July 2009, the House of Lords European Union Select Committee issued a report titled “Money Laundering and Financing of Terrorism” <<http://www.parliament.uk/business/committees/committee-archives/>> [accessed on 5 September 2010], yet nowhere does it deal with the issue of cyberlaundering, which is known to be a principal medium to fund terrorism.

crime. Even where jurisdiction can be established,<sup>218</sup> one might still need to answer some other burning legal questions such as those pertaining to privacy.

The impact of cyberlaundering is becoming increasingly evident in the world today. Probably the most glaring of these effects is the fact that the economies of many underdeveloped countries are being crippled by it.<sup>219</sup> Also, from the different scenarios of cyberlaundering that have been discussed, it is clear that cyberlaundering is not always an end in itself, but could be a means to an end. Terrorism could be one of such aims, and because cyberlaundering ties in with terrorist financing, it greases the wheels of terrorist activities.<sup>220</sup>



## 5.2 THE FUTURE: A PROGNOSTIC SURVEY

Technology is certainly not static. As a result of the advent of cyberlaundering and the lessons it teaches, one cannot look forward to new technological advancements without harbouring fears of the loopholes that could further exist for criminal enterprises. This section portends briefly what the future holds for technology, as it concerns cyberlaundering.

With respect to online gaming, the different forms existent now are a far cry of what is yet to come. A few years back, when scientists spoke about the concept of virtual communities, it seemed as though one were reading a fictional movie script like *Star Wars* to a lay audience. But today, it is a reality. Virtual communities are gaining

---

<sup>218</sup> See the theories discussed above in Chapter 4, paragraph 4.6.3.

<sup>219</sup> See Chapter 1, paragraph 1.2 for an elaborate discussion.

<sup>220</sup> This opinion is shared by the Financial Action Task Force. See Financial Action Task Force (2010A: 15).

popularity by the second, and the traditional (non-internet) form of gaming<sup>221</sup> is already old-fashioned in our internet-based world. The predominant gaming companies which have not been offering a virtual community-type game such as PlayStation and Xbox 360 are reportedly going to incorporate virtual communities-type games into their game packages.<sup>222</sup> And what would this mean for cyberlaundering? If the existing loopholes earlier identified in virtual communities<sup>223</sup> are not fixed, criminals would have a field-day using virtual communities as an avenue to further wicked schemes. Not only is the number of participants in the virtual community growing,<sup>224</sup> but also, the addiction to this form of gaming is spawning unprecedented vices.<sup>225</sup>

Mobile phones are also being used increasingly to effect electronic payments. Although present statistics show that mobile phones are more efficient for micro-payments<sup>226</sup> rather than macro-payments,<sup>227</sup> the latter payment form is generally more suited for cyberlaundering. One must not underestimate the potential of cell-phone transactions for money laundering. Having high-tech smart phones (like the iPhone and the BlackBerry), with phenomenal internet browsing features, many can actually access the internet from their cell phones without necessarily sitting in front of a computer. As

---

<sup>221</sup> This would include PC-type games, PlayStations 1 and 2, and Xbox 360.

<sup>222</sup> PlayStation is already incorporating a PlayStation 3 Home feature (which is its own virtual community) in every Play Station 3 console. See Wong (2010: 1).

<sup>223</sup> See paragraph 3.4.6 supra.

<sup>224</sup> Currently, a combined total of 80 million gamers are registered with all the existing virtual communities, and this figure is set to triple to a whopping 240 million by 2015. See Wong (2010: 2).

<sup>225</sup> Recently, a competitor on one of these virtual communities (Legend of Mir 3) killed a co-competitor in real life for stealing a “cyber sword” which he had won in a contest. See Wong (2010: 1).

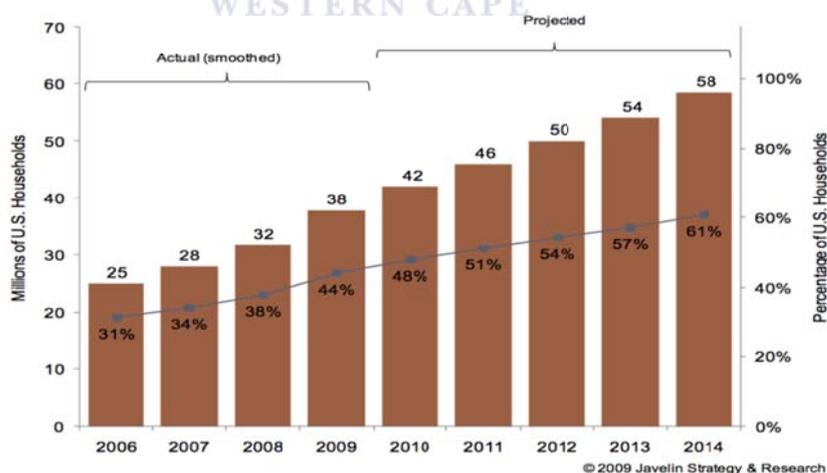
<sup>226</sup> Micro-payments are transactions involving a very small amount of money. PayPal defines micro-payments as transactions involving payments below \$12. See <<http://www.paypal.com/info/micro-payments/>> [accessed on 5 September 2010].

