THE LEGAL REGIME FOR ANTI-CYBERLAUNDERING

BY

DANIEL ADEOYE LESLIE

A thesis submitted in fulfilment of the requirements for the degree Doctor of Laws in the Faculty of Law of the University of the Western Cape, South Africa

Supervisor:

Professor Lovell Fernandez

Faculty of Law

University of the Western Cape

4 October 2012
DECLARATION

I, Daniel Adeoye Leslie, declare that The Legal Regime for Anti-Cyberlaundering is my work and that it has not been submitted for any degree or examination in any other university or institution. All the sources used, referred to or quoted have been duly acknowledged.

Daniel Adeoye Leslie

Signed................................

4 October 2012

UNIVERSITY of the WESTERN CAPE
ACKNOWLEDGMENTS

I thank God for the strength, fortitude and grace given to me to undertake this thesis. I am beholden in gratitude to my supervisor, Professor Lovell Fernandez, of the Faculty of Law, University of the Western Cape, Bellville, South Africa, and Co-Director of the South African-German Centre: Criminal Justice Division. I am grateful for his assiduous supervision and careful guidance. I am also grateful for his constructive criticism always given timeously; and for his detailed attention and always prompt, searching and insightful comments on my drafts. My very special thanks goes to Professor Gehard Werle, of the Faculty of Law, Humboldt University, Berlin, Germany, and Co-Director of the South African-German Centre: Criminal Justice Division, for his guidance and unwaning support throughout the research, and for making it possible for me to carry out the needed research in Germany.

I am deeply indebted to the Deutscher Akademischer Austausch Dienst (German Academic Exchange Service) for funding the research and for causing it to become reality. I heartily thank Dr. Moritz Vormbaum for his kind assistance and support during the research. I am also grateful to Dr. Paul Christoph Bornkamm for availing himself, lending his advice and encouragement during the research. I would also like to acknowledge the help of Mr. Jonathan Hancock for his editorial assistance with the thesis.

I thank Mr. Nicolas von zur Mühlen, of the Max Planck Institute for Foreign and International Criminal Law, Freiburg, Germany, for his help and assistance.
during my research stay at the Institute. I owe gratitude as well to Frau Anja Schepke and Frau Ulrike Brodien for their helpful administrative support, and for making my research stay in Germany most comfortable. I also acknowledge the kind assistance of the library staff of the Peace Palace Library, The Hague, the Netherlands, as well as the library staff of the Law Libraries of Humboldt University, Berlin, Germany, and of the University of Leiden, Leiden, the Netherlands. I thank Ms. Sylvia Papadoupoulos, of the Faculty of Law, University of Pretoria, Pretoria, South Africa, for her advice and guidance since the start of the research. I also thank Ms. Elzet Hurter, of the Faculty of Law, University of Pretoria, Pretoria, South Africa, who has remained very supportive of me.

My most profound depth of gratitude goes to my family. I am grateful for the incorruptible values instilled in me from very early in life by my late father, Hon. Justice Dr. Sunday Idowu Leslie and my mother, Mrs. Magaret Modupe Leslie. I appreciate my siblings, Kayode Leslie, Tayo Leslie, Yetunde Leslie, Bimbo Leslie, Vera Leslie, Kenneth Leslie, Buki Leslie and Bolanle Leslie, for their unwavering love and support.

I would also like to thank my colleagues, Juliet Okoth, Sostenes Materu and Windell Nortjie, as well as my friends in South Africa, Germany, the Netherlands and Nigeria who have kept me in their thoughts and prayers during the course of the research.
TABLE OF CONTENTS

Declaration ii
Acknowledgement iii
Table of Contents v
Abstract xvii
Key words and Abbreviations xviii

CHAPTER 1
INTRODUCTION

1.1 PROLOGUE 1
1.2 EPISTEMOLOGICAL BASIS OF STUDY 1
1.3 SIGNIFICANCE OF STUDY 3
1.3.1 The problem of cyberlaundering: A legal concern 3
1.3.1.1 Cyberlaundering and organized crime 5
1.3.1.2 Cyberlaundering and terrorism 6
1.3.1.3 Cyberlaundering and the world economy 7
1.3.2 The non-existence of a proper ACL legal regime 9
1.4 LITERATURE SURVEY 10
1.5 FOCUS OF STUDY 12
1.5.1 Research question 12
1.5.2 Aims and objectives of study 13
1.6 SCOPE OF STUDY 15
1.7 METHODOLOGY 16
1.8 STUDY OUTLINE 17
CHAPTER 2
MONEY LAUNDERING AND CYBERCRIME:
A BACKGROUND STUDY

2.1 INTRODUCTION 20

2.2. MONEY LAUNDERING: AN OVERVIEW 20

2.2.1 Understanding the meaning of money laundering 20

2.2.2 The history and evolution of the
    anti-money laundering legal regime 24

2.2.2.1 The regulation and prevention phase 25

2.2.2.2 The criminalization and internationalization phase 28

2.2.2.3 The supranationalization phase 30

2.2.2.4 The terrorist financing phase 31

2.2.3 The process of money laundering 32

2.2.3.1 Placement 33

2.2.3.2 Layering 34

2.2.3.3 Integration 36

2.2.4 Money laundering techniques 37

2.2.4.1 Cash 37

2.2.4.1.1 Cash smuggling 38

2.2.4.1.2 Cash structuring/Smurfing 38

2.2.4.2 Wagering 40

2.2.4.2.1 Casinos 40

2.2.4.2.2 Horse racing and lotteries 41

2.2.4.3 Insurance policies 41

2.2.4.4 Securities 42

2.2.4.5 Hawala 42
2.2.4.6 ‘Shell’ companies 43
2.2.4.7 Wire transfer 44
2.2.4.7.1 What it means 44
2.2.4.7.2 The mechanism 45
2.2.4.7.3 The problem 46
2.2.5 Money laundering and rising challenges: Impact and weight of the problem 47

2.3 AN INTRODUCTION TO CYBERCRIME:
THE ‘CYBER ROOT’ OF CYBERLAUNDERING 51
2.3.1 General 51
2.3.2 Understanding the term ‘cybercrime’ 52
2.3.3 The evolution of cybercrime in brief 55
2.3.4 The present state of the anti-cybercrime: an overview 56
2.3.4.1 Advantages of ICT for criminal enterprises 57
2.3.4.2 Challenges of the present anti-cybercrime regime 58
2.4 SUMMARY 61

CHAPTER 3
CYBERLAUNDERING: CONCEPT AND PRACTICE

3.1 INTRODUCTION 62
3.2 DECRYPTING CYBERLAUNDERING 63
3.2.1 The meaning of cyberlaundering 63
3.2.2 Catalysts of the cyberlaundering dilemma 64
3.2.2.1 Speed of technology 64
3.2.2.2 Access to the internet 65
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2.2.3 Anonymity</td>
<td>69</td>
</tr>
<tr>
<td>3.2.2.4 Boundless borders</td>
<td>70</td>
</tr>
<tr>
<td>3.2.3 Categorizing cyberlaundering</td>
<td>72</td>
</tr>
<tr>
<td>3.2.3.1 Cyberlaundering as a subset of cybercrime</td>
<td>73</td>
</tr>
<tr>
<td>3.2.3.2 Cyberlaundering as a technique of money laundering</td>
<td>73</td>
</tr>
<tr>
<td>3.2.3.3 Cyberlaundering: ‘Money Laundering 2.0’</td>
<td>74</td>
</tr>
<tr>
<td>3.2.4 Elements of the crime of cyberlaundering:</td>
<td>76</td>
</tr>
<tr>
<td>A deductive analysis</td>
<td></td>
</tr>
<tr>
<td>3.2.4.1 Elements of crime: money laundering and cybercrime</td>
<td>77</td>
</tr>
<tr>
<td>3.2.4.2 Elements of the crime of cyberlaundering</td>
<td>79</td>
</tr>
<tr>
<td>3.2.4.2.1 Actus reus</td>
<td>79</td>
</tr>
<tr>
<td>3.2.4.2.2 Mens rea</td>
<td>83</td>
</tr>
<tr>
<td>3.3 ELECTRONIC PAYMENT SYSTEMS: NEW TOOLS FOR LAUNDERING</td>
<td>87</td>
</tr>
<tr>
<td>3.3.1 Electronic money</td>
<td>89</td>
</tr>
<tr>
<td>3.3.2 Models of electronic payment systems</td>
<td>92</td>
</tr>
<tr>
<td>3.3.2.1 The merchant-issuer model</td>
<td>93</td>
</tr>
<tr>
<td>3.3.2.2 The bank-issuer model</td>
<td>94</td>
</tr>
<tr>
<td>3.3.2.3 The non-bank issuer model</td>
<td>94</td>
</tr>
<tr>
<td>3.3.2.4 The peer-to-peer model</td>
<td>95</td>
</tr>
<tr>
<td>3.3.3 Storing methods and examples of electronic money</td>
<td>96</td>
</tr>
<tr>
<td>3.3.3.1 ‘Software money’</td>
<td>96</td>
</tr>
<tr>
<td>3.3.3.2 ‘Real time or prepaid tokens’</td>
<td>97</td>
</tr>
<tr>
<td>3.3.3.3 ‘Electronic cheques’</td>
<td>101</td>
</tr>
<tr>
<td>3.3.3.4 ‘Alternative methods: The e-barter system’</td>
<td>102</td>
</tr>
</tbody>
</table>
3.4 CYBERLAUNDERING AND THE THREE-PRONGED PROCESS

3.4.1 Placement
3.4.2 Layering
3.4.3 Integration

3.5 VULNERABLE INDUSTRIES AND TECHNIQUES OF CYBERLAUNDERING

3.5.1 Online banking
3.5.1.1 Examples of cyberlaundering through online banking
3.5.2 Online auctioneering
3.5.2.1 Example of cyberlaundering through online auctioneering
3.5.3 Online gambling
3.5.3.1 Example of cyberlaundering through online gambling
3.5.4 Online barter trade
3.5.4.1 Example of cyberlaundering through online barter trade
3.5.5 Virtual worlds
3.5.5.1 Example of cyberlaundering using virtual worlds

3.6 WHAT THE FUTURE HOLDS FOR CYBERLAUNDERING

3.6.1 The advent of mobile payment systems
3.6.2 Growth in predicate offences for cyberlaundering

3.7 SUMMARY
### CHAPTER 4
THE PRESENT LEGAL FRAMEWORK AGAINST CYBERLAUNDERING: A SURVEY OF RELEVANT LAWS AND POLICIES

<table>
<thead>
<tr>
<th>Section</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 INTRODUCTION</td>
<td>143</td>
</tr>
<tr>
<td>PART 1</td>
<td></td>
</tr>
<tr>
<td>4.2 AN OVERVIEW OF THE CURRENT AML LEGAL REGIME</td>
<td>144</td>
</tr>
<tr>
<td>4.2.1 General</td>
<td>144</td>
</tr>
<tr>
<td>4.2.2 Pillar 1: Prevention</td>
<td>147</td>
</tr>
<tr>
<td>4.2.2.1 Customer due diligence and record keeping</td>
<td>147</td>
</tr>
<tr>
<td>4.2.2.1.1 CDD for banks</td>
<td>149</td>
</tr>
<tr>
<td>4.2.2.1.2 CDD for correspondent banks</td>
<td>161</td>
</tr>
<tr>
<td>4.2.2.1.3 CDD for mutual funds and pooled investment vehicles</td>
<td>164</td>
</tr>
<tr>
<td>4.2.2.1.4 CDD for wire transfers</td>
<td>165</td>
</tr>
<tr>
<td>4.2.2.1.5 CDD and the risk-based approach</td>
<td>169</td>
</tr>
<tr>
<td>4.2.2.1.5.1 Specific risks criterion for PVs</td>
<td>173</td>
</tr>
<tr>
<td>4.2.2.1.5.2 Risk variables and further measures</td>
<td>173</td>
</tr>
<tr>
<td>4.2.2.1.5.3 High measure CDDs versus simple measure CDDs</td>
<td>176</td>
</tr>
<tr>
<td>4.2.2.2 Reporting</td>
<td>177</td>
</tr>
<tr>
<td>4.2.2.1 Grounds for reporting</td>
<td>177</td>
</tr>
<tr>
<td>4.2.2.2 The obligation to report</td>
<td>181</td>
</tr>
<tr>
<td>4.2.2.3 To whom reporting should be made</td>
<td>183</td>
</tr>
<tr>
<td>4.2.2.3 Regulation and Supervision</td>
<td>185</td>
</tr>
<tr>
<td>4.2.2.4 Deterrent measures</td>
<td>186</td>
</tr>
<tr>
<td>4.2.3 Pillar 2: Enforcement</td>
<td>187</td>
</tr>
<tr>
<td>4.2.3.1 The principle of mutual legal assistance: a bind chord</td>
<td>188</td>
</tr>
</tbody>
</table>
PART II

4.3 THE ACL LEGAL REGIME: A SURVEY OF EXISTING RELEVANT LAWS, POLICIES AND INTIATIVES

4.3.1 General

4.3.2 Present legal framework for cyberlaundering

4.3.2.1 General

4.3.2.2 The relationship between the AML and ACL legal regime

4.3.2.3 Cyberlaundering and the Council of Europe Convention on Cybercrime

4.3.2.4 Present attempts to regulate cyberlaundering through international policies

4.3.2.4.1 The FATF

4.3.2.4.2 The Wolfsberg Group

4.3.2.4.3 The Basel Committee on Banking and Supervision

4.3.2.4.4 The Egmont Group

4.3.2.4.5 The World Bank

4.3.2.4.6 International Police Organization

4.3.3 Present national legal framework for cyberlaundering

4.3.3.1 General

4.3.3.2 Germany
4.3.3.3 United Kingdom 228
4.3.3.4 India 230
4.3.3.5 United States 231
4.3.3.5.1 The Federal Bureau of Investigation 233
4.3.3.5.2 The Financial Crimes Enforcement Network 233
4.3.3.5.3 The Drugs Enforcement Administration 234
4.4 SUMMARY 236

CHAPTER 5:
REGULATING CYBERLAUNDERING

5.1 INTRODUCTION 238
5.2 RATIONALE FOR REGULATION 239
5.3 REGULATORY ISSUES AND CHALLENGES 241
5.3.1 Corporate concerns 241
5.3.2 Fluidity of the cyberlaundering process 243
5.3.3 Enforcement challenges 244
5.3.4 Problems associated with root concepts of cyberlaundering 246
5.4 AN ADAPTIVE APPROACH TO REGULATING CYBERLAUNDERING 247

5.5 PREVENTION PILLAR FOR THE ACL LEGAL REGIME 248
5.5.1 General preventive measures against cyberlaundering 248
5.5.1.1 Threshold considerations: Premise for regulation 248
5.5.1.1.1 Conceptualizing cyberlaundering legally for regulatory purposes 249
5.5.1.1.2 Fighting predicate offences 251
5.5.1.1.3 Awareness towards lax jurisdictions 253
5.5.2 Target approach to cyberlaundering regulation 255
5.5.2.1 Adopting new CDD measures 256
5.5.2.1.1 Modifying the KYC principle 257
5.5.2.1.2 Adopting new wire transfer models 262
5.5.2.2 Protected biometry and cryptography 265
5.5.2.2.1 Employing biometric methods for identification 265
5.5.2.2.2 Ensuring better encryption methods 267
5.5.2.3 Regulating electronic payments systems 270
5.5.2.3.1 Establishing electronic money institutions 271
5.5.2.3.2 Stricter controls for smart cards 274
5.5.2.3.3 Fusing the money-trail with the bit-trail 278
5.5.2.4 Regulating online gaming 280
5.5.2.4.1 Measures against the avenue of virtual worlds 281
5.5.2.4.2 Measures against the avenue of online gambling 285

5.6 COMPLIANCE PILLAR FOR THE ACL LEGAL REGIME 287
5.6.1 Duty to comply 288
5.6.2 Duty to ensure compliance 289
5.7 SUMMARY 291

CHAPTER 6
PROSECUTING CYBERLAUUNDERING

6.1 INTRODUCTION 293
6.2 PATH TO PROSECUTING CYBERLAUUNDERING:
ISSUES AND CHALLENGES 294
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1 Practical and logistic challenges</td>
<td>295</td>
</tr>
<tr>
<td>6.2.2 The right to privacy</td>
<td>296</td>
</tr>
<tr>
<td>6.2.2.1 Personal information and new electronic devices</td>
<td>296</td>
</tr>
<tr>
<td>6.2.2.2 The legal protection of personal data versus investigative needs</td>
<td>298</td>
</tr>
<tr>
<td>6.2.2.3 Balancing the scale between privacy and public interest values</td>
<td>300</td>
</tr>
<tr>
<td>6.2.3 Electronic evidence and the question of admissibility</td>
<td>301</td>
</tr>
<tr>
<td>6.2.3.1 Nature and characteristics of electronic evidence</td>
<td>301</td>
</tr>
<tr>
<td>6.2.3.2 The admissibility of electronic evidence</td>
<td>304</td>
</tr>
<tr>
<td>6.2.3.3 Electronic evidence and cyberlaundering</td>
<td>307</td>
</tr>
<tr>
<td>6.3 INVESTIGATING CYBERLAUNDERING</td>
<td>308</td>
</tr>
<tr>
<td>6.3.1 Applicability of conventional money laundering investigative techniques</td>
<td>310</td>
</tr>
<tr>
<td>6.3.2 Fundamentals of digital investigation</td>
<td>311</td>
</tr>
<tr>
<td>6.3.2.1 Role players in the investigative process</td>
<td>311</td>
</tr>
<tr>
<td>6.3.2.2 Concept and methodologies of computer forensics</td>
<td>312</td>
</tr>
<tr>
<td>6.3.2.3 Scientific techniques and digital investigations</td>
<td>316</td>
</tr>
<tr>
<td>6.3.3 Employing digital investigative techniques for cyberlaundering:</td>
<td>317</td>
</tr>
<tr>
<td>A practical assessment</td>
<td>319</td>
</tr>
<tr>
<td>6.3.3.1 Threshold considerations</td>
<td>320</td>
</tr>
<tr>
<td>6.3.3.1.1 Adopting the scientific approach</td>
<td>320</td>
</tr>
<tr>
<td>6.3.3.1.2 Case management</td>
<td>321</td>
</tr>
<tr>
<td>6.3.3.1.3 Statutes of limitation</td>
<td>321</td>
</tr>
<tr>
<td>6.3.3.2 Detection</td>
<td>322</td>
</tr>
<tr>
<td>6.3.3.3 Survey</td>
<td>326</td>
</tr>
</tbody>
</table>
6.3.3.3.1 Establishing the actus reus element of cyberlaundering 327
6.3.3.3.2 Authorization 330
6.3.3.4 Seizure and confiscation of potential evidence 331
6.3.3.5 Preservation 333
6.3.3.6 Examination 334
6.3.3.7 Analysis 336
6.3.3.7.1 Knowledge of the illegality of the funds 337
6.3.3.7.2 Associative intention with the funds 338
6.3.3.8 Reporting and testimony 340
6.3.4 Mutual legal assistance for cyberlaundering investigations 341

6.4 ESTABLISHING JURISDICTION
FOR CYBERLAUNDERING 342
6.4.1 Applicability of money laundering principles of jurisdiction 346
6.4.2 Applicability of cybercrime principles of jurisdiction 349
6.4.2.1 The territoriality principle 350
6.4.2.1.1 Location of the act 351
6.4.2.1.2 Location of the computer 353
6.4.2.1.3 Location of the victim 356
6.4.2.1.4 Location of the effect 357
6.4.2.2 The nationality principle 358
6.4.2.3 The universality principle 359
6.4.3 Guidelines for establishing cyberlaundering jurisdiction 362
6.4.3.1 Determine the cyberlaundering conduct 363
6.4.3.2 Determine the cyberlaundering avenue 363
6.4.3.3 Determine the applicable jurisdictional principles 364
6.5 THE NEED FOR AN ACL PROSECUTORAL FRAMEWORK: CASE STUDIES

6.5.1 United States of America v E-Gold Ltd, Douglas Jackson, Barry K. Downey, and Reid A. Jackson

6.5.1.1 Facts

6.5.1.2 How cyberlaundering comes into play

6.5.2 The pending case against Megaupload Ltd

6.5.2.1 Facts

6.5.2.2 How cyberlaundering comes into play

6.6 FORMALITIES INVOLVED IN ESTABLISHING THE ACL LEGAL FRAMEWORK

6.7 SUMMARY

CHAPTER 7

CONCLUSION AND RECOMMENDATIONS

7.1 GENERAL

7.2 THE TRIPPLE-PILLAR COMBAT TRATEGY

7.2.1 Increased awareness amongst regulatory authorities

7.2.2 Continuous research

7.2.3 Capacity building

7.3 EPILOGUE

LIST OF REFERENCES
ABSTRACT

Along with its inumerable wonders, the advent of the internet has brought with it very bad vices. The notion of convenience, which comes with the use of the internet, can be attributed to criminals who wish to disguise the proceeds of their ill-derived funds, or what is better known as cyberlaundering. Cyberlaundering is a phenomenon that seems negligible on face value, but, to the contrary, has very dire effects, especially on national economies, which are in no way trifling.

This study describes the problem of cyberlaundering, pointing out the various legal issues pertaining to it. Given that cyberlaundering is a comparatively new crime, which is not yet conceptualized legally, criminal justice authorities find it hard to detect, investigate and prosecute cyberlaundering. An adequate legal regime against cyberlaundering is currently non-existent, as there is presently no concise international or national legal framework in place to contain the problem. Whilst the chief focus of the thesis is to devise a legal framework to combat cyberlaundering, considerable attention is also devoted to the tension that arises between public and private interests, amongst several other legal issues that come to play along the way. This is a debate that necessarily arises when legislatures resort to more radical anti-cyberlaundering laws. The study advocates a middle ground, which leads to the desired end of curbing the exponential growth of cyberlaundering, at the very least.
### KEY WORDS AND ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACC</td>
<td>Anti-Cybercrime</td>
</tr>
<tr>
<td>ACL</td>
<td>Anti-Cyberlaundering</td>
</tr>
<tr>
<td>AML</td>
<td>Anti-Money Laundering</td>
</tr>
<tr>
<td>BCBS</td>
<td>Basel Committee on Banking Supervision</td>
</tr>
<tr>
<td>CDD</td>
<td>Customer Due Dilligence</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>ICT</td>
<td>Information Communications Technology</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer</td>
</tr>
<tr>
<td>STR</td>
<td>Suspicious Transaction Report</td>
</tr>
</tbody>
</table>
CHAPTER 1
INTRODUCTION

1.1 PROLOGUE
Cyberlaundering refers to the way in which the mechanism of the internet is used to launder illegal proceeds of crime in order to make such proceeds appear clean. The advent of the internet has yielded this new breed of crime. On the internet, there are various avenues exploited by criminals to convert ‘dirty’ money into ‘clean’ money.¹ What has been understood as money laundering in the past is not necessarily the case anymore. Money laundering now wears the cloak of cyberlaundering, because criminals today are one step ahead of the law. These criminals are constantly devising new ways in which to evade the prying eyes of law enforcement, hence the shift to cyberlaundering.

1.2 EPISTEMOLOGICAL BASIS OF STUDY
The subject of cyberlaundering has constantly been evaded.² This is mainly because it is a hybrid subject which merges aspects of information

---
¹ Prevalent avenues, amongst a host of others, include online banking, online gambling, e-gaming, online auctioning and digital payments methods. These methods will be further explained in detail in the chapters below.
² The topic has constantly been avoided simply because little is known about it. For instance, in July 2009, the House of Lords’ European Union Select Committee issued a report titled ‘Money Laundering and Financing of Terrorism’ available at <http://www.parliament.uk/business/committees/committee-archives/> [accessed on 11 February 2011], yet nowhere does it deal with the issue of cyberlaundering, in spite of its relatedness to terrorist financing. Also, as evidenced in this study, present international laws against money laundering and cybercrime have not been reviewed in light of the currency of the dilemma. For money laundering, examples of such laws are
technology, computer science and law. Its evasiveness has caused it to be very mystifying. As long as the internet remains an integral part of our lives, criminals will continue to exploit this avenue for laundering proceeds of crime, unless possible means of regulation and control are devised. Very little is known about cyberlaundering because very little research has been done on it. This is the main impetus for undertaking this research.

The broader field of money laundering is one that is also fraught with regulatory challenges, with very strong links to organised crime and terrorism, which are also colossal problems in the world today, and which current legal infrastructures are battling to contain. These issues are seamlessly interrelated, and with cyberlaundering, the link is only fortified further, with the internet being used frequently to ‘wash’ the proceeds of organised crime and to fund terrorist activities. By effectively combating the problem of cyberlaundering, one is ripping out one of the main roots of these problems, thus helping to subdue other related vices such as money laundering, cybercrime, fraud and corruption.

The subject of cyberlaundering has reached a point where it can no longer be swept under the rug and alas, its current state is not anywhere nears its peak.

---


3 Cf discussion in paragraphs 1.3.1.1 and 1.3.1.2 below.
Although it is often said that the law is dynamic, in truth, the same can be said of crime. As proposed in this study, there is a desperate need for the ‘adaptation’ of relevant policies, laws and regulations to deal effectively with the menace of cyberlaundering, failing which the enactment of new laws becomes imperative. This study therefore explores the problematic aspects of cyberlaundering comprehensively. It does so by identifying the reasons why it has evolved into the legal concern it is today; how it manifests itself in practice; whether current laws exist to deal with the problem; and more importantly, what laws can be introduced or adapted to surmount the problem. In other words, this study seeks to establish an anti-cyberlaundering (ACL) legal regime.

1.3 SIGNIFICANCE OF RESEARCH
The proposed ACL legal regime springs from a gap in the law that needs to be filled. It is therefore important to understand the significance of this research, which serves as a rationale that constitutes the basis for the ACL legal framework that will be proposed in this study.

1.3.1 The problem of cyberlaundering: A legal concern
Cyberlaundering originated with the advent and exponential growth of the internet. With more and more people gaining access to it, many lives are
‘lived’ on the internet. It has become a medium through which we talk to each other and socialize with each other. However, the bitter and very unsettling truth here is simply that the advent and rapid expansion of the internet has also given rise to menacing practices, cyberlaundering being one of such, but what a diabolical one at that! The issue is one of legal concern as it foretokens formidable legal questions that need to be answered.

As a fundamental reason explaining the problematic nature of cyberlaundering, law enforcement agencies are yet to fathom fully the phenomenon of internet criminality. Several regular internet operations that seem to be common, perfunctory practices that appear untainted with illegality, such as e-gaming and online gambling are sanctuaries for criminals who desire to ‘wash’ their ill-derived funds. The problem of cyberlaundering cannot be couched in simple terms. To better understand the enormity of the problem, one needs first to assess its effects and the areas where the problem rears its head. To further comprehend the dire effects of cyberlaundering, one need only look to see how it ties up with organized crime, with terrorism and, more broadly, how it impacts on the world economy.

---

packet-switching network. In 1985, the ARPANET became more global in scope and was no longer confined to government use, as was the case in the United Kingdom and the United States. Arguably, it can be said that the internet exploded onto the world stage when, in the mid-1990s, private organisations gained access to it. See Living Internet ‘History of the Internet’ an undated internet article available at <http://www.livinginternet.com> [accessed on 10 February 2011].
1.3.1.1 Cyberlaundering and organised crime

Cyberlaundering bears an inextricable link to organized crime, and the organized crime pattern in West Africa is a case in point. Organised criminal activities in West Africa are evidenced in the operations of the ‘419 syndicates.’ These criminals are popularly known to be scam artists who use the internet to perpetrate their wicked schemes. They send out scam emails and notices to lure people into dealing with them. At the end of the day, their victims are duped and fleeced of their money. The 419 syndicates are synonymous with cyber criminality, having propagated and popularized its different forms. The image of Nigeria, as well as other West African countries, has been severely blemished as a result of the activities of these criminal gangs.

One might be inclined to ask, where do the proceeds of these crimes go, or how are they funnelled back into the pockets of the perpetrators? The answer lies mainly within the concept and compass of cyberlaundering. There is a huge amount of ‘dirty’ money circulating on the internet, and the proceeds of these crimes rarely leave the realm of the internet. This is because the criminals want to ‘wash’ the proceeds in some way, in order to make them look ‘clean,’ hence the concept of cyberlaundering. The crimes of cyberfraud and cybertheft that are often perpetrated by these criminals are all predicate

---

6 The term ‘419 criminal’ originated in Nigeria, and refers to violators of section 41(9) of the Nigerian Criminal Code, which deals mainly with fraud.

The Legal Regime for Anti-Cyberlaundering / Daniel Leslie
offences\(^{7}\) for money laundering activities, and in this case, cyberlaundering. To this end, several cyberlaundering techniques, such as online banking\(^{8}\) or online gaming\(^{9}\) can be used. Cyberlaundering is therefore a viable means to an evil end.

1.3.1.2 Cyberlaundering and terrorism

Cyberlaundering is also inextricably linked to terrorism. It is said that the attacks by Al-Qaeda on the Twin Towers in New York on 11 September 2001 were financed mainly through internet fraud.\(^{10}\) This caused a rude awakening about how the internet can be used to commit heinous crimes. However, a perplexing question that has since defied any answer is how the proceeds of these crimes were converted to ‘clean’ money, which served to foster the aims of Al-Qaeda. In other words, how did these proceeds ‘travel out’ of, or how were they siphoned out of the internet?

The Financial Action Task Force\(^{11}\) (FATF) tried to solve this riddle by conducting a typology survey of new money laundering techniques.\(^{12}\) The

---

\(^{7}\) A predicate offence is an offence which precipitates the crime of money laundering. It is the underlying offence that gives rise to the money laundering offence. Money laundering has an endless list of predicate offences, like theft, fraud, robbery, etc. For a concise list of these predicate offences, see article 2(h) of Palermo Convention. Cf Appendix to the Warsaw Convention.

\(^{8}\) Cf detailed discussion in Chapter 3, paragraph 3.5.1.

\(^{9}\) Cf detailed discussion in Chapter 3, paragraph 3.5.4.


\(^{11}\) The Financial Action Task Force is an inter-governmental body established in 1989 by the Group of Seven (G7) Summit, comprised of Ministers of its Member jurisdictions. It is tasked with protecting the integrity of the international financial system by setting global and uniform standards against money laundering, terrorism and corruption, amongst other threats posed to the international financial system. Recently, in a way similar to that done in 2004, the mandate of the FATF was extended to the year 2020. See Financial Action Task Force (2012B: 2) and Financial Action Task Force (2004A: 1). Cf in relation to the regulation of cyberlaundering, see detailed discussion on the FATF in Chapter 4, paragraph 4.3.2.4.1.
FATF identified the internet as a “new risk area” for money laundering, and stated that the avenue of online casinos opens up endless possibilities for money laundering.\textsuperscript{13} The fact that cyberlaundering is a ‘new risk area’ is the only thing known about it at present. Its mechanisms have not yet been explored thoroughly, neither are there currently clear-cut legal provisions against the problem. Given the clandestine nature of terrorist activities, which is a mould within which cyberlaundering is emboiled, its instrumentality and significance to terrorist operations cannot be over-emphasized.

1.3.1.3 Cyberlaundering and the world economy

The global economy is but one sphere in which the impact of cyberlaundering is most felt.\textsuperscript{14} Currently, on a global scale, the amount of money being laundered annually is unfathomable. The World Bank recently estimated that, globally, about $4 trillion is laundered annually, but the amount is what is called a mere guestimate or “questionate.”\textsuperscript{15} Nevertheless this amount equals the combined value of the economies of most underdeveloped countries. What is more, this amount is set to triple if cyberlaundering is not kept at bay. One’s fear is further heightened by a recent report by the International Monetary Fund (IMF), which indicates that about five to seven per cent of the world’s gross domestic product (GDP) is laundered annually.\textsuperscript{16} As far back as

\begin{footnotesize}
\begin{itemize}
\item[14] See Unger (2007: 158), who identifies other sectors like the real estate sector and the legal profession as equally threatened by the activities of modern day money launderers.
\end{itemize}
\end{footnotesize}
1998, money laundering was said to be the world’s third largest market, after the US domestic bond market and the Euro bond market.\textsuperscript{17} With economics statistics from the United Nations Crime and Justice Database, in 1998, a model for estimating money laundering was devised, which put the amount of money laundered annually at $2.85 trillion.\textsuperscript{18} Over the years, an identifiable feature of money laundering has been its non-static nature. The figures identified above are growing numbers, and with the escalation of money laundering activities, especially on the limitless world of the internet, the sky is the limit for money launderers. In fact, the problem has reached such alarming proportions that the FATF believes that it is hard to publish actual estimates for fears or unreliability, given its growing nature.\textsuperscript{19} The fact that money laundering has an indirect impact on the economy\textsuperscript{20} is a veil covering the true nature and gravity of the money laundering dilemma. The truth is that several stagnant and collapsing economies today are the consequence of money laundering activities\textsuperscript{21} – a fact that is unknown to many. The emergence of the cyberlaundering phenomenon further compounds what is already a colossal problem. Cyberlaundering is therefore a problem which should not be underplayed, because without any form of legal regulation, it has the dire effect of hindering economic growth and development.

1.3.2 The non-existence of a proper ACL legal regime

This significance of this research also lies in the fact that there is, as yet, no proper legal framework against cyberlaundering. This is ascribable to a key feature of cyberlaundering, which is the element of disguise inherent in the concept. If cyberlaundering activities cannot be easily identified or detected, how much more its regulation. These activities change as new avenues for laundering money on the internet are always sniffed out by criminals. Due to the vacillating nature of the fabric with which the internet is built, which constantly renders the internet susceptible to attacks and threats, present attempts to regulate cyberlaundering have been rendered futile. It is almost as if one is shooting at a moving target. The fact of the matter is that the existing anti-money laundering (AML) laws have remained static while the evil that they seek to eradicate mutates constantly. It is primarily because of this state of affairs that this study will attempt to come up with a legal framework to combat cyberlaundering. As we shall see in the course of this study, attempts have been made to come to grips with the problem, and this will be evaluated too. For example, on the international plane, in 2008, the FATF conducted a survey of online casinos as a possible avenue for cyberlaundering. In its report, the FATF recommends certain regulatory measures to which online casinos should be made subject. Similarly, the World Bank also made

---

22 Cf Chapter 4 of this study, which explores and justifies the reality of this position by examining the current legal and international legal framework against cyberlaundering
23 Cf discussion in Chapter 4, paragraph 4.3.1.
25 Cf detailed discussion in Chapter 4, paragraph 4.3.2.4.1.
certain recommendations for the regulation of cyberlaundering. In one of its reports, it points out certain deficiencies in the electronic payment system (e-payments systems).\textsuperscript{26} On the national plane, little or nothing has been done to curb cyberlaundering.\textsuperscript{27}

1.4 LITERATURE SURVEY

There is a dearth of literature on the subject of money laundering and cybercrime.\textsuperscript{28} Most of the literature does not address the issue of...

\textsuperscript{27} Cf detailed discussion in Chapter 4, paragraph 4.3.3.
cyberlaundering. Even though some of the literature has touched on the topic,29 these works merely scratch the surface of the subject, without an in-depth legal investigation into the concept and its legal ramifications. The reality of this fact forms part of the theoretical basis for embarking on this study.

In addition, the available literature on cyberlaundering does not have a legal direction. This might be a reason for the lack of a juridical focus on the subject. Despite the fact that the bulk of the material on cyberlaundering focuses on its techniques, the available literature on the subject is bereft of legal focus. This is precisely why this study seeks to etch out a new path in the law by attempting to erect an ACL legal regime.

---

1.5 FOCUS OF STUDY

Cyberlaundering is problematic because of the absence of an ACL legal regime. There are several questions that crop up, and it is presently these that this study addresses:

1.5.1 Research question

The principal question that this study attempts to answer is this: How can an ACL legal regime be established?

This question is one under which other legal issues are subsumed. There are no straightforward answers, nor are there simple solutions. The questions that are addressed in this study include how cyberlaundering can be legally conceptualized; how existing national and international laws can be adapted to address the problem; how the legal regulation of cyberlaundering is possible through establishing prevention and compliance mechanisms; and as an equally indispensable issue, how cyberlaundering can be regulated by establishing adequate enforcement mechanisms. The latter will include looking at how cyberlaundering can be investigated, and how jurisdiction can be founded for it.

This study proceeds from the standpoint that the legal issues that will be identified are concerns for states that attach great value to procedural fairness and the features of a constitutional state based upon the Rule of Law (Reichstaat). Even though cyberlaunderers are bent on undermining the authority of the state and its institutions, it would be counterproductive for the
state to chisel away at the very foundations upon which it is built in its attempts to bring cyberlaundurers to book. To flout constitutional and procedural safeguards would serve only to undermine the integrity of the law even more, thus rendering the state even more vulnerable to the machinations of money launderers.

The legal issues mentioned above represent the parameters of this study. By disserting on them and on the way they can be brought to bear on the menacing problem of cyberlaundering, we open up practical and realistic ways of responding effectively to the problem.

1.5.2 Aims and objectives of study

In light of the above, broadly speaking, there are four objectives that this research seeks to achieve. They are the following:

1. Given that cyberlaundering currently lacks any form of legal conceptualization or categorization, and given, too, that the logic and rationale underlying the first step to be taken in addressing a problem is to define it, this study attempts to conceptualize cyberlaundering legally.\(^{30}\)

2. The second objective is to analyse and assess whether these are existent laws at national and international level that have any bearing on cyberlaundering. This is done in order to see how laws can be adapted

---

\(^{30}\) This is the primary goal of Chapter 3 of this study. Also, the supporting concepts of money laundering and cybercrime, which are root concepts of cyberlaundering, as discussed in Chapter 2 of this study, contributes to an understanding of the latter. Cf Chapter 3, paragraph 3.2, and Chapter 5, paragraph 5.5.1.1.
and co-ordinated to form a formidable arsenal of legal measures that could be used to counteract cyberlaundering.\(^{31}\)

3. Thirdly, this study seeks principally to set in place legal measures that can ensure the regulation of cyberlaundering. Identifying the problem and laws is one thing; it is entirely quite another to fashion out measures necessary to regulate cyberlaundering. In addition to establishing ACL measures that are adapted from existing hard and soft laws, the third objective of this study is to establish preventive and compliance pillars that will form part of the ACL legal regime.\(^{32}\)

4. The fourth objective is to complement the regulations with an enforcement pillar. Certain legal issues that serve as a barrier to the effective prosecution of cyberlaundering will be addressed. These pertinent prosecutorial issues include how cyberlaundering can be investigated; how jurisdiction can be founded or determined for it, and, more broadly, how certain technical considerations involving the realization of the ACL legal regime can be addressed. By addressing these very pertinent issues, together, the enforcement pillar of the ACL legal regime can be assured.\(^{33}\)

\(^{31}\) This is the primary purpose of Chapter 4 of this study.

\(^{32}\) Chapter 5 of this study serves this purpose.

\(^{33}\) Chapter 6 of this study is devoted to achieving this purpose. For deliberation on these issues, see Straub (2002: 35) and Ping (2004: 29).
1.6 SCOPE OF STUDY

The study focuses solely on the concept of cyberlaundering. However, as is inevitable and necessary, certain other subject areas that are related to cyberlaundering are addressed as well. A focus on these other areas is important for the understanding of cyberlaundering and for devising regulations against it. Given the novelty of cyberlaundering in this regard, one is guided by the parameters of this study, as determined above.\(^34\) As such, in this study, other than frequent references to certain principles of cybercrime and money laundering, which are the two main roots of cyberlaundering, reference is also made to certain principles of information technology, computer forensics and certain general principles of international law.

Though money laundering is one of the main legs of cyberlaundering, this study does not explore the entire academic landscape of the subject, but only considers it to the extent that it is relevant or related to cyberlaundering and its proposed regulation.\(^35\) To this end, money laundering, as a subject area, is considered mainly as a background to cyberlaundering in light of the fact that an understanding of the AML legal framework is indispensable for understanding and establishing an ACL legal regime.

In addition, although money laundering is inextricably linked to terrorist financing, which is a separate subject area on its own, this study does not

---

\(^{34}\) Cf discussion in paragraph 1.3 above.

\(^{35}\) The bulk of the discussion on the subject of money laundering is in Chapters 2 of this study, which is a background chapter, and Chapter 4, which addresses present international and national laws against cyberlaundering.
consider the latter, except for its causal relatedness to the advent of cyberlaundering as discussed earlier.\textsuperscript{36}

Similarly, this study recognizes cybercrime as the second main leg of cyberlaundering, but just as with the subject of money laundering, the subject of cybercrime is given attention only to the extent that it is related to the discussion on cyberlaundering and its legal regulation, without substantial regard to other various forms of cybercrime that exist. Hence, cyberlaundering as it relates only to money laundering and cybercrime constitutes the scope of this study.

1.7 METHODOLOGY

This is a desk-based study. Relevant sources have been garnered from various institutional libraries and resource centres, such as resources at the Max Planck Institute for Foreign and International Criminal Law, Freiburg, Germany; the Law Library of Humboldt University, Berlin, Germany; the University of Applied Sciences, Coburg, Germany; the Law Library of Leiden University, Leiden, the Netherlands; the Peace Palace Library in the Hague, Netherlands; the Law Library of the University of the Western Cape, Bellville, South Africa, and the Law Library of the University of Pretoria, Pretoria, South Africa.