<sup>227</sup> A macro-payment system is the opposite of a micro-payment system, because it involves large amounts of money. What constitutes a large amount of money is a question of fact which will be entirely dependent on the nature of the relevant transaction. Going by the definition given by PayPal (footnote 219), this would be transactions exceeding \$12.

most communities in underdeveloped countries have poor internet facilities, money launderers have plentiful opportunities to use such mobile phones to suit their purposes.

Furthermore, the future will also witness a significant increase in the use of the Peer-to-Peer payment model facilitated by the use of smart cards. As mentioned earlier,<sup>228</sup> this payment system enables a consumer to effect electronic payments without involving a financial institution. The Peer-to-Peer payment system is a common feature of the different cyberlaundering techniques identified earlier.<sup>229</sup> As at 2003, an estimated 250 million Peer-to-Peer payments were made in the United States alone.<sup>230</sup> This estimate only represents about 15% to 20% of the households in the United States. By 2014, it is estimated that over 60% of all households in the United States will be using the Peer-to-Peer payment systems. The graph below shows these projections.<sup>231</sup>

Figure 20: Online Person-to-Person Transfers Actual 2006-2009, Forecast to 2014, by Millions and Percentages of U.S. Households



<sup>228</sup> See paragraph 3.2.2 supra.

<sup>229</sup> See paragraph 3.4 supra.

<sup>230</sup> Global Information Inc. (2004) "Consumer e-payment: What does the Future Hold?" <<http://www.the-infoshop.com/press/iv/>> [accessed on 2 September 2010].

<sup>231</sup> See Sherter (2010: 12).

Should the flaws identified with smart cards go unchecked, the proliferation of smart card usage would mean an increased possibility of cyberlaundering operations. This does not portend well for the future.

### **5.3 RECOMMENDATIONS**

Having discussed some of the aspects of cyberlaundering, including their ramifications, it is submitted that the following recommendations merit consideration:

#### **5.3.1 Bringing cyberlaundering to the centre stage**

The concept of money laundering is constantly evolving. What one might have understood as money laundering in the past decades is not necessarily the case today. Money laundering at present wears the cloak of cyberlaundering. The general myth that criminals are always one step ahead of the law finds a home in the concept of cyberlaundering. Therefore cyberlaundering should be the focal point of researchers, law makers, law enforcement agencies and governments in general and in tandem. This also implies that there is a need to expand the focus of the traditional concept of money laundering, to include cyberlaundering. This would help to give the issue more currency. As a consequence, law makers would for once be steps ahead of the criminal.

It is therefore recommended that money laundering, internet and cyber crime laws be amended to expressly accommodate the new phenomenon of cyberlaundering. In order to foster this expectation, awareness campaigns need to be conducted to educate the

responsible authorities as to its prevalence. Given the hybrid nature of cyberlaundering, further research on it should be encouraged both in the fields of law and computer science. With continuous research on the subject, new possibilities would be uncovered for dealing with the problem.

### **5.3.2 Better policing**

The subject of cyberlaundering is one which requires very careful attention. Specialised agencies, some of which might be known as cyber crime units, must pay better attention to cyberlaundering operations. Possible detection mechanisms can only be discovered with continuous research on the subject, which would aid the relevant enforcement agencies. Also, a government's information technology (IT) body, which also conducts internet supervision, must be on constant alert. These IT institutions must work closely with enforcement agencies for possible detection of cyberlaundering operations. In this regard, a recent innovation known as semantic technology should be used when conducting investigations. The semantic technology can 'automatically identify companies based on language grammar and rules, tag and store relationships such as links, as well as other relations like family relationships, roles and positions and monies or assets.'<sup>232</sup> In essence, money launderers with shell companies on the internet can be exposed easily with this system.

Another crucial area that can only be tackled with the cooperation of IT institutions is the entry barrier system for future internet service providers (ISPs). By sifting through

---

<sup>232</sup> See Mulukutla and Ruegg (2009: 80) for more details.

the viability of these ISPs, a risk management system is conducted. This exercise would be particularly necessary for informal financial service providers like E-gold Ltd (www.e-gold.com).<sup>233</sup> Informal money transmitters can be scrutinized by subjecting them to licensing and registration. With such entry barriers in place, it would be easy to fish out non-registered websites. A non-registered website is a salient characteristic of a website that is operated for money laundering purposes. Most online gambling sites fit tightly in this frame.<sup>234</sup>

However, law enforcement agencies are not the only bodies concerned here. The required intervention also involves financial institutions and electronic card companies, which must give full and unflinching cooperation to the law enforcement agencies by reporting suspicious transactions and fraudulent misuse of smart cards.<sup>235</sup>



### **5.3.3 Extending the term of the FATF beyond 2012**

The FATF has undoubtedly played a phenomenal role in shaping the current anti-money laundering law (AML) regime.<sup>236</sup> The FATF has also helped blaze the trail with regard to cyberlaundering by giving early indications of threat areas like online gambling.<sup>237</sup> The FATF is, however, not a permanently structured body. In 2004, when

---

<sup>233</sup> See the discussion in paragraph 3.4.5 supra.

<sup>234</sup> See paragraph 3.4.4 supra.

<sup>235</sup> In practice this might be easier said than done. This is because most smart card companies (just like other profit-oriented companies) are gain driven. These companies are mostly not welcoming of law enforcement agencies snooping around their business. They might get the impression that third parties might think their business is tainted with illegality. One can allay these fears by enacting laws that would strictly make these companies file suspicious transaction reports.

<sup>236</sup> See paragraph 4.3.2.1 supra.

<sup>237</sup> Financial Action Task Force (2010B: 66). Also see the Financial Action Task Force (2008: 59). See annexure.

the original mandate of the FATF expired, it was again extended to August 2012.<sup>238</sup> As part of its renewed mandate, the FATF has undertaken to conduct typological exercises which would highlight new threat areas of money laundering.<sup>239</sup> Its 2008 report on online gambling is proof of this.<sup>240</sup>

The FATF would certainly need more time to delve into the issue of cyberlaundering. It has little time left to conduct the kind of field work which is required for the problem. Considering the fact that the FATF reports are highly valuable and its recommendations are authoritative, the same weight would be attached to future reports it might issue on cyberlaundering. One harbours the fear that if the FATF's mandate is not extended beyond August 2012, eventual development in the field of anti-cyberlaundering law would be greatly hindered. Conversely, with increasing fears of the dangers posed by new techniques of cyberlaundering, there might be sufficient reasons to give the FATF more time to deal with the situation effectively.

## 5.4 CONCLUSION

In the 1920s, French writer Marcel Labordere said that 'man will never be able to know what money is no more than he will be able to know what God is... [M]oney is not the infinite but the indefinite, an astounding complex of all sorts of psychological as well as material reactions.'<sup>241</sup> Money is thus a sociological phenomenon which shapes

---

<sup>238</sup> See Financial Action Task Force (2004A: 10). One cannot undermine the value of the FATF. In retrospect, the FATF principles and recommendations are now popularly accepted soft law, and have now become the skeletal framework upon which most domestic money laundering legislations are based.

<sup>239</sup> See paragraph 9, Financial Action Task Force (2004A: 13).

<sup>240</sup> Financial Action Task Force (2008: 30). See annexure.

<sup>241</sup> Pollitzer (2001: 1). Also see Presley (1979: 809).

human behaviour. Invariably, an understanding of this phenomenon equates to an understanding of a particular form of human behaviour. The study of money laundering fits within this framework. Human greed and the insatiable depths of the human mind represent the philosophical and sociological explanation for the problem of money laundering. This same explanation holds for the concept of cyberlaundering, even though it appears as another level of money laundering. The evil of cyberlaundering is just another representation of the fact that malignity inheres in the human mind's stream of consciousness.<sup>242</sup>

Thus, if this paper serves an ultimate purpose, it would be to cause a rude awakening, because the journey has only just begun. One cannot afford to lag behind one bit, or be deterred by the many complexities and tangled knots of cyberlaundering. If the right guards are put up in the necessary areas, and with the exercise of due vigilance, this problem would certainly not be insurmountable.

[Word count: 20, 976]

---

<sup>242</sup> This fact is reminiscent of an observation made by the 14<sup>th</sup> century writer, William Shakespeare, that 'the evil that men do lives after them; the good is oft interred within their bones'. Shakespeare (1994: 42).

## LIST OF REFEREENCES

### 1. PRIMARY SOURCES

#### 1.1 International instruments

The European Council Directive, 2002/22/EC. Adopted on 7 March 2002.

The European Union Convention on Cybercrimes 23.XI. Adopted on 12 April 2001, and came into force on 1 July 2004.

The UN Convention against the Illicit Traffic in Narcotic Drugs and Psychotropic Substances. Adopted on 20 December 1988, and came into force on 1 November 1990.

The United Nations Convention against Transnational Organized Crime, Resolution 55/25. Adopted on 15 November 2000 and came into force on 29 September 2003.

The Warsaw Convention: Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism. Adopted on 16 May 2005, and came into force on 1 December 2009.

#### 1.2 Laws

##### 1.2.1 *India*

The Bombay Wager Act IV of 1887.

### **1.2.2 *South Africa***

Electronic Communications and Transactions Act 25 of 2002.

Electronic Telecommunications Act 103 of 1996.

National Gambling Act 7 of 2004.

Regulation of the Interception of Communication and the Provision of Related-Information Act 70 of 2002.

### **1.2.3 *The United Kingdom***

Computer Misuse Act, c.18 of 1990.

Proceeds of Crime Act, c.29 of 2002.



### **1.2.4 *The United States of America***

Electronic Communications Privacy Act 18 of 1986, U.S.C.

Illegal Gambling Business Act 15 of 1970, U.S.C.

Money Laundering Control Act 18 of 1986, U.S.C.

NV Senate Bill 82-75<sup>th</sup> (BDR 14-266). Adopted on 1 July 2009 by the House of Senate, Nevada, United States.

Right to Financial Privacy Act 12 of 1982, U.S.C.

Telecommunications Act 56 of 1996, U.S.C.

The Bank Secrecy Act 31 of 1970, C.F.R.

The Federal Wire Act 87 of 1961, U.S.C.

The Uniting and Strengthening America by Providing Appropriate Tools Required  
To Intercept and Obstruct Terrorism Act 115, Stat. 272 of 2001.

Unlawful Internet Gambling Enforcement Act 4 of 2006.

### 1.3 Case law

*California Bankers Association v Schultz* 39 L Ed 2d 812 (1974).

*California Bankers Association v Schultz* US Supreme Court 416 21 (1974).