The study is based mainly on an analysis of primary materials such as relevant treaties, conventions and agreements on cybercrime and money

\textsuperscript{36} Cf paragraph 1.2.1.2 above.
laundering. Several official reports issued by reputable anti-money laundering institutions and agencies are also considered. The study furthermore references certain national laws insofar as they have any bearing on cyberlaundering. To a certain degree, a country’s level of adherence to current AML laws is a yardstick that determines why that country’s national law is studied in the first place.\textsuperscript{37} Other primary sources used in this study are decided court cases and indictments.

The secondary sources to which this study will refer include books, journal articles, internet articles, newspaper articles and commentaries. But given the paucity of secondary sources on the subject of cyberlaundering, this study also relies largely on cyberlaundering operations in practice. As regards the latter, the study assesses the activities of certain online companies and websites insofar as they are linked to the main focus area.\textsuperscript{38}

\section*{1.8 STUDY OUTLINE}

Broadly, this study is divided into seven chapters. A summary of each chapter is given briefly below.

Chapter 1, the \textit{Introduction}, sets out the essence of what this study contains.

The chapter introduces, albeit generally, the concept of cyberlaundering; the significance of the study; the focus of the study, which includes the question

\textsuperscript{37} In the past, the FATF black-listed countries having weak, or non-existent AML laws, branding them as Non-Compliant Countries and Territories (NCCTs). For the list of countries previously on the FATF’s black list, see Financial Action Task Force (2002A: 11). Currently, the FATF no longer uses the black-list system to ensure adherence. Cf detailed discussions in Chapter 4, paragraph 4.3.3, and Chapter 5, paragraph 5.5.1.1.3 below.

\textsuperscript{38} This exercise is, largely, a constituent part of Chapters 3, 5 and 6 below.
of research and aims and objectives of the study, as well as the methodology adopted to achieve the purposes of the study.

Chapter 2, *Money Laundering and Cybercrime: A Background Study*, provides the needed background to the study. It uncovers the roots of cyberlaundering. Here, the concepts of money laundering and cybercrime are discussed generally with a view to forming a better understanding of the concept and practice of cyberlaundering.

Chapter 3, *Cyberlaundering: Concept and Practice*, investigates cyberlaundering as a legal concept and how it manifests itself in practice. It attempts to demystify the concept of cyberlaundering and attempts to conceptualize it legally, which is one of the primary aims of this study.

Chapter 4, *The Present Legal Framework against Cyberlaundering*, explores and compares existing laws in place against cyberlaundering. Part I sets out broadly the current AML legal regime, with the primary focus on the international level. Part II examines the current ACL legal regime and the attempts presently made to establish one. The latter serves the purpose of identifying the strengths and weaknesses of certain AML laws and anti-cybercrime (ACC) laws at a national and international level, with a view to finding and establishing an appropriate regulatory framework for the problem of cyberlaundering, which grows out of both subject areas.

Chapter 5, *Regulating Cyberlaundering*, attempts to construct a legal regulatory framework for cyberlaundering. Borrowing from the founding pillars upholding the current AML legal regime, an adaptive approach is
posed in order to establish and fortify the prevention, compliance and enforcement pillars, which are proposed for the ACL legal regime. However, this chapter considers only the prevention and compliance pillars. The enforcement pillar, which has unique issues, is discussed in the following chapter.

Chapter 6, *Prosecuting Cyberlaundering*, is an extension of the previous chapter. It proposes an enforcement pillar for the ACL legal regime. It explores certain prosecutorial issues relating to cyberlaundering, such as the investigation of cyberlaundering and how jurisdiction can be founded for it. This chapter also addresses the technicalities involved in the overall establishment of the ACL legal regime.

Chapter 7, the *Conclusion*, concludes the study with a set of recommendations.
CHAPTER 2
MONEY LAUNDERING AND CYBERCRIME: A BACKGROUND STUDY

2.1 INTRODUCTION
This chapter is a background study of money laundering and cybercrime. It focuses on certain historical aspects that are crucial to the primary task of the study, which is to study how an effective legal framework can be established for combating cyberlaundering. The chapter serves two main purposes: First, it seeks to put cyberlaundering into perspective by exploring the history and development of money laundering and cybercrime in tandem. Secondly, it traces the development of these two main roots of cyberlaundering, thereby attempting to uncover certain deep-seated issues currently associated with this problematic concept.

2.2 MONEY LAUNDERING: AN OVERVIEW
2.2.1 Understanding the meaning of money laundering
Before one goes ahead to attempt to define money laundering, it is important to note from the outset that the concept of money laundering is constantly evolving. This has affected its definition over the years, even though the principle that underlies the concept remains unchanged. Perhaps one of the earliest and most important definitions of money laundering is outlined in Article 3(b) of the United Nations Convention Against Illicit Traffic in
Narcotic Drugs and Psychotropic Substances\(^{39}\) (the Vienna Convention), which reads as follows:

The conversion or transfer of property, knowing that such property is derived from any [drug trafficking] offense or offenses or from an act of participation in such offense or offenses, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offense or offenses to evade the legal consequences of his actions; The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offense or offenses or from an act of participation in such an offense or offenses.

Article 3(c)(i) of the Convention further adds:

The acquisition, possession or use of property, knowing at the time of receipt that such property was derived from an offense or offenses [\(\ldots\)] or from an act of participation in such offense or offenses.

Interestingly, the term ‘money laundering’ was never used in the Convention, although its provisions create the widest possible ambit within which the conduct of laundering money would fall. Another key feature of this somewhat encompassing definition is that the conduct described is limited to the predicate offence of drug trafficking, which is understandable, given the nature of the Convention, its aims and objectives.\(^{40}\) However, the direct legal

\(^{39}\) The Convention was adopted by the General Assembly of the United Nations on 7 December 1987, and it came into force on 11 November 1988.

\(^{40}\) For more elaborate discussions on the Vienna Convention as it pertains to money laundering, see the following: Stessens (2000: 25); Savona (2000: 40); Levi (2002: 38) and Gill and Taylor (2004: 587).
implication of this definition is that a criminal would go scot-free if the underlying predicate offence for which he is charged is not a drug-related offence, such as theft, robbery, kidnapping, tax evasion, etc. Subsequent international legal instruments such as the *United Nations Convention against Transnational Organized Crime*\(^{41}\) (the Palermo Convention) attempted a correction of this anomaly by broadening the scope of the predicate offences for money laundering to include serious offences.\(^{42}\) The Financial Action Task Force (FATF)\(^{43}\) finally put its stamp of approval on the definition of money laundering described in the Vienna Convention by adopting certain technicalities of the definition. It includes a very salient recommendation in line with the provisions of the Palermo Convention, which requires that predicate offences for money laundering be widened as far as possible to include all serious offences.\(^{44}\)

According to the FATF’s definition, money laundering is the “the processing of criminal proceeds to *disguise* their illegal origin in order to legitimize the ill-gotten gains of crime.”\(^{45}\) But this is no more than a fine-tuned and succinct version of the definition set out in the Vienna Convention. In what looks to be a following of the trend set by the Vienna Convention, academics have

---

\(^{41}\) The Convention was adopted by the General Assembly of the United Nations on 15 November 2000, and came into force on 29 September 2003.

\(^{42}\) See Article 2 of the Palermo Convention. Cf discussion in Gill and Taylor (2004: 590).

\(^{43}\) See footnote 11 above.


built on this traditional definition of money laundering. For example, money 
laundering has also been defined as “the process by which criminals try to 
hide the origins and ownerships of proceeds of their criminal activities.”\(^{46}\)

The definitions given above can be grouped into traditional definitions of 
money laundering. As can be garnered from these definitions, the overall aim 
of money laundering is to enable criminals to retain control over the proceeds 
of their crime(s). The most common words used to describe how criminals 
can ‘retain control of their illegal funds, are ‘washing,’ ‘cleaning,’ ‘disguising,’ ‘hiding’ and ‘converting’ ‘dirty’ money. The upshot of most of 
the metaphoric associations to the act of money laundering, (i.e. the 
traditional concept) is that such definitions often have the concept of actual 
money as a main subject. This is an anomaly, and is not suited to modern 
times and realities. Currently, money laundering does not simply entail 
washing dirty money, because in many instances actual money is not 
involved. The current trend shows that criminals are trying to distant 
themselves from the ‘loot’ as far away as possible by creating a complex web 
of transactions in order to evade detection and to detach the illegal proceeds 
from their origin.

In light of this modern trend, Hopton gives a descriptive definition of money 
laundering as follows: “Money laundering occurs every time any transaction 
takes place or a relationship is formed which involves any form of property or

\(^{46}\) See Hopton (2009: 1) where the traditional concept of money laundering is expounded further. Cf Savona (2000: 33) and Stessens (2000: 22).
benefit, whether it is tangible or intangible, which is derived from criminal activity.”

This definition is more plausible for the following reasons:

1. The notion of ‘benefits’ is not only confined to money (the so-called object of the crime) but other things of value derived from criminal activities, and as such, it casts a much wider net;

2. Following on the above, the definition is particularly relevant to the concept of cyberlaundering, given the very complex trails criminals create on the internet in laundering illegal proceeds. In this case, the concept of ‘proceeds’ extends to things of value, for example, stolen software, which is often of great value, and which a thief could conceal or launder without actually reducing it to monetary value.

2.2.2 The history and evolution of the anti-money laundering legal regime

The syntactic origin of the phrase ‘money laundering’ does not lie in the mechanism of a washing machine, as could be easily presumed, even though one would understand the underlying euphemism. The term ‘money laundering’ was coined as a result of the Watergate scandal involving President Richard Nixon in the United States in 1973 and 1974. An enquiry was launched to unveil the shroud over the receipt of certain anonymous campaign contributions made to Nixon’s Committee to Re-elect the President

‘CRP’).\textsuperscript{48} The press used the term ‘laundering’, albeit colloquially, to refer to the highly publicized activities and conduct of the CRP.\textsuperscript{49} The first legal usage of the term ‘money laundering’ is traceable to the United States Supreme Court decision of 1982 - \textit{United States of America v $4,255,625, 39\textsuperscript{50}} - a case which involved the civil forfeiture of large sums of money.\textsuperscript{51}

The development of the global anti-money laundering (AML) legal regime, however, dates as far back as the 1980s. At the time, the Nixon scandal had become an anecdote for this new breed of economic crime. The pivotal points in the history of money laundering will be discussed under the following sub-headings: the regulatory and preventive phase; the criminalisation and internalisation phase; the supranisation phase and the terrorism-influenced phase of money laundering law.

\textbf{2.2.2.1 The regulation and prevention phase}

The development of the money laundering legal regime began on a domestic scale. This first stage in its evolution started with the enactment of the United States Bank Secrecy Act 1970 (BSA).\textsuperscript{52} Given its neatly stipulated reporting and record keeping requirements, it is clear that the BSA was put in place to regulate the crime of money laundering rather than to control or repress it.

The BSA’s record keeping requirements provide for the ‘Know-Your-
Customer’ (KYC) principle, which is now a corner stone of the current AML legal regime. In terms of the KYC principle, financial institutions are required to keep a record of the identity of every customer who conducts a transaction with the bank, and record such transactions in line with the basic principles set out in the Act.53 A violation of the record keeping requirements would constitute a felony under the BSA, and is punishable by imprisonment of a period not exceeding five years or a fine not exceeding $10,000, or both.54 The BSA also provides for very stringent reporting requirements. It places an obligation on financial institutions to report domestic transactions valued at more than $10,000.55 Similarly, persons transporting money or monetary instruments into or out of the United States in excess of $5000 are required to report such activity to the relevant body.56 Another significant provision of the BSA is the obligation placed upon United States citizens conducting business within the United States to file reports of their transactions or relationships with foreign financial institutions.57 However, the stringent provisions of the BSA were a thorn in the flesh for many financial institutions in the United States, and consequently, they caused much controversy. In the case of California Bankers Association v Schultz,58 certain banks in the state of California were averse to the cumbersome provision of the BSA, and contested their constitutionality. The

53 See section 101, Title I of the Act.
54 Section 101, Title I of the Bank Secrecy Act.
55 See sections 221, Title II of the Act. Also see Shams (2004: 19).
56 See sections 231, Title II of the Act. Also see Shams (2004: 19).
57 See section 231, Title II of the Act, and Shams at 19.
United States Supreme Court found their allegations to be baseless, and confirmed the constitutionality of the BSA. The court noted that the right which the BSA seeks to protect far exceeds the inconvenience it might cause to financial institutions.\textsuperscript{59}

After the enactment of the BSA, similar regulatory and preventive laws were passed in Switzerland, known for its strong bank secrecy laws. With the growing nature of the Swiss financial sector, it became important for Switzerland to adopt self-regulatory laws in order to protect its image and reputation, especially with its international clients. As a consequence, in 1977, financial institutions in Switzerland signed an \textit{Agreement on the Observance of Care by Banks in Accepting Funds and on the Practice of Banking Secrecy}.\textsuperscript{60}

Aside from the attempts made domestically in the United States and Switzerland to regulate money laundering at the time, signs of regulation at the international level had begun to surface gradually. In 1973, the \textit{US-Switzerland Mutual Legal Assistance Treaty}\textsuperscript{61} (MLAT) was signed. The MLAT came as a result of the growing concerns of the United States government that Swiss banks had started to house illegal funds of criminals.

Thus, the MLAT also served as a necessary safeguard for the United States.

\textsuperscript{59} See pages 745 to 803 of the judgment. The dissenting judgment of Judge Douglas at 851-857 of the judgment is also noteworthy. The Act has also been criticized by academics. For example, see Hughes (1991: 283) and Richards (1999: 44).

\textsuperscript{60} A revised version of the agreement was made in 1998. This can be found in the Agreement on the Swiss Bank Code of Conduct with Regard to the Exercise of Due Diligence (28 January 1998), available at <http://www.swissbanking.org/en/home/> [accessed on 11 January 2011]. For an elaborate discussion of this, see Shams (2004: 24).

\textsuperscript{61} 27 UST 1979, TIAS 8302. The treaty was signed on 23 May 1973 and came into force on 23 January 1977.
The main purpose of the MLAT is to foster international cooperation between Switzerland and the United States in criminal investigations and proceedings.

2.2.2.2 The criminalization and internationalization phase

The 1980s witnessed a significant development in the field of anti-money laundering law. The concept of money laundering as a crime began to take shape both within domestic borders and in the international sphere. The first landmark in this embryonic stage of money laundering law, as recorded by authorities, is the first legal usage of the term money laundering by the United States Supreme Court in _US v $425562539_. In this case, the court repeatedly used the word ‘laundering’ without defining it expressly or elaborating on it further.

In the mid-1980s, there were parallel developments in the field of money laundering law in the United States and the United Kingdom. Both countries enacted far-reaching laws that criminalised the laundering of criminal proceeds with the widest possible ambits. In the United States, for example, the Money Laundering Control Act – symbolic for criminalising money laundering at the Federal level – was enacted. On the other hand, the United Kingdom enacted laws such as the Drug Trafficking Offences Act and the

---

65 In the United States, the Money Laundering Control Act 18 of 1986 was enacted.
67 Chapter 32 of 1986.
Prevention of Terrorism (Temporary Provisions) Act.\textsuperscript{68} While the latter was the first law in the United Kingdom to criminalise the laundering of proceeds of drug trafficking, the former was one of the earliest indicators of a link between terrorist activities and money laundering.

On the international plane, the term ‘money laundering’ was first used by the Select Committee of Experts on Violence in Present Day Society in Recommendation R(80)10 - ‘Measures Against the Transfer and Safekeeping of Funds of Criminal Origin.’\textsuperscript{69} The upshot of this document was its non-binding nature, although it encouraged member states to criminalise the transfer of funds of criminal origin.

A more pertinent international anti-money laundering instrument was the Vienna Convention of 1988. Aside from providing a very extensive definition of money laundering,\textsuperscript{70} the Convention was the first international instrument that burdened states parties with the obligation to criminalise the laundering of the proceeds of drug trafficking. The Vienna Convention made the fight against money laundering a matter of international concern. It was given further momentum by the adoption of subsequent international legal instruments such as the Palermo Convention\textsuperscript{71} and the \textit{Statement of Principles on the Prevention of Criminal Use of the Banking System for the

\textsuperscript{68} Chapter 4 of 1989. However, this Act was later repealed and replaced with the Prevention of Terrorism Act 807of 1997.

\textsuperscript{69} Council of Europe: Measures Against the Transfer and Safekeeping of Funds of Criminal Origin: Recommendation No R (80) and Explanatory Memorandum, adopted by the Committee of Ministers of the Council of Europe on 27 June 1980. See Gilmore (1995: 171), where the recommendation is reproduced.

\textsuperscript{70} See the discussion in 2.2.1 above.

\textsuperscript{71} See the discussion in 2.2.1 above.
The Legal Regime for Anti-Cyberlaundering / Daniel Leslie

_Purposes of Money Laundering_\(^{72}\) issued by the Basel Committee on Banking Supervision.\(^{73}\) The latter instrument is significant for the fact that it entrenches a very salient principle in the anti-money laundering legal regime, namely that financial institutions should not be used for purposes of hiding illegal funds.

### 2.2.2.3 The supranationalisation phase

Towards the late 1980s, the nature and character of the crime of money laundering as a truly transnational crime had become entrenched. Most countries in North America and Western Europe began to respond actively to the growing phenomenon. With the Vienna Convention and the recommendations of the Basel Committee in place, the international cooperation of the international community in forging a strong anti-money laundering (AML) regime had been triggered. However, the AML regime did not gain full momentum until the FATF was established in 1989.\(^{74}\) The FATF has succeeded in supranationalising money laundering law. Its ‘carrot and stick’\(^{75}\) methods of inducement and coercion have opened up a new level of

---


\(^{73}\) The Basel Committee was established in 1974, and it consists of central bank governors of countries consisting of the United States, the United Kingdom, Switzerland, Sweden, Spain, the Netherlands, Luxemburg, Japan, Italy, Germany, France, Canada and Belgium. See The Basel Committee ‘About Basel Committee’ available at <http://www.bis.org/about> [accessed on 20 February 2011].

\(^{74}\) The FATF was established in 1989 by the Group of Seven (G7) consisting of France, Germany, the United Kingdom, the United States, Canada, Italy and Japan. See the Financial Action Task Force (an undated internet webpage) ‘About the FATF’ available at <http://www.fatf-gafi.org/about/> [accessed on 21 February 2011]. See footnote 11 above.

global awareness of the problem, and have ensured compliance with certain basic standards in respect of AML law. Thanks to the efforts of the FATF, the issue of money laundering has been put at the top of the priority list of major international financial institutions such as the World Bank, the International Monetary Fund (IMF) and the European Bank for Reconstruction and Development. Also, the AML regime has been entrenched in the legal framework of most national jurisdictions.

2.2.2.4 The terrorist financing phase

This phase can be described as the darkest in the evolution of the AML regime. After the Al Qaeda attacks on the Twin Towers in New York City on 11 September 2011, the crime of money laundering appeared in a new light. There was a need to look into tackling the crime from the angle of terrorist financing, as it became a novel field needing attention. The AML regime became the only likely remedy and the most appropriate apparatus with which to control terrorist financing. The September 11 attacks have spawned the enactment of various domestic anti-terrorism and AML laws in different countries, the most notable of which is the United States Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept

---

76 Primarily, the FATF monitors to see whether countries abide by its measures, recommendations and standards as set out in the FATF’s 40 Recommendations and Nine Special Recommendations (available at <http://www.fatf-gafi.org/publications/fatf_40_Recommendations> and accessed on 11 February 2011). It was the practice of the FATF to blacklist countries that are non-compliant with its recommendations (the so-called ‘Non-Compliant Countries and Territories’ - NCCTs). The FATF no longer follows this system of assessment, and there are currently no countries blacklisted by the FATF.

and Obstruct Terrorism Act\textsuperscript{78} (US PATRIOT ACT). The inextricable link between terrorist financing and money laundering was further evidenced by subsequent terrorist attacks such as the attacks in London on 7 July 2005.

Not many agree that terrorist financing should be necessarily linked to money laundering. Some authors are of the view that terrorist financing should not be seen as an extension of the subject matter of money laundering.\textsuperscript{79} These authors argue that terrorism should be seen as principle-based, and it should be considered as a due process limitation to AML law.\textsuperscript{80} However, regardless of how it is couched, what is clear is that there are no clear-cut parameters of the dangers posed by money laundering, and the link to terrorism makes this glaring.

2.2.3 The process of money laundering

The ‘cleaning’ or ‘conversion’ of ‘dirty money’ to ‘clean money’ involves a resort to transactions, real or imagined, which would be designed to confuse the onlooker and confound the inquirer.\textsuperscript{81} On face value, it becomes clear that misrepresentation is a fundamental denominator underlying the process of money laundering. Such ‘misrepresentation’ often unfolds, as commonly described, in three main stages – the placement, layering and integration stages.

\textsuperscript{78} Act 115, Statute 272 of 2001.
Before discussing the three stages of money laundering, it should be noted upfront that these stages are often blurred, especially in modern times, with the advent of cyberlaundering. Broadly speaking, money laundering can occur without necessarily following the three processes. Tax evasion is a good example. If one places the proceeds of a legitimate activity directly into a bank account in another country, there is no problem because the money is legitimate. But where the account holder fails to declare his income on a tax return in a country where this was earned, the funds are laundered through the bank, although the bank would be unaware of this. Therefore, the following discussion should be considered with circumspection, as the placement, layering and integration stages are not a closed list of the money laundering process.

2.2.3.1 Placement

The term placement refers to the initial process of money laundering where the proceeds derived from crime are deposited in a financial institution. The amount of money placed in a financial institution would depend on money laundering techniques adopted by the criminal. These proceeds are usually large amounts or denominations which the criminal disperses across several financial institutions. The idea here is to evade the reporting requirements outlined in such laws as the Bank Secrecy Act.\(^\text{82}\)

\(^\text{82}\) See the discussion in paragraph 2.2.2.1 above.
2.2.3.2 Layering

Layering is the second key stage in the money laundering process. It refers to an attempt to forge the ultimate disguise of the illegal funds. The criminal uses various tactics to evade traceability. The layering stage involves several sub-processes. Firstly, the criminal would need to ‘wash’ these illegal proceeds in order to give them a legitimate appearance. This can be done by either mixing the dirty money with the clean money. As an example, illegal proceeds can be integrated with the legal proceeds of legitimate businesses such as a pizzeria or by under-invoicing the imports of an international business trade in the form of a commodity trading company, or by defacing the medium through which the money is paid. A clear example of the latter case is usually where casino chips are purchased, using illegal proceeds (in the case of a traditional casino game) which are then converted back into cash. Another method of washing is the concealment of the beneficial ownership of the tainted funds by financial institutions, such as creating fake mortgages to purchase securities in bearer form, and using a lawyer’s trust account.

Within the contextual framework of cyberlaundering, the complexities which criminals try to create reach a distinctive peak. The internet has become a very effective means through which illegal proceeds can be washed, and more often than not, smart cards are used to foster such purposes, given that these

---

cards can be simply loaded with money and used to conduct all manner of transactions online.

Over the years, Offshore Financial Centres\(^{86}\) (OFCs) have become crucial to the layering process of money laundering. It is becoming a steady norm that criminals with illegal proceeds prefer to spread these proceeds across various OFCs. Two main explanations can be given for this: Firstly, the criminal tries to evade the prying eyes of local law enforcement, and secondly, OFCs often thrive on their large base of foreign clienteles. For many years, countries in the Caribbean with fervent OFCs have been attractive to money launderers on the other side of the Atlantic Ocean. Some of the countries like the Cayman Islands, Nauru and Barbados were blacklisted by the FATF as Non-Compliant Countries and Territories (NCCTs). However, the FATF has done away with the method of blacklisting countries to ensure compliance with its basic recommendations. Though abrogated, this method of compliance could be considered successful in light of the fact that most of the blacklisted countries made genuine attempts to domesticate the global AML regime in their jurisdictions by adopting and implementing local anti-money laundering laws.\(^{87}\)

---

\(^{86}\) The International Monetary Fund (‘IMF’) has defined OFCs as financial centres where the bulk of financial sector activity is offshore on both sides of the balance sheet, that is, the counter-parties of the majority of financial institutions liabilities and assets are non-residents, where the transactions are initiated elsewhere, and where the majority of institutions involved are controlled by non-residents. See International Monetary Fund Monetary and Exchange Affairs Department (2000) ‘Offshore Financial Centres: IMF Background Paper’ available at <http://www.fsfoum.org> [accessed on 22 April 2011].

\(^{87}\) At its Eighth Annual Review of Non-Cooperative Countries and Territories 2006-2007 dated 12 October 2007, the FATF listed no countries as non-cooperative or non-compliant. Financial Action Task Force (2007: 4). However, on 25 February 2009, the FATF did issue a statement that Pakistan,
2.2.3.3 Integration

The integration stage of money laundering comes as a result of the need to reintegrate the illegal proceeds back into the legal economy or the commercial world. Although it is arguable that a criminal could continue to layer his ill-derived funds without the need to reintegrate them, reintegration makes economic sense because “the economic realities associated with the opportunity cost of money means that a portion of the criminally derived money will need to be invested in other endeavours, regardless of whether they are legal or illegal.”

The buy-back technique is probably the most popular method through which criminal proceeds can be reintegrated into the legal economy. An example of the buy-back technique is as follows: X has illegal proceeds derived from drug trafficking, and he uses such proceeds to buy a recording company. He signs himself as a record producer to this company, and contracts the terms in such a way that the company will pay him royalties every month, even though he would not be producing any record. In such a way, the illegal proceeds are ‘cleaned’ and reintegrated into the commercial cycle.

There are various other techniques at the disposal of criminals who seek to reintegrate criminal proceeds back into the commercial world.


2.2.4. Money laundering techniques

An attribute that is common to most money launderers is the art of conniving. A money launderer who has successfully acquired funds that are derived from criminal activities can clean such funds, using a wide range of tricks and techniques at his/her disposal. These techniques are in no way exhaustive – and this fact forms the underlying rationale that explains the complexity inherent in the concept of money laundering. It is important to understand that the numerous techniques which a criminal adopts to hide his/her illegal funds, because this reflects on the very essence of the crime of money laundering as a process crime. An understanding of these techniques is also important for the purpose of fostering the AML campaign, because one fights blindly should one try to fight the crime without understanding it. Also, it is important to study briefly some of these techniques because it helps to paint a better picture of how the techniques involved in money laundering have transitioned to cyberlaundering. Of the almost infinite chain of traditional money laundering techniques, a select few are discussed below.

2.2.4.1 Cash

As a fundamental basis, the profits derived from a crime often return to the criminal in the form of cash, which then needs to be reintroduced into the mainstream commercial sector in order to feign legitimacy. Cash can therefore be manoeuvred in different ways in order to execute such a purpose.
2.2.4.1.1 Cash smuggling

Cash smuggling is probably the oldest but most practical method of laundering dirty money. In the early days of money laundering, it was common practice for ‘dirty cash’ to be concealed in very surreptitious places in order to evade law enforcement and to remove the illegal funds as far away as possible from the scene of the crime. It is often the case that these illegal funds are transported across borders, and there are truly endless possibilities involved here,- ranging from the concealment in cargo ships, car tyres, tin trunks, doors, airplanes and even in the sole of the criminal’s shoe. Cash smuggling does not always have to be clandestine. Money launderers could simply use courier services such as the United Parcel Service (UPS) or Federal Express (FedEx) in order to launder cash, or could purchase legitimate businesses, such as a shipping business, in order to store cash inside the cargo.\footnote{Reuter and Truman (2004: 28). See also Rider (1999: 45), Levi (2002: 188) and Leong (2007: 149).}

Cash smuggling is a good example of the placement stage of money laundering, and it is probably the most obvious method available to money launderers in order to evade the numerous reporting and record keeping requirements.

2.2.4.1.2 Cash structuring / Smurfing

Cash structuring entails breaking down a large quantity of cash into amounts that fall within the stipulated reporting threshold of the relevant financial
system. This is also known popularly as smurfing. The money launderer often uses the services of persons acting as agents who are in cahoots with him (also called smurfs). The idea is that the smurfs would make deposits systematically in banks of amounts below the prescribed threshold. In the United States, for instance, the reporting threshold set in the BSA is $10,000. Cash smurfing is one of the several flaws occasioned by the BSA, which the subsequent Money Laundering Control Act sought to correct. Cash structuring can be done through different avenues. Firstly, a regular deposit of the funds can be made into accounts in amounts that fall below the reporting threshold. Secondly, the illegal funds can be used to purchase negotiable instruments such as bank cheques and bank drafts, or, in the case of cyberlaundering, to load onto credit cards or smart cards, or onto gift cards in amounts falling below the reporting threshold. Thirdly, multiple deposits of the illegal funds can be made into several branches of a financial institution, often in quick succession in order to avoid detection. Alternatively, the money launderer opens accounts at different financial institutions, or could use third parties, for example, smurfs to make deposits into a single account or multiple accounts. In a nutshell, the possibilities are legion.

90 The term ‘smurfing’ is derived from the little blue cartoon characters in the popular 1980s television show called The Smurfs.
91 See section 101 of the Act. Most jurisdictions have a similar threshold. In Canada, for example, the threshold is 10,000 Canadian Dollars, as outlined in the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (S.C. 2000, c. 17). Also in Europe, the European Union has set a threshold of €10,000, in terms of the Article 3 of Regulation (EC) No 1889/2005, adopted by the European Parliament on 26 October 2005 and which came into force on 15 December 2005.
Cash structuring is also a good example of the placement stage of money laundering, and, as is obvious, the main goal is to evade the various reporting and record-keeping requirements.

2.2.4.2 Wagering

Betting or wagering services have also proven to be a safe hub for money launderers. Casinos, horse racing and lotteries are very good examples. These are discussed further below.

2.2.4.2.1 Casinos

Casinos are known to be very lucrative for hiding illicit funds.\textsuperscript{94} Illegal funds are often used to buy casino chips, which a criminal would then trade in for a cheque in the name of a third party (usually in cahoots with the criminal).\textsuperscript{95} It appears irrelevant for a criminal to play with his chips, given the risk of losing associated with games of chance and the lack a standard rule in casinos that all chips must be used or played.

The fact that casinos have multijurisdictional establishments makes it even easier for criminals to transfer funds across borders. This convenience has been further facilitated by the advent of online casinos, which makes it all the

\textsuperscript{94} In its March 2009 report on the Vulnerability of Casinos and the Gaming Sector, the FATF identified casinos as a wide open avenue for money laundering. See Financial Action Task Force (2009B: 12).

more difficult for law enforcers to establish the physical location of the launderer.

2.2.4.2.2 Horse racing and lotteries

In the case of horse racing, a money laundering operation is as simple as a criminal buying a winning ticket at a low premium, which he can then claim back. The catch here is that the launderer will be able to evade payment of taxes on his winnings and he could also collect a cheque from the track.\(^{96}\)

With lotteries, it works even more easily because a criminal could simply use his illegal funds to purchase winning tickets from the winners as they arrive at the lottery office.\(^{97}\)

2.2.4.3 Insurance policies

Illegal funds can be laundered through insurance policies, using several methods. A single insurance premium is a good example. Here the criminal uses his illegally obtained funds to pay the full premium once-off rather than in instalments, thus enabling him to redeem his full policy at a discount.\(^{98}\) By paying all required fees and penalties and getting ‘clean’ funds back from the insurance company, the criminal invariably launders his funds.

\(^{98}\) Lawrence (2008: 82) and Reuter and Truman (2004: 30).
2.2.4.4 Securities

In its 2002 report, the FATF points out that there is now a steady shift of laundering operations from the traditional banking sector to the non-bank financial sector, such as the securities market.\footnote{99} The securities market is an attractive arena for laundering activities, particularly at the layering and integration stages. A launderer could purchase securities with illicit funds transferred from one or more accounts, and could use the proceeds of the securities as legitimate money when resold.\footnote{100} In addition, the security market often has an international dimension, making it ideal for embezzlers, security fraudsters and insider traders, amongst others, who are present within the financial system.

2.2.4.5 Hawala

Hawala\footnote{101} is an informal money transfer system which is based on mutual trust between the parties to the agreement. Hawala works in such a way that money is made available internationally without actually moving it or leaving a record of the transaction. The system often involves at least three persons – the hawaladar who offers the remittance service; the client who wishes to transfer money abroad; and the hawala agent in the destination country who makes delivery of the service.

\footnote{99} Financial Action Task Force (2002B: 44). In this report the FATF identifies the vulnerabilities of the securities market for purposes of money laundering by pointing out the glaring loopholes. It also details some corrective measures which are most feasible for remedying the problem.


\footnote{101} The term ‘hawala’ is an Arabic word which means an underground banking system of an international nature.
Although the hawala system appears to be peculiar to most Middle Eastern and South Asian societies, it is not a strange concept in other societies. For instance, in China it is known as ‘fe chi’en,’ and in Cameroon it is known commonly as a ‘cooperative.’ In a more formal set up, the hawala system can be likened to formal money transfer systems such as the popular Western Union money transfer.102

2.2.4.6 ‘Shell’ companies

A shell company is usually set up to facilitate the layering of illegal funds. More often than not, it is based offshore, complete with banks accounts to aid the layering of the funds.103 A shell company serves as a vehicle for business transactions without itself having any significant assets or operations. Although shell corporations are not in themselves illegal, they may have legitimate business purposes.104 A classic example of how shell corporations intertwine with money laundering involves the real estate market. Real estate can be bought with illicit funds and then resold for a nominal sum to one’s own shell corporation, which can again be resold to an innocent third party for the original purchase price.105

102 There is currently a brewing argument about the difference between the hawala system as an informal money transfer system and the more formal establishments such as Western Union. Some argue that there is an invisible line between the two, even though the latter is often illegal and the former is not. See Nkhasi (2007: 475) and Perkel (2004: 194). Cf Cuéller (2003: 450).
104 Madinger and Zalopany (1999: 32). Examples are where a criminal who has a fully functioning oil company in an OFC uses the same company as a camouflage to facilitate his illicit activities by siphoning funds through such a company. Lilley (2006: 154), Gill and Taylor (2004: 543).
However, the current trend involves the setting up of shell corporations on the internet. As will be explored later, the boundless borders of the internet, along with its anonymity features, have paved a way for shell companies to flourish. It has become much easier to establish such companies on the internet, as it only takes a few clicks of the mouse.106 With the advent of the internet, criminals have been able to bypass the hassle of fulfilling certain long-standing prerequisites for establishing physical companies, such as the lodging of an application with the registrar of companies, notifications of the local tax revenue services, amongst several others. The loopholes in local laws and international laws regarding the establishment of companies on the internet, which inadvertently foster cyberlaundering activities, will be considered further in later chapters of this study.

2.2.4.7 *Wire transfer*

The concept of wire transfer is intertwined with the notion of cyberlaundering. For this reason, it deserves a closer attention.

2.2.4.7.1 *What it means*

Wire transfer, or credit transfer, is a type of electronic funds transfer according to which funds, or the value thereof, are transferred from one person, or from one institution, to another. Wire transfers are often effected from one bank account to another, or at a cash office where the transfer of

---

cash is usually done. As a method of money laundering, wire transfer is peculiar to the subject of cyberlaundering, especially online banking, because it occasioned the dawn of electronic payment systems, which form the bedrock of cyberlaundering.

In the past, an order to transfer funds was done by way of telegraph. This was before the shift to cables. Today, funds are transferred electronically. Wire transfer is an individualized transaction which can be effected both locally and internationally.\textsuperscript{107}

2.2.4.7.2 The mechanism

For wire transfers that are done locally, depending on the country, there are several electronic funds messaging services that are established with the purpose of effecting such transfers. For example, in the United States, the Federal Reserve Bank has the FedWire system. For international wire transfers, there are also several electronic funds messaging services that perform wire transfers. The most common of these is known as the Society for Worldwide Interbank Financial Telecommunications (SWIFT).\textsuperscript{108} SWIFT


\textsuperscript{108} SWIFT is by far the largest and most popular electronic messaging service. According to its website, ‘SWIFT has its headquarters in Belgium and has offices in the world’s major financial centres and developing markets. SWIFT provides additional products and associated services through Arkelis N.V., a wholly owned subsidiary of SWIFT, the assets of which were acquired from SunGard in 2010. SWIFT does not hold funds nor does it manage accounts on behalf of customers, nor does it store financial information on an on-going basis. This activity involves the secure exchange of proprietary data while ensuring its confidentiality and integrity.’ See SWIFT (an undated website document) ‘Company Information’ available at <http://www.swift.com/about_swift/company_information/index.page?lang=en> [accessed on 15 September 2011].

is known for its ability to process high value transactions. For example, in the United States, this includes credit payments of up to $2 million and debit transfers of up to $100,000.\footnote{Pillai and Julian (2008: 219). Cf Financial Crimes Enforcement Network (2008A: 12).}

2.2.4.7.3 The problem

Wire transfer is relevant to all stages of money laundering, especially the layering stage. This can occur by transferring funds across several jurisdictions in order to erase all trails leading back to the source of the funds.\footnote{Reuter and Truman (2004: 32).} Also, with the use of smurfs who deposit funds into several accounts often located in an OFC, a laudnerer can successfully transfer funds electronically from such accounts, without leaving a trail that leads to the original source of the funds.

This transfer technique is made possible because of the gaping lacuna that exists in the SWIFT service when there is a wire transfer involving a local and an international bank. This problem is elucidated as follows:

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 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].

Thus, criminals deliberately effect wire transfers involving intermediary banks, knowing full well that investigators cannot trace the funds back to them, because such banks are unable to retain records of the person making the transfer and the beneficiary. This clearly overrides the record-keeping and reporting requirements currently prescribed by the present AML regime.

\[2.2.5 \textbf{Money laundering and rising challenges: Impact and weight of the problem}\]

As far back as 1998, when money laundering had not yet reached its current state of growth, it was ranked the world’s third largest market, next only to the US and the Euro bond markets. The impact of money laundering on a global scale is of a great magnitude. Very often the weight of the problem is undermined because money laundering is a crime of an unassuming nature. For a better understanding, it is crucial to distinguish clearly the impact of money laundering in the direct sense of the word on the one hand, and in the indirect sense, on the other hand. The direct effects of money laundering should not be difficult to ascertain, since the costs of the predicate offence can be related easily to the victim and society. It is the latter – the indirect impact of money laundering – which poses as a colossal problem, as the focus is turned away from victims, and shifted to the economy, politics and society.

\[111\] The National Drug Intelligence Program (2010: 14).
on a global scale. The indirect impact of money laundering justifies the nature of the crime as being a truly transnational one.\textsuperscript{114}

The glaring effects of money laundering cut across various sectors of society, chief of which is the financial sector. With the upsurge of money laundering across the world, the integrity, stability and reputation of the financial sector is gravely undermined, and consequently put at risk.\textsuperscript{115} When illegal funds are finally commingled with legitimate funds at the integration stage of money laundering, arguably, the entire financial sector becomes tainted with illegality. Also, the stability of the financial sector is undermined when there is an influx of high capital into commerce and interest rates and exchange rates are rendered volatile.\textsuperscript{116} These indicators suffice to force an economy into a recession.

Money laundering also has a dire impact on the business sector. Economists have argued that money laundering can affect relative prices, which in turn could lead to inflation in the market.\textsuperscript{117} Given that money launderers are willing to pay for assets which are more than their actual worth, in a bid to disguise the illegal origin of their funds, this can affect the general price of such commodities.\textsuperscript{118} For example, in the 1980s, the Medellin Group in Colombia purchased hectares of land in an alleged money laundering operation, which pushed prices up in the real estate market from $500 to

\textsuperscript{114} This is further buttressed by the fact that the ‘act’ or ‘conduct’ requirement of this crime could take place in more than one national jurisdiction across the world, thereby establishing jurisdiction in several states simultaneously.


\textsuperscript{117} Keh (1996: 38) and Unger (2007: 153).

$2000 per hectare.\textsuperscript{119} The problem of money laundering is especially pertinent to the real estate sector because it is a non-transparent market, where the actual value of objects is somewhat uncertain, and where there are sporadic fluctuations in prices.\textsuperscript{120}

In the public sector, money laundering manifests its effects in the form of unpaid taxes or tax evasion. Tax evasion is a problem that is not only typical to developed economies, but to developing and under-developed economies alike. Recent estimates show that in the Netherlands and the United States, tax evasion is the largest part of the estimated criminal income, constituting between 4\% to 6\% and 6\% to 15\% of the Gross Domestic Products (GDPs) of these countries, respectively.\textsuperscript{121}

In addition, a government’s efforts to promote privatisation are thwarted if public enterprises such as transportation, electricity and water supply fall into the hands of criminals who obtain such enterprises for the purpose of laundering money.\textsuperscript{122} In the end this cuts short a society’s hopes for growth and development. At the societal level, certain crimes go hand in hand with money laundering, and as a rippling effect, such crimes gain currency with the spread of money laundering operations. Corruption and the pollution of legal activities through illegal activities are but few examples that can be given.\textsuperscript{123}

\textsuperscript{120} Unger (2007: 157).
\textsuperscript{121} Amedeo, Bagella, and Busato (2008: 18).
\textsuperscript{122} Unger (2007: 147).
Lastly, money laundering activities have calamitous political effects, by virtue of the fact that money laundering can be used to finance terrorism, which invariably causes an increase in terrorist activities, and also undermines political institutions. The latter is a sore point, as it forms one of the principal challenges faced by the current AML regime. It has become increasingly difficult to implement AML laws in most developing countries where political leaders are themselves the perpetrators of the crime. For example, Duvalier, the former president of Haiti, and his son ‘Baby Doc,’ virtually emptied the government coffers during their successive terms as presidents.124 Governments of underdeveloped nations sometimes appear to be deliberately inactive towards the money laundering activities prevalent in their countries, not only for personal gain, but also in the national interest. For instance, the trade restrictions imposed on Iraq in the early 1990s by several neighboring countries were often not implemented. This was done purposely, as some of the countries were of the view that it would be in their own economic interests not to abide by those sanctions, even though money laundering activities that came as a consequence of trade relations with Iraq were continuously fostered on the side.125

The notion of cyberlaundering and its dire effects are not detached from the overall effects of money laundering. Some of the effects pointed out above hold equally true for cyberlaundering, because the latter taints commerce on

the World Wide Web with illegality; it serves as an instrument for political instigation and terrorist financing, and is a good tool with which to facilitate tax evasion, amongst a host of other things. Hence, the frightening impact of money laundering is precisely what makes the threat of cyberlaundering so imminent.