### 1.4 Official reports

Drug Enforcement Administration (2010) “Briefs and Background, Drugs, Drug  
Abuses and State factsheets” <<http://www.justice.gov/dea/programs/money.html>>  
[accessed on 30 July 2010].

E-Standard Forum (2009) “Anti-Money Laundering /Combating Terrorist  
Financing Standard” <<http://www.estandardforum.org/southafrica/>> [accessed on  
21 September 2001].

Financial Action Task Force (1997) “1996-1997 Report on Money Laundering Typologies” <<http://www.fatf-gafi.org/dataoecd/31/29/34043795.pdf>> [accessed on 5 March 2010].

Financial Action Task Force (2001) “Report on Money Laundering Typologies” <[http://www.fatf-gafi.org/reports/money\\_laundering\\_typologies/](http://www.fatf-gafi.org/reports/money_laundering_typologies/)> [accessed on 31 June 2010].

Financial Action Task Force (2002) “FATF Annual Report for 2001-2002” <<http://www.fatf-gafi.org/dataoecd/43/53/34949558.pdf>> [accessed on 5 March 2010].

Financial Action Task Force (2003) “FATF 40 Recommendations, plus 9 Special Recommendations” <[http://www.fatf-gafi.org/dataoecd/forty\\_recommendations/](http://www.fatf-gafi.org/dataoecd/forty_recommendations/)> [accessed on 2 September 2010].

Financial Action Task Force (2004A) “Mandate Renewed For 8 years” <<http://www.fatf-gafi.org/dataoecd/09102/>> [accessed on 2 September 2010].

Financial Action Task Force (2004B) “Revised Interpretative Notes on Special Recommendation VII: Wire Transfers” <[http://www.fatf-gafi.org/dataoecd/revised\\_notes/](http://www.fatf-gafi.org/dataoecd/revised_notes/)> [accessed on 08 August 2010].

Financial Action Task Force (2006) “Money Laundering: Report on New Payment Methods” <<http://www.fatf-gafi.com/documents/51/>> [accessed on 5 September 2010].

Financial Action Task Force (2008) “Report on Casinos” <<http://www.fatf-gafi.org/dataoecd/5/61/41584370.pdf>> [accessed on 25 July 2010].

Financial Action Task Force (2010A) “Global Money Laundering and Terrorist Financing Threat Assessment” <<http://www.fatf-gafi.com/documents/51/>> [accessed on 5 September 2010].

Financial Action Task Force (2010B) “Money Laundering and the Vulnerability of Free Trade Zones” <[http://www.fatf-gafi.org/pages/0,2987,en\\_32250379\\_32235720\\_1\\_1\\_1\\_1\\_1,00.html](http://www.fatf-gafi.org/pages/0,2987,en_32250379_32235720_1_1_1_1_1,00.html)> [accessed on 31 June 2010].

Financial Action Task Force (2010C) “Money Laundering and Terrorist Financing: Vulnerabilities of Commercial Websites and Internet Payment Systems” <[http://www.fatf-gafi.org/resource\\_file678/](http://www.fatf-gafi.org/resource_file678/)> [accessed on 8 August 2010].

Financial Crimes Enforcement Network (1995) “Minutes of the meeting of the Congress Banking Committee, FinCEN (12 November 1995)” <<http://www.fincen.org/resource/>> [accessed on 17 June 2010].

Financial Crimes Enforcement Network (2008) “Strategic Plan for the Fiscal Years of 2008-2012” <[http://www.fincen.gov/about\\_fincen/wwd/](http://www.fincen.gov/about_fincen/wwd/)> [accessed on 9 August 2010].

Financial Crimes Enforcement Network (2009) “Annual Report: Fiscal Year of 2009”

<[http://www.fincen.gov/news\\_room/rp/files/YEreport/FY2009/annualreport.html](http://www.fincen.gov/news_room/rp/files/YEreport/FY2009/annualreport.html)>  
[accessed on 22 June 2010].

Financial Crimes Enforcement Network (an undated report) “Money in Cyberspace” <<http://www.fincen.org/resource-moneyincyberspace/1212>> [accessed on 17 June 2010].

House of Lords: European Union Select Committee (2009) “Money Laundering and Financing of Terrorism”  
<<http://www.parliament.uk/business/committees/committee-archives/>> [accessed on 5 September 2010].

Mindark Ltd (2009) “Semi-Annual Report for Second Quarter: January-June 2009”  
<<http://www.mindark.com/press/financial-reports/documents/>> [accessed on 31 July 2010].



Organisation for Economic Cooperation and Development (2001) “Basic Facts about Money Laundering” <<http://www.oecd.org/fatf>> [accessed on 12 March 2010].

The Basel Committee on Banking Supervision (2010) “Vendor model for risk measurement and management” *Basel Committee on Banking Supervision: Working Paper 17* February 2010 <<http://www.bis.org/publ/bcbs/>> [accessed on 22 August 2010].

The Basel Committee on Banking Supervision (2001) “Customer due diligence for banks” *Basel Committee on Banking Supervision: Working Paper 012* October 2001 <<http://www.bis.org/publ/bcbs/>> [accessed on 22 August 2010].

The International Finance Corporation (2009) “Annual Reports” <<http://www.cait.gov.kw/>> [accessed on 30 July 2010].