From the discussion thus far, we see that the notion of money laundering has come a long way in its evolution. This subject-matter, as has been understood over the years, is what is termed the traditional concept of money laundering. Cyberlaundering builds on this framework. The concept of cyberlaundering as it appears as another level of money laundering is discussed comprehensively in the next chapter.

2.3 AN INTRODUCTION TO CYBER CRIME: THE ‘CYBER ROOT’ OF CYBERLAUNDERING

2.3.1 General

At the outset, it was stated that cyberlaundering is an offspring of two very distinct and indigenous forms of criminality – money laundering on the one hand, and cybercrime on the other. Having considered the concept of money laundering, it becomes equally important to explore briefly the concept of cybercrime. This section attempts to trace the roots of cyberlaundering to cybercrime, for this helps to put the concept of cyberlaundering in its appropriate frame.
2.3.2 Understanding the term ‘cybercrime’

There is often linguistic confusion surrounding the term ‘cybercrime.’ The terms ‘cybercrime,’ ‘computer crime,’ ‘computer-based crime’ and ‘computer abuse’ are all synonyms of the same thing.\(^{126}\) Thus, for the sake of linguistic clarity, this study will use the term ‘cybercrime,’ even though, in some definitions that are yet to be analysed below, the term ‘computer crime’ is used.

Defining ‘cybercrime’ is no doubt a difficult task. Various authors have proposed different definitions for it, some of which will be considered. One of the earliest definitions is given by Don Parker, who uses the term ‘computer abuse,’ and defines it as "any incident involving an intentional act where a victim suffered, or could have suffered a loss, and a perpetrator made a gain and is associated with computers."\(^{127}\) Building on this definition, other authors have drawn out four distinct categories which Parker’s definition presents, being:

i. The computer as the target or the object of the crime;

ii. The computer as an instrument of the crime;

iii. The computer as incidental to a crime; and

iv. Crimes associated with the prevalence of computers.\(^{128}\)

---

\(^{126}\) The term ‘high-technology crime’ is often used interchangeably with the term ‘cybercrime,’ which is not correct. High technology crime refers to the use of information and telecommunications technology to commit or further a criminal act against a person, property, organisation or a network computer system. See Pocar (2004: 45).


Parker’s definition, and the four categories of cybercrime derived from it is problematic because it is technology-specific. It says nothing about what constitutes the crime itself.

Other authors have taken a different approach to defining cybercrime. Majid Yar distinguishes between computer-assisted crime on the one hand and computer-focused crime on the other.\textsuperscript{129} The former entails crimes that predate the internet, but which have taken on a new appearance since the advent of the internet, making such crimes to wear a new look. These include theft, pornography, fraud, sexual harassment, hate speech and money laundering. Cyberlaundering is found within this cocoon. The second category of cybercrime, as identified by Yar, the computer-focused crime, encompasses crimes that emerged with the advent of the internet, and which could not have come about without the existence of the internet. Examples here are website defacement, viral attacks, phishing and hacking.

Besides the two terms often used to categorise cybercrime, catch-phrases are commonly used to group some of the various types of cybercrimes. For instance, the phrase ‘cyber-trespass,’\textsuperscript{130} usually includes computer-focused crimes falling within the second category of cybercrime, whereas the terms ‘cyber-deception,’\textsuperscript{131} under which cyberlaundering falls, and ‘cyber-theft,’ ‘cyber-pornography’ and ‘cyber-violence,’ which include hate speech and

\textsuperscript{132} Interestingly, other than this categorization, a much broader system of categorization was adopted by the International Telecommunication Union, which classifies cyberlaundering as a combination offence, along with cyberterrorism, cyberwarefare and phishing. See International Telecommunications Union (2009: 51).
stalking, are all computer-assisted crimes falling under the first category of cybercrime.\textsuperscript{133}

Hence, in light of the above, the following succinct yet complete definition of cybercrime is submitted: Cybercrime is an act that is punishable by law, using an automatic electronic device that performs mathematical or logical functions.\textsuperscript{134} This definition highlights the existence of a crime as a main focus, and equally portrays the second important aspect, which is the means through which the crime is facilitated – computer/internet/high technology (hence the word ‘cyber’) - which is used to either facilitate the commission of the crime; which is incidental to the crime, or is a target of the crime.

Cybercrime has been difficult to define because of the constantly evolving and growing nature of the concept. It is no wonder that Parker’s definition, which was given in 1976, cannot be as accurate as the definition given by Reyes and others, simply because cyberlaundering did not exist at the time. This, again, shows the currency of the cyberlaundering dilemma.


\textsuperscript{134}Cf Reyes, Brittson, O’Shea, and Steele, (2007: 33), Koops and Brenner (2006: 20) and Wall (2007: 12). A comparable but more elaborate definition is as follows: ‘Cybercrime is the criminal use of any computer network or system on the internet; attacks or abuse against the systems or networks for criminal purposes; crimes and abuse from either existing criminals using technology, or a new crime that has developed with the growth of the internet.’ Pocar (2004: 33). Several international legal instruments and domestic laws have refrained from giving an outright definition of cybercrime. As is the usual pattern, some laws provide the definition of a computer system, and in a very expansive form, detail all types of cybercrime, in a bid to encapsulate sufficiently all computer-related crimes. This is evident in Chapter II of the Council of Europe’s Convention of Cybercrime 23.XI, which was adopted by the Council on 12 April 2001, and which came into force on 1 July 2004, available at <http://www.aph.gov.au/house/committee/jscct/1march2011/report/chapter11.pdf> [accessed on 16 September 2011]. Cf: The violation of information systems, akin to the definition of cybercrime in Article 1 of European Council: Council Framework Decision 2005/222/JHA on attacks against information systems adopted by the European Parliament on 24 February 2005.
2.3.3 The evolution of cybercrime in brief

Since its early days, the topic of cybercrime is one which has been dreaded by criminal investigators and prosecutors. Cybercrime crime cases would be often referred to computer experts for deciphering. Although, as an innovative phenomenon, the computer has been appealing to many since its creation, the technicalities around its operation have not been entirely alluring. Technical terms such as packets, e-mails, instant messaging service (IMS), encryption and decryption are quite tortuous to technophobes. The seemingly complex nature of computer technology creates a ‘layer of confusion,’ and, as a result of this overshadowing effect, the underlying crime component of cybercrime is often overlooked. As a result, growth in the response to the cybercrime epidemic has been slow.

Given that the internet was at an embryonic stage in the early days of computer technology - in the late 1970s and early 1980s – there were no persons personally present on the internet who committed crimes. At the time, the computer was more a target of crime than it was a tool for criminal activities. The predominant crimes against computers were hacking of government computers, phone phreaking and spreading viruses. This changed in the 1990s with the development of the World Wide Web, when people began having a more personal presence on the internet, and when

---

136 Phone phreaking can be described as the art and science of cracking a phone network in order to use it illegally. An example would be where a phone network is cracked in order to make a long distance call. See Telephone Tribute (an undated website document) ‘Phone Phreaking’ available at <http://www.telephonetribute.com/phonephreaking.html> [accessed on 16 September 2011]. Cf Moore (2011: 23).
137 Cf Curtis (2010: 22) and Clough (2010: 22).
there were more opportunities for interpersonal crimes.\textsuperscript{138} In the 2000s, with the outburst of social networks on the internet, cybercrimes reached a record high.\textsuperscript{139}

The notion of cybercrime has come a long way since its days of infancy in the late 1970s. No longer is the label attached to mere sinister attacks against a college computer facility or telephone infrastructure,\textsuperscript{140} but cybercrime now encapsulates traditional crimes which take on a new life in cyberspace – a clear example being cyberlaundering.

\textbf{2.3.4 The present state of the anti-cybercrime legal regime: An overview}

Unlike international conventions such as the Palermo and Vienna Conventions that pertain to money laundering, there are currently no far-reaching international laws against cybercrime. The only true anti-cybercrime (ACC) law, which is comparable, is the Council of Europe Convention on Cybercrime\textsuperscript{141} (the Budapest Convention). However, this Convention is a regional one.

\textsuperscript{139} In 2010 alone, the Internet Crime Complaint Center (‘IC3’), which is a division of the Federal Bureau of Investigation (‘FBI’), received over 2 million cybercrime complaints and processed about 25,000 per month. See Internet Crime Complaint Centre (2010: 1).
\textsuperscript{141} The Convention was drawn up by the Council of Europe in Strasbourg with participation of the Council of Europe and observer states Japan, Canada and China. The Convention was adopted by the Committee of the Ministers of the Council of Europe at its 109th session on 08 November 2001. On 23 November 2003, it was open for signature in Budapest, and on 1 July 2004, it came into force. As at 9 June 2012, the Convention had been ratified by 32 states parties. Together with the Convention is the Council of Europe Convention on Cybercrime: Additional Protocol to the Convention adopted by the Council of Europe on 7 November 2002 and came into force on 1 March 2006. For more information see the Treaties Office of the Council of Europe at

\textit{The Legal Regime for Anti-Cyberlaundering / Daniel Leslie}

56
The fight against cybercrime has proven impractical and contentious for law enforcement agencies lacking knowledge and expertise in information and communications technology (ICT). For them, the intangible nature of the internet simply complicates the problem. This section will look briefly into why ICT has become very useful for criminals. It will explore the existing gaps in the law in that regard.

2.3.4.1 Advantages of ICT for criminal enterprises

The current marriage between ICT and crime is more evident now than ever before. ICTs have certain, known unassailable attributes, which explains why they are good breeding grounds for criminals. They are the following: 142

a) ICTs clear each spatial hurdle and permit a global reach;
b) ICTs are globally avoidable;
c) ICTs are generally speedy;
d) ICTs basically guarantee anonymity;
e) ICTs can be very secure;
f) ICTs are characterised by multimedia capability;
g) ICTs are invariably inexpensive;
h) ICTs are easy to use;
i) ICTs are still under-regulated; and
j) ICTs are difficult for law enforcement authorities to investigate.

From the features listed above, it is clear that there are loopholes in the ICT system that criminals exploit. These loopholes do not only exist because of the fast pace at which technology continues to evolve, but mainly because the legal responses needed to contain the problem are slow, or in many instances, non-existent. This, in short, is the main dilemma of cyberlaundering and a reason why it needs to be dealt with legally.

2.3.4.2 Challenges of the present anti-cybercrime legal regime

The notion of cyber criminality only came to light in conjunction with the fast growth of the internet. Much of the elusive character of cyberlaundering lies in the obscure notion of cybercrime. Investigators, prosecutors and researchers continue to struggle with finding a definitive formula for investigating and prosecuting cybercrime. This is a Herculean task – one which is almost dissimilar to the traditional system of investigation and prosecution of ordinary crimes.

Cybercrime experts, especially investigators, usually operate within the field of computer forensics which, today, is still in its infancy. For example, the American Academy of Forensic Sciences only recently accepted computer forensics as a separate discipline under its much broader field of forensic sciences.\(^{143}\) Given its novelty and currently fluid and undefined state, the current state of computer forensics has certain negative legal ramifications for cybercrime investigators. The first, and perhaps most glaring, is the existing

disparity between the rate at which technology changes and the rate at which laws are made. The lethargic bureaucracies involved in enacting legislation are no match against the speed with which technology changes. This impacts negatively on efforts to combat cyberlaundering and other sub-genres of cybercrime, as criminals continue to have a field day.

Another legal ramification created by computer forensics relates to the collection of evidence. Of all forms of real evidence that exist, electronic evidence has the highest and the most rigid standard of proof. Investigators are required to preserve the data exactly as it appeared during the collection phase. Consequently, any form of alteration or editing would render such evidence inadmissible in a criminal trial. Given the intangible nature of electronic evidence and its susceptibility to corruption and defacement by viruses and other harmful programmes, it is often difficult for prosecutors to reproduce the exact same evidence before court.

Thirdly, the fluid state of computer forensics has indirectly resulted in the proliferation of crimes through the internet. As noted above, apart from cyberlaundering, there are several crimes that are increasingly being facilitated on the internet. If computer forensics remains static, law enforcement will continually struggle to come to grips with the dilemma. Furthermore, the proliferation of these crimes has a negative impact on the

\begin{footnotes}
\footnote{Reyes et al (supra) argues that the standard set for electronic evidence is too high, and should be lowered in order to help the work of cybercrime investigators. Reyes, Brittson, O’Shea, and Steele, (2007: 15).}
\end{footnotes}
economy. Take online piracy,\footnote{Online piracy refers to the unauthorized use of copyrighted or patented material. It is also known as online plagiarism. One of the most common examples is software piracy. See Chapter 3 below, paragraph 3.6.2.} for example: It is currently one of the biggest predicate offences for cyberlaundering.\footnote{See Chapter 3 for further discussion.} Online piracy deprives governments of huge sums in tax revenues. A recent study of the economies of most countries in the United Arab Emirates (UAE) shows that by reducing software piracy\footnote{Software piracy means illegal access granted to internet users to use or download internet software free of charge.} by 10 percent in four years from the year 2010, $566 million in new economic activities would be delivered and 841 new information technology (IT) jobs would be created in the UAE.\footnote{Cherrayil (2011) ‘Pirates still making headway in cybercrime’ available at <http://www.gulfnews.com/mobile/business/technology/pirates> [accessed on 4 April 2011].} Also, the report shows that $23 million in additional tax revenues, which the UAE governments would have otherwise been deprived of, can be generated by 2013. These statistics pertain only to the UAE. On a global scale, the report shows that reducing the global piracy rate by 10 percent over four years would create roughly $142 billion in new economic activity, while adding about 500,000 jobs and generating about $32 billion in new tax revenue by 2013.\footnote{Cherrayil (2011) ‘Pirates still making headway in cybercrime’ available at <http://www.gulfnews.com/mobile/business/technology/pirates> [accessed on 4 April 2011]. For similar projections, see also Gragido, W and Pirc, J (2011: 22).} Given the catastrophic effects of online piracy on a global economy, and the fact that it is a multi-billion dollar industry, one can only imagine how much money is being laundered through it alone.

This does not only show the currency of the cyberlaundering dilemma, but it shows the gravity of the situation and why all existing gaps in cybercrime
need to be filled in order to forge an effective legal regime for cyberlaundering. Also, as is shown in the course of this study, the nature of the Budapest Convention, and the fact that it is the only international ACC law, does not help the fight against cyberlaundering.\textsuperscript{151}

\section*{2.4 SUMMARY}

This chapter paves the way for the ensuing discussions on cyberlaundering. As indicated at the outset, this chapter represents the brick and mortar of this study. It lays the necessary foundation and maps the terrain on which the purpose of this paper can be achieved, which is forging a legal framework to combat cyberlaundering. By properly delineating and understanding the two legs of cyberlaundering - money laundering and cybercrime – subsequent discussions on the subject, its jurisprudence and legal ramifications will not be alien concepts.

\textsuperscript{151} Cf discussion in Chapter 4, paragraph 4.3.2.3.
CHAPTER 3
CYBERLAUNDERING: CONCEPT & PRACTICE

3.1 INTRODUCTION

This chapter investigates the concept of cyberlaundering and attempts to deconstruct the concept legally.\textsuperscript{152} Bearing in mind that cyberlaundering borders the fields of money laundering and cybercrime, the chapter starts off by investigating the rationale behind the advent of cyberlaundering. Furthermore, this chapter attempts to understand and categorize cyberlaundering as a legal concept, after which the elements of the crime of cyberlaundering are identified. This chapter also delves further into some technical aspects of cyberlaundering by assessing the ‘tools’ used for cyberlaundering, in the form of electronic payment systems, which are conducive to the commission of the crime. One needs to understand this at the outset in order to fully grasp the different methods and techniques used by criminals on the internet. This enables one to get an idea of what cyberlaundering might look like in the future. The latter is important for two primary reasons: First, given that the understanding of the cyberlaundering phenomenon is limited, it would be useful to describe the current trend, in order to understand aspects of cyberlaundering better. Secondly, knowing the direction in which the

\textsuperscript{152} The content of this chapter is an elaborate extension of the author’s LLM thesis entitled \textit{Anti-Cyberlaundering Regulation and Control}. See Leslie (2010: Chapter 3).
cyberlaundering wind is blowing helps to devise the regulatory legal framework to minimize the dangers it poses.

### 3.2 DECYPHERING CYBERLAUNDERING

#### 3.2.1 The meaning of cyberlaundering

The definition of cyberlaundering should necessarily reflect both the money laundering and cybercrime elements of it.

Money laundering is something that occurs every time any transaction takes place or a relationship is formed that involves any form of property or benefit, whether it is tangible or intangible, which is derived from criminal activity.\(^\text{153}\)

It is a process crime which, invariably, is not aimed directly at a person or property but against the machinery of justice itself.\(^\text{154}\)

Much like the logic behind other process crimes, such as obstructing the course of justice, contempt of court, and perjury, money laundering is effected by masking or hiding the predicate (or underlying) offence through a web of deceitful and evasive processes.

Cyberlaundering, however, adds a technological perspective to this because it also traverses the much broader terrain of cybercrime. Cybercrime can be defined as an act, which is punishable by law, using an automatic electronic device that performs mathematical or logical functions,\(^\text{155}\) for example, a

---


\(^{154}\) Murphy (2009: 1).

computer. The interplay with cyberlaundering occurs when the relevant ‘act’ in question is that of money laundering. Therefore, in light of this, the following definition of cyberlaundering is proffered:

Cyberlaundering is the use of a computer\textsuperscript{156} to form a transaction or a relationship involving property or benefit, whether tangible or intangible, which is derived from criminal activity.

Although the computer is the tool, the playing field remains the internet, hence the need now to explore the internet as a playing field for money launderers.

3.2.2 Catalysts of the cyberlaundering dilemma

In order to fully grasp the concept of cyberlaundering, one has to know how it evolved. The phenomenon of cyberlaundering was triggered with the advent of the internet, which criminals have come to use to ply their trade of money laundering. Some of the unique features and traits of the internet that form the blueprint upon which cyberlaundering thrives will now be discussed.

3.2.2.1 Speed of technology

Computers today are designed in such a way that they are able to process data at an extraordinary speed, thanks to the capabilities of the computer’s central processing device (‘CPU’). The CPU is measured in giga hertz (‘GHz’),

\textsuperscript{156} See paragraph (c.) of the discussion in paragraph 3.2.4.2.1 below.
which determines the speed with which data is processed. What also determines speed is the computer’s Random Access Memory (‘RAM’) and the graphics card. The former refers to a depository where current files are being used or stored. Hence, with a very fast RAM, easy access to one’s files can be guaranteed. The graphics card on the other hand is the hardware that processes graphics. With a very fast graphics card, more graphics, or displayed images or frames, can be processed per second, which is crucial for computer and online gaming.

The speed of computers is further complemented by an equally fast internet service. With the transition from dial-up internet access to broadband internet access – the latter averaging about four megabytes per second, as opposed to the former’s sixty kilobytes per second – a high data rate connection is guaranteed.

It is certainly not far-fetched to think that cyberlaundering is linked directly to all these basic features of technology, because without these features, the notion of cyberlaundering will be non-existent. This becomes clearer in the discussion on cyberlaundering methods and techniques.

3.2.2.2 Access to the internet

The internet is the virtual playground for cyberlaundering. Evolving originally from several military projects of the United States government in

158 Molly and Parker (2010: 23). Online gaming refers to gaming activities that occur within the environment of the internet. Cf discussion in paragraphs 3.5.3 and 3.5.5 below.
159 Cf Shelly (2010: 44).
the late 1960s, the internet today aids cyberlaundering because it has become a common luxury for all, given its ubiquitous nature and presence. In its early days, which is the 1990s, the internet was popular only amongst businesses and households, mainly in the United States (US) and the United Kingdom (UK). This popularity was based on an increased awareness of the internet’s functionalities and infinite capacity. This is why it can be said that cyberlaundering is borne out of the globalization of the internet. Gone are the days when only an elite class of people had sole access to such opulence.

Today the world is a global village, thanks to the internet. But for certain human activities that cannot be done on the internet, such as eating and drinking (at least not yet), numerous things are doable on the internet.