The National Drug Intelligence Program (2010) “National Drug Threat Assessment 2010” <<http://www.justice.gov/ndic/pubs38/38661/38661ip.pdf>> [accessed on 31 July 2010].

The United States Government Accounting Office (2009) “Internet Gambling, An Overview of the Issues” <<http://www.gao.gov/new.item/do389.pdf>> [accessed on 20 July 2010].

The United States Treasury (2007) “The 2007 National Money Laundering Strategy” <<http://www.treas.gov/press/releases/docs/nmls.pdf>> [accessed on 29 July 2010].

The Wolfsberg Group (2010) “The Wolfsberg Principles” <<http://www.wolfsberg-principles.com/resource/files/>> [accessed on 14 August 2010].

## 2. SECONDARY SOURCES

### 2.1 Books

Beare, ME (2005) *Critical Reflections on Transnational Organized Crime, Money Laundering and Corruption* University of Toronto Press: Toronto.

Blunden, B (2001) *The Money Launderers, how they do it, and how to catch them at it...* Management Books: Gloucestershire.

Grabosky, P and Smith, R (1998) *Crime in the Digital Age, Controlling Telecommunications and Cyberspace Illegalities* The Federation Press: Sydney.

Lilley, P (2006) *Dirty Dealing: The Untold Truth About Global Money Laundering, International Crime and Terrorism* (3<sup>rd</sup> ed) Kogan Page: London.

Pillai, K and Julian, A (2008) *Prevention of Money Laundering Legal and Financial Issues* The Indian Law Institute: New Delhi.

Reichel, P (ed) (2005) *Handbook of Transnational Crime and Justice* Sage: Los Angeles.

Reuter P and Truman, H (2004) *Chasing Dirty Money: The Fight against Money Laundering* Peterson Institute for International Economics: Washington DC.

Robinson, J (1998) *The Laundrymen, Inside the World's Third Largest Business* (2<sup>nd</sup> ed) Pocket Books: London.

Shakespeare, W (1994) *Julius Caesar* Heinemann: Auckland.

## 2.2 Chapters from books

Madinger, J (2006) “Basic Money Laundering Schemes” in Madinger, J *Money Laundering: A Guide for Criminal Investigators* (2<sup>nd</sup> ed) Taylor and Francis: Boca Raton.

Marshall, CE et al (2005) “Computer Crime in Brave New World” in Reichel, P *Handbook of Transnational Crime and Justice* Sage: Los Angeles.

Mulukutla, H and Ruegg, M (2009) “The Importance of Information Technology in Tracing Stolen Assets” in Basel Institute of Governance *Tracing Stolen Assets: A Practitioner’s Handbook* Basel Institute of Governance: Basel.

Richards, JR (1999) “An Introduction to Money Laundering” in Richards, JR *Transnational Criminal Organizations, Cybercrime, and Money Laundering* CRC Press: Boca Raton.

Shams, H (2004) “Money Laundering Law: History and Scope” in Shams, H *Legal Globalization: Money Laundering Law and Other Cases* British Institute of International and Comparative Law: London.

## 2.3 Journal Articles

Atta-Asamoah, A (2009) “Understanding the West African Cyber crime process” 18(4) *African Security Review: Organised Crime Trends in Africa* 107.

- Filipkowski, W (2008) “Cyber laundering: An analysis of typologies and techniques” 3(1) *International Journal of Criminal Justice Sciences* 233.
- Hinsterseer, K (1997) “An Economic Analysis of Money Laundering” 1(6) *Journal of Money Laundering Control* 154.
- Kellerman, T (2004) “Money Laundering in Cyberspace” 11(15) *The World Bank Financial Sector Working Paper* 1.
- Musimanga, DA et al (1998) “Exploring Money Laundering Vulnerabilities Through Emerging Cyberspace Technologies – A Caribbean-based Exercise” 1(2) *RAND and Critical Technologies Institute* 54.
- Philippsohn, S (2001) “Money Laundering on the Internet” 20(6) *Computers & Security* 485.
- Philippson, S (2001) “The Dangers of New Technology - Laundering on the Internet” 1(5) *Journal of Money Laundering Control Thomason* 89.
- Ping, H (2004) “New Trends in Money Laundering – From the Real World to Cyberspace” 5(1) *Journal of Money Laundering Control* 50.
- Presley, JR (1979) “Marcel Labordere: A Neglected French Contribution to the Trade Cycle Theory” 1(32) *Kyklos: International Review for Social Sciences* 809.
- Shazeeda, AA (1998) “A Gateway for Money laundering? Financial Liberalisation in Developing and Transitional Economies” 1(6) *Journal of Money Laundering Control* 322.

Straub, JP (2002) “The Prevention of E-Money laundering: Tracking the Elusive Audit Trail” (25) *Suffolk Transnational Law Review* 534.

Zeldin, MF and Florio, CV (2007) “Strengthening Laws and Financial Institutions to Combat Emerging Trends in Money Laundering” 2(4) *Journal of Money Laundering Control* 412.

## **2.4 Unpublished work**

Jamali, MS (2009) “Cyber Laundering”

A Master’s thesis submitted to the School of Computing Information Technology and Engineering, University of East London, on 25 May 2009, in partial fulfilment of the requirement of Masters of Science in Information Security and Computer Forensics. Available at <<http://www.scribe.com/resources/cyberlaundering09811>> [accessed on 2 June 2010].

## **2.5 Internet resources**

### **2.5.1 Internet articles**

Ask “E-Payments” <[http://www.ask.com/what is e-money?/files/e\\_payment\\_systems/](http://www.ask.com/what%20is%20e-money?/files/e_payment_systems/)> [accessed on 8 June 2010].

Bortner, M (1996) “Cyberlaundering: Anonymous Digital Cash and Money Laundering” <<http://osaka.law.miami.edu/~froomkin/seminar/papers/bortner.htm>> [accessed on 12 April 2010].

Bumeter, BH (2001) “Cyberlaundering: Low Tech Meets High Tech” *Maven Mappers Information* <<http://www.softduit.com/mavenmappersinformation/2001/06/07/1cyberlaundering-low-tech-high-tech/>> [accessed on 21 July 2010].

Drug Enforcement Administration (2007) “National Money laundering Strategy” <<http://www.treas.gov/press/releases/docs/nmls.pdf>> [accessed on 29 July 2010].

E-Standard Forum (2010) “Anti-Money Laundering/Combating Terrorist Financing Standard” <<http://www.estandforum.org/southafrica/>> [accessed on 21 September 2010].

eHow (2009) “How to Launder Money” <[http://www.ehow.com/how\\_2049841\\_launder-money.html](http://www.ehow.com/how_2049841_launder-money.html)> [accessed on 5 March 2010].

eHow (2010) “How SWIFT wires funds” <<http://www.ehow.com/swift/>> [accessed on 4 June 2010].

Global Information Inc. (2004) “Consumer e-payment: What does the Future Hold?” <<http://www.the-infoshop.com/press/iv/>> [accessed on 2 September 2010].

Grow, B (2006) “Gold Rush” *Business Week* (an online news article dated 9 January 2006) <[http://www.businessweek.com/magazine/content/06\\_02/b3966094.htm](http://www.businessweek.com/magazine/content/06_02/b3966094.htm)> [accessed on 1 May 2010].

Molander, RC et al (1998) “Cyberpayments and Money Laundering: Problems and Promises” *RAND Monograph Report* (MR-965-OSTP/FINCEN) <<http://www.rand.org/scitech/stpi/Agenda/public.html>> [accessed on 22 June 2010].

Organisation for Economic Cooperation and Development (2002) “Glossary of statistical terms” <<http://www.bis.org/publ/cpssoob.pdf>> [accessed on 23 March 2010].

Pollitzer, B (2001) “The Future of Electronic Payments” <<http://www.bakersonline.com/e-banking/>> [accessed on 24 September 2010].

Sherter, A (2010) “P2P Payments are Coming, and the Credit Card Companies Won’t Like It” <<http://www.bnet.com/blog/financial-business/p2ppayments/>> [accessed on 2 September 2010].

Singh, VK (2009) “Controlling Money Laundering in India- Problems and Perspectives” <[http://www.igidr.ac.in/~money/mfc-11/Singh\\_Vijay.pdf](http://www.igidr.ac.in/~money/mfc-11/Singh_Vijay.pdf)> [accessed 16 March 2010].

Thomason, CV (2009) “How has the establishment of the internet changed the way offenders launder their dirty money?” *Internet Journal of Criminology* (10 July 2009) <<http://www.internetjournalofcriminology.com>> [accessed 16 March 2010].

Wikipedia (2009) “Virtual Worlds” <<http://www.en.wikipedia.org/wilg/virtual-world/>> [accessed on 22 July 2010].

Wikipedia (2010) “Money Laundering”  
<[http://www.wikipedia.com/money\\_laundering/](http://www.wikipedia.com/money_laundering/)> [accessed on 20 August 2010].

Wong, D (2008) “A World of Warcraft World: 10 Ways Online-Gaming Will Change the Future” <<http://www.cracked.com/article-15657/>> [accessed on 4 September 2010].

### 2.5.2 Websites

Association for Payment Clearing Services  
<[http://www.apacs.org.uk/resources\\_publications/card\\_facts\\_figurse.html](http://www.apacs.org.uk/resources_publications/card_facts_figurse.html)>  
[accessed 12 June 2010].

Barclaycard  
<<http://www.barclaycard.co.uk/>> [accessed on 1 August 2010].

Cybercash  
<<http://www.cybercash.com/about/>> [accessed on 20 March 2010].

Drug Enforcement Administration  
<<http://www.justice.gov/dea/programs/money.html>> [accessed on 30 July 2010].

### E-gold

<<http://www.e-gold.com/unsecure/qanda.html>> [accessed on 14 July 2010].

### Fact Finder

<[http://www.fact-finder.com/file/money\\_laundering/](http://www.fact-finder.com/file/money_laundering/)> [accessed on 31 July 2010].

### Financial Action Task Force

<<http://www.fatf-gafi.org/>> [accessed on 8 August 2010].

### Financial Crimes Enforcement Network

<[http://www.fincen.gov/about\\_fincen/wwd/](http://www.fincen.gov/about_fincen/wwd/)> [accessed on 9 August 2010].



### Freedom Eagle Card

<<http://www.freedom-card.co.uk/>> [accessed on 2 September 2010].

### International Monetary Fund

<<http://www.imf.org/about/projects/worldbank>> [accessed on 13 August 2010].