Access to the internet continues to grow. Recent statistics show that over 2 billion people, of a world population of more than 6 billion people, have access to the internet. In the previous decade, this number was a measly 360 million. The number has increased by a solid 480% between the years 2000 and 2011.

The fact that one’s everyday life basically revolves around the internet has caused it to be an indispensable resource for numerous human activities.

---

162 A breakdown of the figure shows the following: In Africa, there are about 118, 609, 620 people; in Asia 922, 329, 554; in Europe 476, 213, 935; in the Middle East, 68, 553, 666; in North America, 272, 066, 000; in Latin America, 215, 939, 400, and in Oceania/ Australia, 21, 293, 830 people. See Internet World Stats <http://www.internetworldstats.com/stats.htm> [accessed on 15 July 2011].
Accessibility to the internet has become a hotly contested topic, and the debate has even shifted onto the legal sphere, giving rise to many deliberations over the years. In 2003, during the United Nations World Summit on the Information Society, it was proposed that access to the internet should be entrenched as a fundamental human right. Since then, several countries such as Finland, France, Greece, Spain and Estonia have made access to the internet a part of the basic fundamental rights of an individual. This shows the seriousness and importance of the issue of internet accessibility. In the aforementioned countries, and in others as well, it goes without saying that having access to the internet in modern times is crucial for all individuals. It is almost now on the same pedestal as the right to life. The International Telecommunications Union (‘ITU’) has also joined in the campaign to globalize access to the internet, and has spearheaded several projects across multiple continents in order to achieve this goal. The European Union (‘EU’) is also hard at work ensuring that the right to internet access is safeguarded. This is evidenced by the EU Amendment 138/46 of the Telecommunications Reform Package, now article 1(3)(a) of the Framework Directive, which is to be adopted into law into all EU countries that are states parties.

167 For more information on the projects of the ITU see <http://www.itu.int/ africainternet 2000/Documents/doc7_e.htm> [accessed on 15 July 2011].
Other countries that share this notion, but that have yet to entrench it as a fundamental human right, are South Korea, Mexico, Brazil, Turkey and Nigeria. In the same survey conducted, results show that these countries feel strongly against government regulation of the internet, although a majority of other countries in Asia and Europe have disagreed.

Furthermore, access to the internet has not only become affordable, but also convenient, especially with the notion of cloud computing. The latter means anything that involves delivering hosted services over the internet and it works in such a way that one can gain access to data/information contained in a hosted service on the internet, using different computers. What is more, in this modern age, a computer need not be a desktop or laptop apparatus; it could also be a phone or any personal digital assistant (‘PDA’).

---


Government interference or regulation of the internet has always been a sensitive issue. As this study shows, regulation of the internet is very expedient in order to prevent problems such as cyberlaundering that plague economies the world over. However, the main issue is not whether or not regulation should occur, but the extent of it. For instance, in the United Kingdom (‘UK’), the controversial Digital Economy Act 2010 (Chapter 24) promises to deliver universal broadband in the UK by 2012. This law gives regulators new powers to disconnect or slow down the internet connections of illegal file-sharers and other cyber criminals. Countries such as France and Germany are also considering introducing similar laws. British Broadcasting Cooperation <http://news.bbc.co.uk/2/hi/8548190.stm> [accessed on 15 July 2011].


Cloud computing differs significantly from a traditional hosting service, as it is sold on demand. The user can determine how much of the service it wants at a given time and the service is fully managed by the relevant provider. See Searching Cloud Computing (an undated website document) ‘Cloud Computing’ available at <http://searchcloudcomputing.techtarget.com/definition/cloud-computing> [accessed on 15 July 2011].
One very glaring fact is that easy accessibility to the internet on a global scale will spiral in growth over the next couple of years, as statistics have shown. As a downside, without efficient regulators in place to minimize its abuse, especially for purposes of money laundering, the phenomenon of is bound to grow concomitantly.

### 3.2.2.3 Anonymity

The issue of anonymity has always been a subject of contention, even before the debate shifted to internet anonymity. Initially, the issue of anonymity was pitted against one’s fundamental right to freedom of expression, free speech, privacy and so on.\(^{174}\) This debate has been transposed onto the internet since its advent. The internet has the feature of anonymity, as it allows individuals to conduct activities without disclosing their true identities or without any possible direct traceability. However, the notion of anonymity in this context differs from some of its variants, such as pseudonymity and allonymity.\(^{175}\) The latter forms of anonymity, when used on the internet, could have good purposes.\(^{176}\) Amongst some of the advantages that anonymity holds is its possible use by people under a repressive political regime to vent their opinion.\(^{177}\) It could be used to disclose information that is extremely personal, such as sexual problems. It could serve as a platform to express opinions, thus

---


\(^{175}\) Pseudonymity refers to the case where one uses another’s name or takes on another’s persona in order to make an artistic or literary expression. Allonymity is a slight variant of the former, as it refers to a writer’s assumption of an historic literary figure in a literary writing.

\(^{176}\) Cf Joinson (2001: 177), Wallace (1999: 3) and Abelson (2001: 1).

promoting egalitarianism and rendering attributes of gender and race immaterial.\textsuperscript{178}

Unfortunately, the few benefits associated with anonymity on the internet are overshadowed by the more glaring disadvantages. From the seemingly endless list of demerits of anonymity that are germane to the internet’s framework, a criminal could spin a perfect web of transactions over the internet, thus obliterating all traces of the original act. This essentially, is what cyberlaundering is. Given the many dangers that are caused by the internet as a result of its anonymity feature, several authors have argued for a ‘reconstruction’ or ‘restructuring’ of the internet to ensure universal identification, thus completely burying the notion of anonymity.\textsuperscript{179} Though logical, this argument implies, albeit generally, that one should wipe the slate clean on which the internet’s framework is sketched because anonymity is part of the very fabric of the internet, and forms a core of its blueprint. The pros and cons of this argument are considered in an ensuing discussion.\textsuperscript{180}

\textbf{3.2.2.4 Boundless borders}

For much of its life, the internet has witnessed sporadic changes in development, but a constant factor in its evolution is its incessant nature of shrinking the world into one small space. The manner in which information is accessible through the internet traverses physical borders and known

\textsuperscript{180} Cf discussion in paragraph 6.2.2 of Chapter 6.
boundaries. Indeed, the phenomenon of the internet defines modern times. However, such convenience has raised eye-brows and continues to spur curiosity. On the one hand, many wonder why governments of the day are overly cautious about censoring the internet, whereas, on the other hand, the fundamental right of access to information is asserted vigorously.\(^{181}\) For the first argument, the current situation in Italy, involving the presence of the giant internet company, Google, serves as an example. The Italian government recently recognized YouTube\(^{182}\) as a television station which is subject to television regulations.\(^{183}\) This implies that Google would have to start paying taxes as a television broadcaster, and it would be liable for its contents. YouTube has been banned in several countries such as China and Morocco, as people often post videos that their governments have deemed offensive and having the capabilities of inciting anti-government protests.\(^{184}\) Also, in January 2010, the Libyan government blocked access to the website for this reason.\(^{185}\)

The instances cited above, however, are only isolated incidents. The fact still remains that information sharing over the internet continues to grow, and several governments, amongst them those of the United States and the United Kingdom, still promote anti-censorship and strongly uphold the rights of freedom of expression. It could therefore be said that, currently, the pendulum

---

181 Baran (2011: 2).
182 Youtube is owned by Google and is the world’s largest video sharing website, boasting billions of users from around the world.
183 Baran (2011: 2).
is swinging in favour of a borderless internet environment. The difficulty of this issue is expressed below:

The difficult area is that while countries understand the benefits of information sharing on the internet, they also see that practices such as digital terrorism, large-scale crime, fraud, spam, stalking and pornography are on the rise[...] The sensitive part of the debate, as with all debates about censorship, is not whether some of these areas need to be excluded from the internet but where the line is drawn between legitimate threat or security risk and governments taking on the role of our political, moral and ethical minders.\(^{186}\)

The proliferation of information through the internet and the ease of gaining access to it have resulted in both good and evil, with the latter manifesting in the form of cyberlaundering, as further discussions will show.

### 3.2.3 Categorizing cyberlaundering

Cyberlaundering traverses two distinct fields of crime – cybercrime on the one hand, and money laundering on the other. This makes it a hybrid discipline that poses the question: How should one see cyberlaundering and under what category of crime does it fall? As part of the quest to understand the subject for purposes of establishing an appropriate legal framework for it, it is necessary to see it through the right lenses. From the outset, therefore, it must be fitted in the right frame. Without establishing the parameters of

\(^{186}\) Hughes (2010: 1).
cyberlaundering, one may falter along the way, as the notion itself could be ensconced in one big conceptual blur. The following discussion juxtaposes the varying possible categories into which the concept of cyberlaundering falls, or ‘lenses’ through which it should be seen.

3.2.3.1 Cyberlaundering as a subset of cybercrime

Should cyberlaundering be couched just as a subset of cybercrime? If cyberlaundering is indeed seen as a subset of cybercrime, it would mean that it falls squarely within the area of cybercrime, without the element of money laundering. If this is the case, one may be forced to look solely to the field of informatics\(^{187}\) to find regulatory measures for it.

However, this notion cannot be entirely acceptable. Although it is accepted that cyberlaundering has roots in cybercrime, one must not lose sight of the core element of money laundering. Hence, the crime at its core is money laundering, with a technological aspect.

3.2.3.2 Cyberlaundering as a technique of money laundering

Another popular school of thought on cyberlaundering considers not only the money laundering element, but sees cyberlaundering solely as a mere

\(^{187}\) Informatics is the science of information, the practice of information processing, and the engineering of information systems. Informatics studies the structure, algorithms, behaviour, and interactions of natural and artificial systems that store, process, access and communicate information, i.e. the computer. It also develops its own conceptual and theoretical foundations and utilizes foundations developed in other fields. Fourman (2002: 1).
technique within the marquee of money laundering.¹⁸⁸ For this reason, when the method used by a criminal to launder funds is internet-based, then the conclusion is quickly drawn that money laundering has been committed through that technique. This notion might be plausible if one looks at the broad concept of money laundering, which entails several other aspects, for instance, trade-based money laundering.

It would nevertheless be entirely incorrect to accept that cyberlaundering is only a technique of money laundering. To think of something as a ‘technique’ of another would mean that the latter is a means to an end, and, impliedly, that it cannot stand on its own. As regards cyberlaundering, the fact that a criminal utilizes technological resources does not make such resources merely a tool for the money laundering enterprise; conversely, this makes the criminal’s activity the money laundering enterprise.

### 3.2.3.3 Cyberlaundering: ‘Money laundering 2.0’

So what then could be the correct conceptual phrasing of cyberlaundering? The answer lies at the heart of the crime itself, which is money laundering. A rather astute answer is that cyberlaundering is money laundering, which appears at a more advanced level, given its roots in technology. Although it overlaps with the concept of cybercrime, it should not be seen entirely in that light. Arguably, the gravity of the cyberlaundering problem, which already

---

¹⁸⁸ Some authors have described cyberlaundering in this light. See Hunt (2011: 133) and Filipkowski (2008: 4).
embodies the behemoth weight of money laundering, exceeds the severity of other kinds of cybercrimes combined.\(^{189}\)

It is important to know the right category in which cyberlaundering falls, because understanding the right framework, would inadvertently determine the kind of liability it creates. Having accepted that cyberlaundering is money laundering, the primary liability it creates is the liability for money laundering. However, cyberlaundering is unique for the fact that it is likely to create subsidiary or ancillary liability for the criminal other than the liability for money laundering. It could incur liabilities under the broad notion of cybercrime, or other subsets of cybercrime, in jurisdictions where such crimes are recognized. Such ancillary liability differs from the traditional predicate offences that usually establish liability for the crime of money laundering. For instance, a cyberlaunderer is likely to be found liable for crimes such as hacking or cyber-vandalism, both of which might not necessarily be predicate offences for the main crime of money laundering. This comes to light in the ensuing discussion on the vulnerable industries for cyberlaundering.\(^{190}\)

Another point that supports this conceptual phrasing of cyberlaundering is the aspect of prosecution.\(^{191}\) When a prosecutor prosecutes individuals who have

\(^{189}\) This is highly debatable. One report shows that in the United Kingdom alone, banks loose up to £1 million per day in phishing and malware attacks. See Evron, G (2008: 1). Another report shows that, on an annual basis, an average of $52 million is lost to organisations in the United States alone as a result of cybercrime attacks. See ArcSight (2010: 1). These statistics, however, present sector-based facts. There are not very detailed statistics showing the economic impact of cyberlaundering as yet. However, riding on the notion that over $5 trillion is laundered on an annual basis (as far back as 2007), and that a substantial percentage is added through cyberlaundering, the statement would not be far-fetched. See Ehrenfeld and Lappen (2007: 1).

\(^{190}\) See paragraph 3.5 below.

\(^{191}\) See Chapter 5 for further discussion.
engaged in cyberlaundering activities, the name of the crime that should reflect on the charge sheet is the phrase ‘money laundering,’ not cyberlaundering.\textsuperscript{192} In essence, cyberlaundering is not a separate crime from that of money laundering. It remains under the umbrella of the latter. The sad reality is that the gravity of the cyberlaundering dilemma gives rise to an escalation of the current money laundering problem. This hinges on the overall purpose of this study, which assesses the possibilities of forging a proper legal framework to counteract the problem. However, a foreseeable challenge to actualizing this goal lies in one underlying truth - cyberlaundering is a legal problem with very complex legal ramifications.

3.2.4 Elements of the crime of cyberlaundering: a deductive analysis

It is often said that computers do not commit crimes, but people do. However, regarding cybercrime, particularly for law enforcement agencies, identifying the person(s) behind the computer is much like finding a needle in a haystack. Given the highly complicated intricacies of information technology that criminals play on, one is almost led to believe that computers might well be the perpetrators. This is compounded even further when the crime in question is that of money laundering, in which the criminal adopts the existing complexities of the internet to hide illegal proceeds. Therefore, proceeding from the standpoint that cyberlaundering is a crime premised on money laundering, as the mother crime, and with an extension to

\textsuperscript{192} This is so because of the question of legality, hence why cyberlaundering has to be conceptualized legally. See discussion in Chapter 5, paragraph 5.5.1.1.1.
cybercrime, it is important to examine the various elements of the crime. The elements of the crime of cyberlaundering, as discussed below, are not supplementary to the elements of the crime of money laundering, but only complementary. Not only is this important for the sake of having a better understanding of it, but also, knowing the elements of the crime is crucial for prosecuting the crime, as is shown in a subsequent chapter of this study.\footnote{See Chapter 6.} Understanding these elements will aid criminal investigators, as they would be able to identify and prove the existence of cyberlaundering activities, which will help them show that the criminal is guilty of money laundering.

Just as was done with regard to the definition of cyberlaundering given above, it is vital to examine the various elements of the crimes of money laundering and cybercrime, as a basis for determining the elements of cyberlaundering. It is only by juxtaposing the elements of these crimes that one can one deduce definitively the elements of the crime of cyberlaundering.

### 3.2.4.1 Elements of crimes: money laundering and cybercrime

In criminal law, in order for a conduct to constitute a crime, two distinct elements must be present – \textit{mens rea} on the one hand, and the \textit{actus reus} on the other. \textit{Mens rea} refers to the culpable mental state of the perpetrator, otherwise known as the internal or subjective element.\footnote{The full Latin phrase is \textit{actus non facit reum nisi mens sit rea}, which means that the act does not make the person guilty unless the mind is also guilty. Cf Welling (1989: 234), and Schell (2004: 19).} \textit{Actus reus} is the so-called external or objective element, which means the prohibited act or failing
to act when one is under a duty to do so. In order for one to be liable for a crime, both these elements – the subjective and objective elements - must be present.

For money laundering, the *actus reus* requirement exists as the object of the crime and the objective aspect of the crime. The object of the crime refers to the violation of government or state activities and its management system by causing instability in its financial sector, and obstructing the normal activities of the judicial investigation of crime. The objective aspect of the performance refers to the disguise and concealment of the proceeds of the relevant criminal activity. In addition, knowledge or intention must exist on the part of the perpetrator for the conduct described under the *actus reus*, in order to fulfil the *mens rea* element.

The *actus reus* and *mens rea* also form the two main components of the elements of cybercrime. For the *actus reus*, there must be a violation of a right, by way of an act or an omission (the object of the crime), using an automatic electronic device that performs mathematical or logical functions, i.e. a computer (the subject of the crime). The concept of cybercrime is an embedded term which embodies different kinds of crimes, such as cyberlaundering. For example, the right that is violated would therefore depend on the nature of the relevant crime. Thus, for cybercrime, the minimum requirement is for the violation of a right or interest to have

---

197 This aspect of *actus reus* usually follows the money laundering circle of placement, layering and integration. See Welling (1989: 288).
occurred with the instrumentality of information technology or a computer.\textsuperscript{198} The ambit is clearly wide enough to accommodate the concept of cyberlaundering, as will be apparent from the ensuing discussions below. The perpetrator must also have knowledge or intent \textit{in tandem} with what is being done (the act or omission). Also, coupled with the \textit{actus reus} and \textit{mens rea}, for cybercrime, there must be harm caused to persons and/or property.\textsuperscript{199}

3.2.4.2 Elements of the crime of cyberlaundering

In view of the definition given of cyberlaundering, and the elements of the crimes of money laundering and cybercrime, the following elements of the crime of cyberlaundering are identified:

3.2.4.2.1 \textit{Actus reus}

In order to fulfil the \textit{actus reus} requirement of cyberlaundering, certain principal requirements must be met, namely a predicate offence, illegal funds, an activity and a computer.\textsuperscript{200} These are elaborated upon as follows:

(a.) Predicate offence and illegal funds

The presence of illegal funds as an element of cyberlaundering has a direct bearing on the traditional notion of money laundering. By establishing that a criminal is in possession of illegal funds, prosecutors would be able to

\textsuperscript{199} Brenner (2004: 29) and Schell (2004: 10).
\textsuperscript{200} For a practical understanding of these elements, see Chapter 6, paragraph 6.3.3.3.1.\end{flushleft}
establish successfully the fact that the crime of money laundering has been committed. It is important to reiterate, as stated earlier, the jurisprudential resolve that cyberlaundering is still money laundering, albeit appearing at a more advanced level.

The presence of illegal funds means, inadvertently, that a crime must exist (otherwise called a predicate offence) from which such funds are derived. In other words, there must be a predicate offence which occasioned the cyberlaundering activity. As discussed earlier,²⁰¹ in the spirit of the Forty Recommendations plus Nine Special Recommendations of the Financial Action Task Force (FATF), the notion of predicate offences for money laundering entails all serious offences, and is not at all confined to a particular class of offences or crimes.²⁰² Similarly, the predicate offences for cyberlaundering are in no way limited, neither to ordinary internet crimes, or cybercrimes, nor to traditional crimes such as theft and fraud.

The source of the illegal funds that criminals use to conduct activities over the internet must be considered from the hindsight of the notion of legality and illegality. As a standard norm, if one’s conduct is considered a crime in terms of customary law or the statutory law of the relevant jurisdiction where the crime was committed, and at the time it was committed, the principle of legality is met.²⁰³ If otherwise, then one would be dealing with the notion of

²⁰¹ See Chapter 2, paragraph 2.2.
²⁰³ This principle of legality is also known as the nullum crimen sine lege, nulla poena sine lege principle – a literal translation being no crime without law, no punishment without a law. Cf Kreß (2010: 32).
illegality, which would imply that the inherent rationale behind the *nulla poena sine lege* principle has been defied. All crimes are premised on this notion, and it is an important consideration when ascertaining the presence of a predicate offence, or the fact that the suspect is in possession of illegal funds. Thus, in this sense, illegal funds are funds that are derived from an activity or conduct deemed criminal. With that said, one must remember to judge every case according to its own merits.

(b.) An activity

A cyberlaunderer must have been involved in an activity of some sort. According to its dictionary definition, “an activity is a condition in which things are happening or being done or a busy or vigorous action or movement.” In light of this definition, an activity could be a transaction, amongst several other possibilities. What constitutes a transaction depends on the circumstances of each case. However, a transaction is often understood, in the commercial sense of the word, as involving the purchase or sale of goods or items. A good example would be where a criminal purchases casino chips online at an online casino with the proceeds of crime. Alternatively, it is possible for the criminal to simply transact with himself. A perfect example is where the criminal opens a shell company on the internet, and records invoices for phantom transactions in order to create a veneer of legitimacy.

---


205 Cf paragraph 3.5.3 below.
By using the word ‘activity,’ instead of the word ‘transaction,’ one is careful not to be entirely restrictive, given the fact that there are innumerable ways through which a criminal can manoeuvre illegal funds over the internet which would not necessarily constitute a transaction. For instance, the criminal could merely play online games with illegal proceeds. This activity does not exactly fit into the meaning of a transaction, but engaging in such activity might fulfil this fundamental element.