### Living Internet

<[http://www.livinginternet.org/file\\_crypt](http://www.livinginternet.org/file_crypt)> [accessed on 16 August 2010].

### MONDEX

<<http://www.mondex.com/about/>> [accessed on 20 March 2010].

#### National Accountability Bureau

<<http://www.nab.gov.pk/about/>> [accessed on 08 August 2010].

#### National Statistics Online

<<http://www.statistics.gov.uk/CCI/nugget.asp?ID=8&Pos=1&ColRank=1&Rank=192>> [accessed on the 15<sup>th</sup> of March, 2010].

#### Octopus card

<<http://www.octopuscards.com/>> [accessed on 24 August 2010].

#### Oyster card

<<http://www.tfl.gov.uk/oyster/>> [accessed on 12 September 2010].

#### PayPal

<<http://www.paypal.com/about/>> [accessed on 20 March 2010].

#### Red Plc

<<http://www.redplc.com/about/PRISM/>> [accessed on 16 August 2010].

#### Second Life

<<http://www.secondlife.com/corporate/vat.php>> [accessed on 23 July 2010].

### The Times

<<http://www.timesonline.co.uk/tol/news/politics/article620834.ece>> [accessed on 21 July, 2010].

### Virgin card

<<http://www.virgin.co.uk/pre-paidcards/>> [accessed on 9 June 2010].

### Visa

<<http://www.visa.com/>> [accessed on 19 August 2010].

### WiseGeek

<<http://www.wisegeek.com/what-is-online-banking92338>> [accessed on 12 June 2010].



## ANNEXURE

### THE FATF 2008 REPORT ON CASINOS

*The essential threats arising from online casinos in comparison to traditional casinos are elucidated in the FATF 2008 Report on Casinos.*<sup>243</sup>

107. Internet casinos may wish to check customer location because of the additional risks arising from transnational operations.

#### Transaction risk

109. Casinos should consider operational aspects (*i.e.* products, services, games, and accounts/account activities) that can be used to facilitate money laundering and terrorist financing activities. In addition, land-based and Internet casinos have the following potential transaction risks:

Proceeds of crime. However money is transferred to a casino, there is a risk that this money will have arisen from illegal activities such as check fraud, credit/debit card fraud, narcotics trafficking, theft from employer. Paying greater attention to high spenders/rollers will be helpful in mitigating this risk.

---

<sup>243</sup> FATF Report on Casinos (2008) <<http://www.fatf-gafi.org/dataoecd/5/61/41584370.pdf>> [accessed on 25 July 2010].

Cash. Customers may use a land-based casino to exchange large amounts of illicit proceeds denominated in small bills for larger ones that are easier to hide or transport. Also, certain cash deposits by a customer, especially cash deposits which are considered relatively large either in relation to *i)* a particular casino's average receipts, or *ii)* what is known about a customer's financial status.

The majority of payments to Internet casinos are made directly from financial institution accounts. However, Internet casinos can operate as part of mixed gambling chains which also include betting shops and/or land-based casinos. It may be possible for customers to provide land-based outlets with cash which can then be credited to Internet casino accounts. Internet casinos should work closely with their land-based counterparts that initially receive the cash to ensure that CDD measures are applied, including verifying that the depositor is the account holder, and when appropriate, benefit is secured from the personal contact between land-based casino staff and customers.

#### Transfers between customers

If Internet casinos wish to allow inter-account transfers between their customers they should devise careful policies and procedures which monitor the amount of the transfer(s). Internet casinos may also be aware of customers transferring money between themselves more informally without using their casino accounts, which should be taken into consideration in the casino operator's risk assessments.

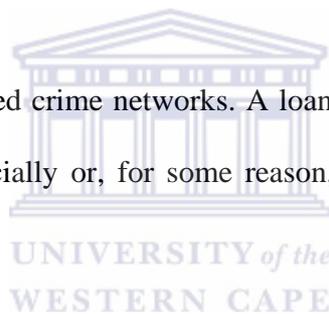
Land-based casinos may also be aware of customers borrowing money from non-conventional sources, including other customers. Informal money lending can be illegal,

and it can also offer criminals an opportunity to introduce proceeds of crime, usually cash, into the legitimate financial system through the casino. Again, this can pose a heightened risk.

Loan Sharking (also known as usury). Casinos in some countries have a problem with this activity which is a crime that involves loaning money to individuals at an interest rate that is above a maximum legal rate, sometimes collected under threat of violence.

Loan sharks may be financed

and supported by organized crime networks. A loan shark usually preys on individuals who are struggling financially or, for some reason, are unwilling to seek credit from legal sources.



- Use of casino deposit accounts. Casinos will wish to encourage their customers to only use their deposit accounts for gambling purposes. Casinos need to consider what constitutes an abuse of such an account and should have policies, procedures, and internal controls, to prevent customers from using such accounts to deposit and withdraw without gambling or minimal play.

- Redemption of Chips, Tickets or Tokens for Currency. Casinos in some countries do not require that customers provide identification for the redemption of chips, tickets, or tokens unless it triggers government reporting thresholds. For a customer that has an

established casino account number,<sup>8</sup> a casino, which is not required by governmental regulations to record such transactions at the cage, nonetheless should have policies, procedures, and internal controls to identify large redemptions<sup>9</sup> to such a customer that were paid with currency<sup>10</sup> (including any large cash outs without gambling for large denomination bills), or through issuance of a cheque.