(c.) A computer

A computer is known by several names. It is usually described as an automatic electronic device that performs mathematical or logical functions, or, put simply, a data processing device. The computer is probably the most powerful innovations in the history of humanity. Computers have enabled people to perform staggering amounts of computations at a very high speed, given that large amount of information is crunched, organized, and displayed at the wink of an eye.

Years back, the idea of a computer was, strictly speaking, a large box (commonly known as a desktop), with an equally large central processing devise (CPU); a key board and a mouse, the hand-held device. Over time, with tremendous technological advancements, the computer was scaled down with reduced energy requirements in order to broaden its capabilities. Today, other than the traditional desktops and laptops, interactive devices of all sorts

---

207 Cf Shelly (2010: 34) and Molly and Parker (2010: 61).
now contain their own computers. For instance, there are cellular phones, portable organizers, personal digital assistants (PDAs – also called palmtop computers and personal data assistants), automated teller machines (ATMs), and most recently, tablet computers with audio-visual capabilities. In spite of the kinds of computers that exist today, and their state of the art features, computers are poised to become more pervasive with the advancement of technology.

And what would the world be without the internet? The internet complements the use of computers and has even inspired the present state of the computer technology. Some of the interactive devices mentioned are virtually useless without them having internet capability. Hence, with the presence of computers and the internet, the perfect combination is created. Albeit good and bad, the latter resonates in the area of cybercrime, and, for purposes of this study, cyberlaundering.

Thus, a computer plays a vital role in establishing the actus reus element of the crime of cyberlaundering.

3.2.4.2.2 Mens rea

The element of mens rea is an element of a criminal conduct that is necessary to incur liability. Mens rea refers to the state of mind of the accused – the so-called internal or subjective element – which tends to justify the conduct, or act, or, omission of the accused. This element is applicable to virtually all

---

209 Cf Molly and Parker (2010: 30).
kinds of crimes, except strict liability crimes, in terms which the state of mind of the accused plays no role. Determining the relevant *mens rea* always proves to be daunting, due to the fact that it is not very easy to ascertain the contents of the human mind. Before one delves into how *mens rea* is ascertainable within the spectrum of cyberlaundering, it is important to first engage in a careful deconstruction of the notion.

Given the fluidity of the human mind, there are several levels or categories of this subjective element in the form of intent, knowledge, recklessness, negligence and wilful blindness.\(^{210}\) Intent is the highest level of *mens rea*, and it means that the person’s state of mind is such that he/she desired to carry out the action and can foresee the results.\(^{211}\) Intent is often determined by studying any available evidence in order to determine the state of mind of the accused when he committed the relevant crime.\(^{212}\) Depending on the relevant crime, intent could be general (that the accused consciously performed the act that constitutes the offence) or specific (that the accused had a further intent to commit the particular crime in addition to the general intent he has already).\(^{213}\)

---

\(^{210}\) Snyman (2002: 167).

\(^{211}\) Determining the relevant *mens rea* can be quite daunting, and even more so within the context of cyberlaundering. Cf discussion in Chapter 6, paragraph 6.3.3.7.

\(^{212}\) Snyman (2002: 167).

\(^{213}\) Good examples are the crime of breaking and entering with the intent to commit an indictable offence, or assault with the intent to commit grievous bodily harm. For a more elaborate discussion on this, see Snyman (2002: 167).
Knowledge is also another form of *mens rea*. In this case, *mens rea* is determined from the wording of the relevant statute or law.\(^{214}\) Here, knowledge of certain facts will be sufficient to provide *mens rea* without proving that the accused had the intent to perform the said act. *Mens rea* could also appear as recklessness, which means consciously taking an unjustifiable risk with the safety and property of others that a reasonable person would not take. *Mens rea* could also be present by way of negligence. Negligence would suffice where the accused failed to take certain steps to avoid a danger which a reasonable person would have taken if in the position of the accused, but the accused failed to do so.\(^{215}\) The latter differs from wilful blindness which occurs where a person acts knowing, almost convincingly, that his/her actions are criminal but decides to turn a blind eye to it.\(^{216}\)

The possibility of applying the different levels of *mens rea* to the case of cyberlaundering would depend entirely on the merits of each case, and the facts upon which the prosecution relies to prove its case.\(^{217}\) Gleaning from the different components of the *actus reus* requirement, as a general rule, the *mens rea* for cyberlaundering should often include the following:

---

\(^{214}\) For example, section 342 (1) (d) of the Criminal Code of Canada, Revised Statute of Canada, 1985, states that ‘everyone who uses a credit card that knows is revoked or cancelled is guilty’ of an offence. Therefore, here, one need only prove that the accused used the credit card, *knowing* it is revoked.


\(^{216}\) Cf Snyman (2002: 168).

\(^{217}\) See Chapter 6, paragraph 6.3.
(a.) *Knowledge* of the illegality of the funds

A cyberlaunderer should have knowledge of the fact that the funds in his/her possession are illegal. It is not sufficient that the accused merely thinks, or is negligent of the origin of the funds. Actual knowledge is essential to found liability. This requirement will not be met where the accused is in possession of illegal funds and is ignorant that such funds are illegal.

(b.) *Associative intention* with the illegal funds

In order to completely establish the *mens rea* element, it would not suffice for the cyberlaunderer to have only knowledge of the fact that the illegal funds in his/her possession are illegal. An associative intention is necessary. This begs the question: For what purpose are the funds held? Herein lies the requisite intention. An accused should be in possession of the illegal funds for the *purpose* of conducting one or more of the following activities:

(i.) Hiding funds from law enforcement bodies; or

(ii.) Concealing or disguising the nature, location, source and or ownership or control of the proceeds of the crime; or

(iii.) Avoiding a legal obligation to report the transaction under the law.

These three possibilities are all geared towards one overarching purpose, which is to prevent the violation of the protected interests of the Anti-Money Laundering (AML) regime. The protected interests of the AML regime are the stability of the economy, both local and international, and the effective operation of judicial and law enforcement bodies and/or agencies. When a criminal tries to ‘clean’ ‘dirty money’ by circumventing standards, norms,
rules and regulations that exist to maintain the stability of the local and/or international economy, this has a crippling effect on the economy as the conduct destabilizes both local and international economies.\textsuperscript{218} Moreover, the functions of the judiciary and law enforcement bodies are undermined by the criminal’s connivances and trickery.

These \textit{actus reus} and \textit{mens rea} elements are discussed more practically in Chapter 6 of this study.\textsuperscript{219}

\section*{3.3 ELECTRONIC PAYMENT SYSTEMS: NEW TOOLS FOR LAUNDERING}

It was once said that money does not have to be a legal tender created by governments. Like law, language and morals, it can emerge spontaneously.\textsuperscript{220} The exponential growth of electronic payment systems (e-payment systems) caused by the internet affirms this statement.

E-payment systems refer to the means through which payment can be made over the internet.\textsuperscript{221} It entails a financial exchange, usually in the form of an encrypted financial instrument, such as an encrypted credit card number, digital cash or an electronic cheque, which is usually backed by a bank, an

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{218} Cf discussion in Chapter 1, paragraph 1.2.1.3.
\item \textsuperscript{219} The \textit{actus reus} and \textit{mens rea} elements are discussed elaborately in Chapter 6 of this study, which deals with the prosecution of cyberlaundering, at paragraphs 6.3.3.3.1, 6.3.3.7 and 6.5.
\item \textsuperscript{220} Von Hayek (1978: 12). Cf Dionysios (2010: 19).
\end{itemize}
\end{footnotesize}
The Legal Regime for Anti-Cyberlaundering / Daniel Leslie

intermediary, or a legal tender.\textsuperscript{222} The evolution of e-payment systems began with the concept of electronic funds transfer\textsuperscript{223} (EFT) in the 1940s.\textsuperscript{224} EFT gave rise to the notion of a transferable information-based data through computer and telecommunication components. The concept of EFT has now been largely replaced with electronic commerce payment systems which are online-based.

E-payment systems are becoming more institutionalised by the sheer propagation of its trust-based system,\textsuperscript{225} even as established institutionalized financial infrastructures fail to fully comprehend the workings of this novelty. Similar to the terrestrial commerce systems which depend entirely on the notion of trust between strangers, the exacerbation of the e-payment system is fuelled by this rationale, because trust between its users is being forged increasingly.\textsuperscript{226}

Cyberlaundering is based on the concept of e-payments. As a sickle is to a wheat farmer, so is electronic money, or e-money, to a cyberlaunderer. E-money is particularly significant because of the notion of ‘illegal e-money.’ In the terrestrial world where the traditional notion of money laundering is the order of the day, the opposite concept exists in the form of illegal hardcash.

Illegal e-money refers to funds which are either derived from the cyberworld,

\begin{flushright}
\textsuperscript{223} Electronic Funds transfer refers to the transfer of funds initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape in order to instruct or authorize a financial institution to debit or credit an account. Manzoor (2008: 214) and Lassila (2011: 54).
\textsuperscript{225} Dionysios (2010: 19).
\end{flushright}
which is the environment of the internet,\(^{227}\) or funds that were originally illegal hardcash, but became converted into illegal e-money.\(^ {228}\) With respect to the second category, illegal hardcash can be converted into illegal e-money through the use of e-payment systems. This is why the ensuing discussion is of great relevance.

In this section, the notion of e-money is explored in further depth, in order to bring to light the practicalities surrounding it, and why it represents the perfect weapon being wielded for cyberlaundering purposes.

3.3.1 Electronic money

Electronic money (‘e-money’) can be described as monetary (or equivalent) value which is represented in an electronic format.\(^ {229}\) A more elaborate definition is as follows:

[Electronic money] is a system that allows a person to pay for goods or services by transmitting a number from one computer to another. Like the serial numbers on real dollar bills, the digital cash numbers are unique. Each one is issued by a bank and

\(^{227}\) An instance where illegal funds can be derived from the cyberworld is when one profits from running an unlicensed website on the internet. See elaborate discussion in Chapter 6, paragraph 6.5.2 below.

\(^{228}\) An example of this can be seen in several cyberlaundering techniques, such as virtual worlds, online banking, online gambling and online barter trade to name a few. See discussion in paragraph 3.5 below.

\(^{229}\) Cf an alternative definition by the European Union: “Electronic money means electronically, including magnetically, stored monetary, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions […], and which is accepted by a natural or legal person other than the electronic money issuer.” See Article 2(2), Council of Europe: Council Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions, adopted by the Parliamentary Assembly on 16 September 2009, and which came into force on 30 October 2009.
represents a specified sum of real money. One of the key features of digital cash is that, like real cash, it is anonymous and reusable.\footnote{Webopedia (an undated website document) ‘Digital Cash’ available at <http://www.webopedia.com/TERM/D/digital_cash.html> [accessed on 04 August 2011]. Several other definitions of e-money have been proposed as well. For example, the Electronic Money Institutions European Directive defines it as monetary value as represented by a claim on the issuer which is: (i) stored on an electronic device; (ii) issued on receipt of funds of an amount not less in value than the monetary value issued; (iii) accepted as means of payment by undertakings other than the issuer.’ See Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions (O.J.E.C. L275/39, 27/10/2002). The latter definition is very elaborate. One very important criticism that can be levied against it is that it confines the notion of electronic cash to monetary value, thereby automatically excluding internet cash, such as DigiCash and store reward points.}

A key feature of e-money is that it is usually held in online banking systems, and not in physical form. In countries such as the United Kingdom and the United States, only a small fraction of money is held in cash, as most of it is in the digital form.\footnote{Javelin Strategy and Research (2010) ‘Online Retail Payments Forecast 2010 – 2014: Alternative Payments Growth Strong but Credit Card Projected for Comeback’ available at <https://www.javelinstrategy.com/research/Brochure-171> [accessed on 4 August 2011].} Despite the dip in the economies of these countries in recent times, domestic e-commerce climbed 10.8% from $185 billion (£113 billion) in the year 2008 to $205 billion (£125 billion) in the year 2009, respectively.\footnote{Javelin Strategy and Research (2010) ‘Online Retail Payments Forecast 2010 – 2014: Alternative Payments Growth Strong but Credit Card Projected for Comeback’ available at <https://www.javelinstrategy.com/research/Brochure-171> [accessed on 4 August 2011].} This increase was facilitated by the spiralling growth in e-payment systems in the 2000s.\footnote{Compan
proliferation of cyberlaundering practices over the internet, should the status quo of the dilemma remain unchanged.

The advent of e-money can be attributed to several factors, such as the continuous decrease in the costs of technology. This can be attributed further to the growing affordability and availability of computers on the one hand, and, on the other hand, the advent of the internet. The ubiquitous nature of technology has driven commerce online, and is causing an unprecedented growth in e-commerce. What is more, traditional payment systems are becoming cumbersome, especially when compared to the ease and convenience created by e-payment systems, and the fact that the customary payment systems do not support micro-transactions in a way the internet is known to do and to facilitate. Another important consideration is the fact that e-money is shrouded in anonymity, which renders it a more attractive tool for cyber launderers. E-money guarantees anonymity either directly or indirectly. For the former, a cyber launderer could make use of truly anonymous products that do not use customer identification, whereas, for the


235 Fairlie and Chatterji (2011: 23). Cf paragraph 3.2.2.2 supra.


latter, the cyberlaunderer could abuse personalised products by using false identities, smurfs,239 or a nominee third party.240

According to the Financial Crimes Enforcement Network (‘FinCEN’),241 the surging proliferation of e-money in modern times might have its advantages for consumers, albeit incomparable to the threat it poses, as shown below:

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.242

3.3.2 Models of e-payment systems

E-payments can either be card-based or software-based.243 In order to understand these methods or kinds of e-payments in greater depth, it is crucial to delineate the different patterns or models of e-payment systems. According to a report by the World Bank, there are predominantly four e-payment systems that expose the different avenues through which e-payments can be made.244 These include the merchant-issuer model, the bank-issuer model, the

239 Cf discussion in Chapter 2, paragraph 2.2.4.1.2 above, and footnote 89.
241 FinCEN is the financial intelligence arm of the United States Department of Treasury. It is tasked with the regulation and control of financial crimes. See Financial Crimes Enforcement Network (2009: 2).
244 Kellerman (2004:3).
non-bank-issuer model and the peer-to-peer model. An understanding of these models of e-payment is crucial because they represent the different possibilities of payment systems on the internet. This is important to the study of cyberlaundering, due to the fact that the system of e-payment forms the bedrock for cyberlaundering. These models will be closely considered.

3.3.2.1. The merchant-issuer model

The merchant-issuer model of e-payment refers to a rather ambiguous scenario where both the issuer of a smart card, or pre-paid card, and the seller of goods are the same person. In other words, one is faced with the situation where the merchant, who sells the goods and services to whom payment would be made, is also the issuer of the services. The object that is traded here is often an electronic card. Some examples of companies of this kind are Barclaycard, Visa, the Oyster card used by the Transport of London, and the Creative Star card used by the Hong Kong transit system.245

This model does not pose a threat immediately on face value. However, the risks exist that it is used for illegal purposes, especially in the case of lesser known card companies. Merchants/issuers could be unscrupulous businessmen or organized crime syndicates that operate businesses online and use their enterprise as a façade for washing illegal funds. The ultimate goal is for these merchants to conceal their identities from law enforcement officers. A

245 Jamali (2009:14) and Reuter and Truman (2004:124). Countries in the Caribbean have often been the dumping ground for funds derived from criminal activities, as they are known to have very weak financial systems. It is only recently that the Financial Action Task Force removed several of those countries from its black list.
study has shown that a majority of these companies are registered in jurisdictions that hoard funds unscrupulously, such as Costa Rica, Curacao, Antigua and Cyprus.246

3.3.2.2. The bank-issuer model

The bank-issuer model is the direct opposite of the merchant-issuer model. In this case the merchant and the issuer of the electronic cards are two separate entities. This scenario is commonly seen in the traditional financial system, where a bank-customer relationship exists. The traditional financial system is used to clear transactions, and for this reason, it is a more secure model of electronic payment. Good examples are the Danmont card, used in Denmark, and the Banksys’ Proton card in Belgium.

3.3.2.3. The non-bank issuer model

In this case, the customer or user buys electronic cash from the issuers using, traditional money, after which he/she uses the electronic cash to conduct transactions online with participating merchants. These merchants would then redeem the traditional cash equivalent of the electronic cash from the original issuers.247 Traditional banking systems are not involved in the process, which raises curiosity about the legality of the transactions. This is not to say that this model is entirely smeared with illegality. The model could not be more tailored for cyberlaundering practices, for cyberlaunderers prey on avenues

---

247 Kellerman (2004:3).
that are completely detached from reporting and record-keeping regulations. Popular examples of the non-bank issuer model are the electronic coin product of Cybercash, the Virgin Card and the Freedom Eagle Card.

3.3.2.4. The peer-to-peer model

The peer-to-peer model features a scenario wherein bank and non-bank-issued electronic cash is transferable between users. This system is rather flexible, given that electronic cash is transferable between users without encumbrances. Thus, the only point of contact between the traditional payment system and electronic cash is when the electronic cash is initially purchased from the issuer and when it is later redeemed from merchants and individuals. Therefore, as with the physical activity of handing over cash directly to another, electronic cash could be transferred directly from one person to another, either with or without the use of traditional banking systems. The MONDEX stored value card is a good example of the peer-to-peer system. Also, an electronic barter trader such as E-gold Ltd is a very good example.

---

249 The Virgin pre-paid cards are especially popular in the USA, South Africa, the UK and other parts of Europe. For more information, see Virgin Cards (an undated website document) ‘About us’ available at <http://www.virgin.co.uk/pre-paidcards> and Freedom Eagle Card (an undated website document) ‘About’ available at <http://www.freedomeagle.com> [both accessed on 19 June 2011].
252 See paragraph 3.5.4 below.
The peer-to-peer model has the characteristic of defying jurisdictional borders, which portends many dangers for the traceability of funds, especially for law enforcers. Hence, when illegal funds are transferred from one user to another, in another country or jurisdiction, the transaction would reflect that it originates from another person - the sender or original user - and not the issuing company, merchant or bank, if issued originally by one.\textsuperscript{253}

Clearly, the peer-to-peer model of e-payment creates infinite latitude amongst individuals, with minimal oversight by issuers and merchants. This holds dire consequences that are far-reaching, for the risk inheres in the fact that very complex trails can be created by criminals with illegal funds who seek to transfer e-money, at different times, to several accomplices or co-perpetrators. This possibility is considered further in this study.\textsuperscript{254}

3.3.3 Storing methods and examples of electronic money

Other than the overarching models of e-payment discussed above, which are largely broad in nature, the ensuing discussion delves into narrower examples of different forms of e-money, and the several ways in which it can be stored.

3.3.3.1 ‘Software money’

‘Software money’ is a system through which software is stored in a computer hard drive by means of a proprietary software system.\textsuperscript{255} This program creates

\begin{itemize}
\item See Reuter and Truman (2004:125).
\item See paragraph 3.5 below.
\end{itemize}
an electronic wallet, also known as e-wallet, which can be loaded with money from an existing bank account. With this e-wallet, the user can purchase goods and services from merchants and vendors. However, this transaction is encrypted and the identity of the user would be unknown to the merchant.256 A good example of a company that provides such software is E-cash.257

3.3.3.2 ‘Real time or prepaid tokens’

Real time or prepaid tokens refers to the use of prepaid instruments to conclude transactions. Prepaid tokens usually take the form of cards such as smart cards, debit cards, e-wallets,258 and gift cards issued by most department stores. These cards are quite secure, given that they have well-encrypted microchips, and monetary value can be stored on them. This is very convenient, especially for banks that issue debit cards or banks cards. Virtually every bank with a competitive edge today issues debit cards to its customers, enabling them to conclude transactions. Customers could easily swipe the card on a teller machine, or could merely type in an encrypted code of the card online. Given the convoluted nature of smart cards and their distinct dynamism, the concept will be considered more closely.

As examples of a real time or prepaid token, smart cards are very pertinent to the study of cyberlaundering. The service provider of a smart card, also

258 In spite of the discussion in the preceding paragraph, e-wallet can also be considered as a prepaid token because it has the feature of a prepaid instrument, even though it is created by a software programme.
known as the issuer, operates the networks on which the cards can be used. There is also a prepaid account that is established by the issuer which is linked to the value of the smart card, similar to the nature of debit or credit cards.259 Smart cards are generally divided into open-loop or closed-loop cards.260 Closed-loop cards are limited in nature, and their uses are very specific. A smart card can, for example be, for example, limited to a pre-determined value without the possibility of reloading it. Smart cards exist that enable the card holder to add value to the card to a certain limit, and there are smart cards that can be reused or reloaded by the card holder.261 Examples of the closed-loop smart cards are gift cards, long distance service and transmit system cards.262

Open-loop smart cards, on the other hand, are more diversified, with a wider range of purposes, and have the key characteristic of being multi-jurisdictional. By reason of the fact that their use transcends local borders, they appeal more to international clients with large scale businesses. Also, open-loop smart cards can be used by multiple parties, and not just a single party. These cards are often linked to e-payment merchants such as MasterCard or Visa, which facilitate use on an automated teller machine (ATM). Good examples are payroll cards and cash cards which are meant for

persons without bank accounts and are often reloadable.263 Such extraordinary capabilities render the open-loop smart cards more susceptible to use by money launderers.