110. There are a number of specific transaction issues which apply to Internet casinos (including “mobile casinos”):

*Multiple casino accounts or casino wallets.*

An internet operator may own and control multiple web sites. Single web sites can also offer a range of different types of gambling. Operators will need to monitor customers' aggregate position across the whole of their casino business.

Customers may wish to separate the different types of gambling they are conducting with the same operator, or through the same web site, for legitimate reasons, *e.g.* to monitor their performance in different areas. Casinos should implement procedures and systems to assist in the identification of customers opening multiple accounts or wallets for dishonest or inappropriate reasons, including attempting to obscure their spending levels, or to avoid checks undertaken at a threshold level.

*Changes to financial institution accounts.* Casino customers commonly use their accounts with financial institutions to gamble over the internet. Customers may hold a number of financial institution accounts, and they may wish to change which of these

accounts they use in the casino. Casinos may wish to consider updating customer due diligence following such changes.

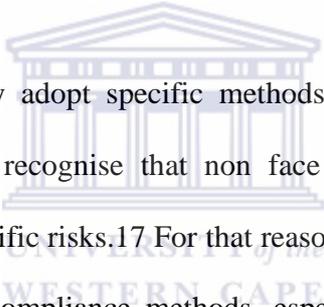
. *Identity fraud.* Details of financial institution accounts may be stolen and used on web sites. Stolen identities may also be successfully used to open financial institutions accounts, and such accounts may also be used on web sites. Internet Provider (IP) Number checks are useful in preventing criminals from opening multiple casino accounts using stolen identities, using the same computer. Casinos will be aware of these risks because of the 'charge back' system. Internet casinos also have a responsibility to protect their customers from having their identities stolen when using their web site, and will therefore wish to provide adequate security.

. *Pre paid cards.* Using cash to fund a pre-paid card poses similar risks as cash. Casinos cannot make the same level of cross reference checks on some types of pre paid cards as they are able to perform on financial institution accounts.

. *Electronic wallets (e- wallets).* Not all e-wallets are licensed in reputable countries, and a number of e-wallets accept cash as deposits. However, e-wallets which only accept money from financial institution accounts in the customer's name will not usually pose any greater or lesser money laundering risk than if funds are received directly from the financial institution. However Internet casinos should be aware that when customers make payments into e-wallets from their financial institution accounts, the statements issued by their financial institutions may only record the payment to the e-wallet, not the transaction to the Internet casino. This may be useful for dishonest customers who wish to disguise their gambling. (See

paragraph below regarding the related issue of casinos purposefully obscuring payments made to financial institution accounts held by customers).

. *Games involving multiple operators.* Poker games often take place on platforms (*i.e.* a central computer system that links electronic gambling devices for purposes of game selection, operation, monitoring, security, and auditing) shared by a number of different casino operators. The platform is likely to play a key role in monitoring the pattern and value of play for potential money laundering activities, *e.g.* chip dumping. The operator and the platform should have clear policies in respect to respective roles, alerts, enquiries, and subsequent actions, for AML/CFT.



121. Internet casinos may adopt specific methods of customer's identification. The FATF Recommendations recognise that non face to face business relationships or transactions can carry specific risks.<sup>17</sup> For that reason non face to face business requires alternative or additional compliance methods, especially in the area of CDD. These methods may rely upon new technologies, including the deposit and withdrawal methods offered on the website, and checks on the customer's IP address.

122. In the majority of cases Internet casinos do not meet their clients, except perhaps their high spenders. Internet casinos are therefore usually unable to form social relationships with them, or to form judgements as a result of those relationships. They are also unable to verify customer's physical appearance against photographic identification documents.

123. If casinos use software systems to assist with CDD the software should access a range of positive and negative checks. Although not available in all countries, public source data can be particularly valuable in identifying PEP's and individuals subject to various sanctions, as well as identifying associations with organised crime and/or terrorist financing activities. In addition, casinos may wish to do Internet searches in an effort to obtain additional information about a customer (see also paragraph 138 below).

124. If basic database checks are not sufficient, perhaps because of a raised risk level, Internet casinos can use a variety of other checks: *i)* traditional checks using customer's personal and official documents; *ii)* checks on customers' source of funds;<sup>18</sup> *iii)* using direct contact via telephone or email, using personal or electronic means.

128. With regard to Internet casinos, checks may be made on the location of the computer used when casino accounts are opened, or during gambling, including IP checks<sup>19</sup>. IP addresses provide information about the country where the computer being used is located.

129. It may be helpful to cross reference IP number information about jurisdiction with *i)* personal data provided by the player and the data provider by the Internet service provider; *ii)* the information the customer provides about their postal address and *iii)* if

payment is made to the casino from a financial institution account, the country where the financial institution account is held, which may be ascertainable from a BIN check.

130. Internet casinos are dependent upon IT systems. These IT systems should be adapted to ensure accurate monitoring of accounts and customers, and to ensure that adequate records are kept and retained. Decisions may need to be made about the necessary level of details of the transaction records which are retained. A risk based approach cannot solely rely upon IT, there must also be an element of human supervision and staff levels should be proportionate to risk levels.