Transactions on the internet today are better effected with smart cards, which are often the preferred avenues for internet service providers (ISPs). Smart cards can be quite simple to use, given the easiness with which the credit card can be credited with funds. The card could simultaneously be used as a debit or credit card, depending on the purpose the user has in mind.264 The fact that smart cards are generally tarnished by being prone to misuse for money laundering purposes undermines their benefits, chief of which is the convenience that they offer, considering the unease and unwieldiness accompanying the physical carrying of bulk cash.265

In the year 2009, it was reported that about US $120 billion was loaded onto smart cards, and this number is expected to surpass US $440 billion by the year 2015.266 Smart cards carry a great risk of danger because of the way in which money is transferred onto them. Funds could be transferred easily onto a smart card

---

265 A smart card certainly has numerous advantages, as it does not merely create convenience for individuals personally, but for governments and institutions as well. Recently, the Pakistani government partnered with a bank to distribute smart cards with a value up to about 25,000 Pakistani rupees to its citizens. At the same time the bank and the smart card company set up wireless point of sale terminals where people can buy basic supplies. This initiative comes as result of the fact that most Pakistanis are without bank accounts, making it impossible to make payments directly into any bank account. Financial Action Task Force (2010D: 13). Cf Visa Corporate Site (2010) ‘Financial Inclusion - Pakistan eases the burden of displaced citizens by delivering financial support through “Visa,”’ available at <http://www.currency ofprogress.com/__ media/pdfs/case_studies/VISA_Inclusion-Pakistan.pdf> [accessed October 2010].
266 Payment News (2010: 23).
by several means. For example, this could be done via a telephone, or either from an e-wallet\(^{267}\) or an ATM machine, or from the hard drive of one’s computer, or online from one’s bank account, or, more generally, from cyberspace (the legitimacy of which is always questionable).\(^{268}\)

Also, smart cards are problematic because majority of them do not presently require transactions to be reported to a central computing system. A good example is the MONDEX card, which is part of MasterCard International.\(^{269}\)

What is more, some of these cards do not even require one to have a bank account, as is the case with the PayPal card, and persons with false identities can be in possession of them effortlessly. This is a crucial trait of the cyberlaundering phenomenon, for the evasion of reporting requirements remains a recurring theme within the study of money laundering.\(^{270}\)

Cyberlaunderers exploit prepaid tokens because of the very high possibility of circumventing the Know Your Customer (‘KYC’) procedures\(^{271}\) – the very heartbeat of the current anti-money laundering (AML) regime. Most ISPs are very unscrupulous and inapt about verifying the identity of their customers.

For example, the United Kingdom-based Freedom Eagle Cash Card, amongst


\(^{268}\) This is usually the case with the occurrence of identity theft, where criminals acquire monetary value by stealing another person’s details, like a credit card or account number. This is called identity theft.


\(^{270}\) This was noted by Stanley Morris (the director of FinCEN) in his 1995 address to the Congress Banking Committee, available at <http://www.fincen.org/resource> [accessed on 17 June 2011].

\(^{271}\) The Know Your Customer principle was first introduced in section 100 of the Bank Secrecy Act (1970), PubL 91-508; 841114. The principle mandates financial institutions and the like to undergo a thorough vetting process for prospective customers before transacting with them. See Chapter 2, paragraph 1.2.2 for greater details.
a slew of others, does not require any kind of identification from potential customers. This card can be purchased online easily within minutes, and can be recharged repeatedly, with no actual limit on the value stored on the card.\textsuperscript{272} This method of e-payment is wholly unfettered, and this raises the bar for potentially curbing the dilemma of cyberlaundering.\textsuperscript{273}

### 3.3.3.3 Electronic cheques

Electronic cheques, also known as e-cheques, occupy a separate category of the unique form that e-money can take. An e-cheque is no different from a paper cheque, because it serves as a message to a bank to make payment to a third party. The only exception is that it assumes a technological format, with sophisticated protection measures. The account number on an e-cheque is usually encrypted, and its digital signature and digital certificate are used to validate the payer, the payer's bank, and the account.\textsuperscript{274} This makes it more advantageous than conventional cheques.

E-cheques can carry illicit funds, which a cyberlaunderer would use to transact over the internet. However, the threat is analogous to prepaid tokens, such as smart cards, given the fact that they are considered to be safe security measures.

\begin{itemize}
  \item \textsuperscript{272} Freedom Eagle Cash Card available at <http://www.freedom-card.co.uk/> [accessed on 2 September 2010].
\end{itemize}
3.3.3.4 Alternative methods: the e-barter system

Other than software money, prepaid tokens and electronic cheques, payment can be made electronically using other methods. Online barter trade, in which commodities are traded for other commodities or cash, is a good example. For instance, the trade in electronic metals such as e-gold has been the trend for a while now.

E-gold is a digital electronic currency that operates in the World Wide Web. It is operated by the Gold and Silver Corporation, under the name e-gold Ltd.\(^{275}\) E-gold is account-based. As a traditional gold barter trade, specified weights of gold can be traded with another e-gold account holder, and ownership is exchanged.\(^{276}\) Because this suits international transactions, its operations are aided by the borderless nature of the internet. E-gold Ltd also purports to trade other e-metals such as e-silver, e-palladium and e-platinum.\(^{277}\) However, e-gold Ltd is plagued by illegality, having encountered legal woes since its inception because of its strong money laundering capabilities.\(^{278}\)

As in the case of e-gold, several other alternative e-payments methods have been developed to rival the afore-mentioned examples of e-payments systems. They claim to have much tighter in-built security measures for fending off fraudsters, thus making them attractive to both merchants and

---


\(^{278}\) This is discussed extensively in Chapter 6, paragraph 6.5.1.
customers. An example is Bitcoin, which was created in 2009. Bitcoin is a virtual or digital currency which uses the peer-to-peer system, and given the nature of peer-to-peer transactions, there is no central authority that issues new money or tracks transactions. However, Bitcoin has attracted much criticism, such as that it is susceptible to hackers and money launderers.

Another criticism is that Bitcoin is plentifully available, which robs it of its intrinsic value – a feature of any true currency.

### 3.4 CYBERLAUNDERING AND THE THREE-PRONGED PROCESS

This aspect is reminiscent of a very crucial characteristic of money laundering, namely the triadic cycle of placement, layering and integration. Given the fact that money laundering is a process crime, these standard stages help to explain the flow, the process and the workings of the crime. Cyberlaundering also embodies this process, with each stage having a technological ambit to it. Although money laundering on the internet is an entirely different playing field than that of its terrestrial analogue, the rationale remains unchanged. The fact remains that illegal funds are made to

---


282 See Chapter 2, paragraph 2.2.3. The three stages of money laundering are always described extensively in almost every discussion on money laundering. The following are some examples of works that provide such detailed discussions: Reuter and Truman (2004: 43), Madinger and Zalopan (1999: 54), Filipkowski (2008: 45) and Ping (2004: 43).
wend their way through all kinds of nooks and crannies, making them almost impossible to trace, let alone recognise. However, it should be added that the three-phased process is not cast in stone, as some phases can be made to overlap, resulting in less complex processes. But, the process is crucial as it helps one to understand the underlying intricacies better. The ensuing section looks at how the three-phased process manifests itself in the cyberworld, which is the realm of cyberlaundering.

3.4.1 Placement

In the world of cyberlaundering, placement occurs when e-money, having the label of illegal funds, is used to purchase goods and services with the intention to clean or convert it into ‘clean money.’ This is one of the many wonders of e-money, which has very adverse effects in the commercial world: Its virtue lies in the fact that it alleviates the need to ‘carry’ cash money physically. It also renders face-to-face transactions superfluous.\(^{283}\) Thus, e-money can be exchanged from one person to another, or between multiple parties, without the involvement of any intermediary. This is further made possible because transactions involving the use of e-money are shrouded in anonymity, on which cyberlaundering thrives.

Method wise, illegal e-money can be ‘placed’ in various ways, many which would involve online transactions. For instance, illegal e-money can be used to purchase foreign currency for the purpose of re-selling it, as shares in the

stock-exchange, or it can be invested in a totally legitimate business enterprise.\textsuperscript{284} Online gaming, particularly online casinos, can also be used to place the funds. This is done by buying gambling chips on the casino, using illegal e-money.\textsuperscript{285} A win results in the casino paying out the winnings in cash, thus legitimizing the illegal e-money. Also, online barter trade that involves several businesses such as e-gold is also a very lucrative platform for placement. E-gold, for example, has been largely labelled as such.\textsuperscript{286} Other methods of placement include transfers of values stored in one’s hard-drive or email account, or transfers done from an ATM, or sometimes, simply, telephonically.\textsuperscript{287}

The placement stage is probably the simplest of the three stages. Where the goods or services purchased are consumables, the buck often stops here. This often means that there is no need to proceed to the stages of layering or integration. However, for cyberlaundering on a more complicated level, the placement stage is only the beginning.

\textbf{3.4.2 Layering}

The layering stage of cyberlaundering is the attempt at an ultimate disguise, as the intention of the cyberlaunderer comes to bear. Here, the criminal tries to mastermind the most complex of plans, schemes and designs to whisk the

\begin{itemize}
\item \textsuperscript{285} See paragraph 3.5.4. below for a full discussion on this.
\item \textsuperscript{286} See the full discussion on E-gold Ltd in paragraph 3.5.4. below.
\item \textsuperscript{287} The process could be as simple as an existing customer of an electronic card company calling the company to credit an already exhausted smart card, or to give an order to transfer some value from an electronic card with illegal money to another person’s account.
\end{itemize}
illegal funds as far away as possible from the source of the criminal activities. Simply put, this stage usually entails a very difficult maze that the criminal devises and negotiates with the illegal funds. The inherent possibilities are indeed endless.

The process entails a separation of the illegal funds from their true origin and then dispersed or ‘layered’ through different avenues. Amongst existing possibilities is the use of several online shell companies\textsuperscript{288} to transfer the funds, or simply purchasing goods online for purposes of resale, or by paying company or income taxes on the funds.\textsuperscript{289} Other than these, online banking has proven to be the main tool for the purposes for layering funds. As discussed further below, online banking is a very effective layering mechanism because an internet bank account can be opened without a face-to-face contact and an existing link to a traditional bank account. Thus, online banks with very poor vetting processes run the risk of serving cyberlaunderers who exploit their ineffective system to perform endless layering transactions. A cyberlaunderer is able to open different bank accounts online with a false identity and transfer funds amid several jurisdictions without creating audit trails. The use of electronic funds transfers (EFTs) also comes in handy at this stage for the cyberlaunderer, as is

\textsuperscript{288} See Chapter 2, paragraph 2.2.4.6 for discussion. An online shell company serves as a vehicle for business transactions, without itself having any significant asset or operation. It is usually set up to aid the layering of funds, and has several key features, such as being registered in very unscrupulous jurisdictions and having an existing bank account that facilitates the movement of funds. See Reuter and Truman (2004: 33).

\textsuperscript{289} Philipsohn (2002: 4).
a complementary feature or consequence of online banking.\textsuperscript{290} The mix of e-money and online banking forms a powerful combination for cyberlaundering, especially in the internet environment where anonymity and boundless jurisdiction are key features. The numerous possibilities for cyberlaunderers that exist at this stage are seen further in the discussion on the vulnerable industries and techniques for cyberlaundering.\textsuperscript{291}

\textbf{3.4.3 Integration}

The integration stage of cyberlaundering comes as a result of the need to create an appearance of legitimacy to the outside world. This stage is distinguishable from the layering stage because of the underlying rationale behind it. At the layering stage the key intention is to create a web of complexities in order to evade traceability from regulatory authorities, whereas at the integration stage, the cyberlaunderer intends to feign legitimacy of the funds. The latter can be accomplished by integrating the funds into the broad commercial market. There are several plausible avenues through which this can be achieved. While, in the traditional sense, this can be accomplished by creating fake invoices for goods and services, in the case of cyberlaundering, illegal funds can be reintegrated into the commercial world by opening online shell companies that render ostensible services of different kinds. Online shell companies are not only relevant to the layering stage, as indicated above, but, also, they play a key role in the integration of

\textsuperscript{290} Jamali (2009: 14).

\textsuperscript{291} See paragraph 3.5 below.
funds, especially when these companies have been created for legitimate purposes. Thus, using an existing bank account created in the name of the company, the illegal funds can be commingled with legitimate funds, thus creating the impression that the flow of illegal funds is geared towards fulfilling a legitimate purpose. Furthermore, it does not help that majority of these online shell companies are registered in very porous jurisdictions having very weak financial regulations.\textsuperscript{292} Online gaming companies such as online casinos exhibit such traits.\textsuperscript{293} Such companies try to keep within the confines of their ‘legitimate businesses’ in order to prevent raising the eyebrows of regulatory authorities. After all, the overall purpose of integration is established when there is lack of adequate oversight by such authorities.

### 3.5 VULNERABLE INDUSTRIES AND TECHNIQUES OF CYBERLAUNDERING

Cyberlaundering thrives in very peculiar environments on the internet. This aspect delves into the nitty-gritty of cyberlaundering operations, identifying the most infested industries and most common techniques available on the internet that perpetuate the operations of cyberlaundering. The tides are rising more than ever before, as various industries are increasingly being exploited, such as online banking, online gaming, online auctioneering and online barter trade. It is a very prominent trait of money launderers to exploit perfectly legitimate commercial industries for laundering purposes, thereby tainting


\textsuperscript{293} Filipkowski (2008: 6).
such industries as a result. The ensuing discussion identifies some of these industries and unravels some of the techniques being currently used for the purposes of cyberlaundering.

3.5.1 Online banking

Online banking refers to the use of an internet-based bank to perform regular banking activities such as account inquiries, payment of bills and transfer of funds. With the advent of online banking, customers enjoy a new level of convenience, because customers can conclude certain basic banking transactions without being physically present at the bank. This, again, is one of the many good fruits that the internet yields. With the growth and dominance of the internet, the world has become a cyber-hub and a truly global village. This is further evidenced by recent statistics showing that 97.7% of all the banks in the world today, regardless of their location, have become internet-based.294

Online banking has become the most dominant technique of cyberlaundering.295 It facilitates cyberlaundering operations for the following reasons:

(i.) Cash held by most internet-based banks (electronic cash or e-cash) does not fall within the ambit of hard cash, which is subject to regulation and control. For instance, in the United States, most banks are insured under

the Federal Deposit Insurance Corporation (FDIC),\textsuperscript{296} which guarantees the safety of deposits in member banks. However, given that e-cash is often created by private vendors, rather than the Federal Reserve Bank, it is unaffected by monetary supply or policy as it does not form part of the market place of hard currency. This makes it difficult, and virtually impossible, to apply for e-cash the regulatory measures prescribed in laws such as the Money Laundering Control Act of 1986\textsuperscript{297}. Hence, the highly revered KYC principle, which requires terrestrial banks to report suspicious transactions to law enforcement agencies, cannot be applied directly to online banks.\textsuperscript{298} Needless to say, those online banks that fall outside the ambit of current banking regulations have no obligation to file currency transaction reports (CTRs);

(ii.) Also, opening an account at an online bank can be done with the greatest of ease and convenience, without any substantial vetting process conducted by the relevant bank. The identity of the potential customer is not verified, neither is it authenticated. At terrestrial banks, there is a face-to-face encounter at the bank, where potential customers are required to present identification documents, which are verified before opening an account at a bank. This is not so with online banks.

\textsuperscript{296} The FDIC was created by the Banking Act of 1933 (\textit{Public Law Number: 73-66}). The Act is generally known as the Glass-Steagall Act, after its legislative sponsors, Senator Carter Glass and Senator Henry B. Steagall. The Act introduced major banking reforms in the United States, which include a differentiation in the activities of commercial banks and investment banks. The FDIC currently guarantees the safety of deposits by individual depositors to the tune of $250,000. See Federal Deposit Insurance Corporation (2012) ‘Frequently Asked Questions About the FDIC’ available at <http://www.fdic.gov/about/affaq.html> [accessed on 02 September 2011].

\textsuperscript{297} Act 18 of 1986. See paragraph 2.2.2.2, Chapter 2, for more detailed discussion.

The marketing strategy of most online banks is designed to allow anyone to open an account, regardless of where the person is located. Hence, whatever information is provided for the opening of an account is the only evidence seen by the bank, and the true identity of the criminal seated at the other end of the computer remains unknown;

(iii.) Another advantage of online banking for cyberlaundering is the fact that it perpetuates layering. Layering can be achieved easily, especially where a criminal uses smurfs to disperse illicit proceeds into several of his/her accounts held at an online bank.299 Another factor to consider is that online banks are not registered at the place where deposits are made, and this rules out the possibility of direct regulation. Along with the common problem that smurfs operate under the monetary limit or stipulated threshold, which negates the need for online banks to file a CTR, it is extremely difficult to identify the activity of smurfing or structuring, especially in such an illusive environment as the internet. Most governments/agencies have to rely on bank employees to blow the whistle on suspicious activities. An important issue that intertwines with this is the right to privacy, which, in this case, includes the right to unauthorized interception of electronic communications, and which

begs the question: To what extent are law enforcement agencies allowed to ferret out crime because of a hunch or suspicion? As a complementary tool, smart cards come in handy for layering illicit funds over the internet. With smart cards, especially the open-looped types, the possibilities of layering are indeed endless. It is the perfect tool with which a web of deception is created, and not a single trail is left;

(iv.) As with other cyberlaundering techniques, the issue of jurisdiction further compounds the vulnerability of online banking for cyberlaundering purposes. An online bank is not always registered at a place that falls within the limits of any international standard regulating it. It is unclear which country would have jurisdiction if the website of an online bank is registered in a place different from where the customer operates, since such international norm is lacking, and the reporting standards adopted by conventional banks are not mandatory. To compound the situation, most countries still refuse to cooperate with one another in sharing intelligence on such issues; and

(v.) Furthermore, with the spiralling growth of identity theft on the internet, cyberlaundering through online banking is aided, as a consequence. Hackers are using very complex encryption methods that

---

300 The issue of privacy is a very sensitive one, as it affects the fundamental right of the person as well as the public interest, and the interests of justice. Cf detailed discussion on the right to privacy in Chapter 6, paragraph 6.2.2.


302 The question of jurisdiction is one of the many grey aspects of cyberlaundering, which this thesis attempts to answer. This is discussed thoroughly in Chapter 6 below, paragraph 6.4.
make online banking permeable to their devices. Without leaving a single shred of evidence, hackers can encrypt certain programs to transfer funds electronically from one bank account to another.\textsuperscript{303} Hackers also have special software that can be used to retrieve or steal an individual’s personal data, such as bank details and credit card numbers, which could be useful to a cyberlaunderer when conducting certain banking operations online.\textsuperscript{304} The trend currently leans towards purchasing fake identities from hackers, which are then used to open a bank account online. Within this web of complexity, the placement and layering stages of cyberlaundering are well secured.\textsuperscript{305}

\subsection*{3.5.1.1 Example of cyberlaundering through online banking}

The following presents a hypothetical scenario of how online banking is exploited for cyberlaundering purposes:

Jack Sparrow is a jobless man who is very conversant with the internet. He constantly browses job websites like www.findjobs.com and www.jobfinder.co.uk in search of job opportunities. John Doe, on the other hand, is a fraudster, who runs a fake charity organisation on the internet called Aid-For-All www.aidforall.com (a shell company). Amongst several of the other illegal activities operated by John Doe, this is the most lucrative. John Doe opened a bank account at an online bank (B Bank) for this organisation in its name. As John Doe constantly

\begin{flushright}
\textsuperscript{303} Marshall, Robinson and Kwak (2005:115).
\textsuperscript{305} Jamali (2009:18). Cf Pillai and Juian (2008: 14). Another method by way of which one’s identity can be stolen online is through the use of spoof websites. These websites make certain attractive offers to the visitors on the condition that they provide them with certain personal details. See Atta-Asamoah (2009:109).
\end{flushright}
scours jobsites on the internet looking for gullible accomplices, he crosses paths with Jack Sparrow, who, agrees to help John Doe wash the proceeds of his illegal activities. The aim is to siphon these funds into the mainstream commercial sector. John Doe deposits a portion of the illicit funds into his savings account in B Bank (i.e. placement). Jack Sparrow then loads several smart cards and gift cards with the remaining funds, albeit at different times, in order to evade suspicion. Jack Sparrow employs another party, Sally Shore, and they both make deposits under different identities and in the form of a donation to the bank account of the charity organisation (i.e. layering). Jack Sparrow and Sally Shore both perform these operations online at B Bank. Note: John Doe could accomplish his aims quicker and in a more elusive manner by employing several other smurfs along with Jack Sparrow and Sally Shore. Alternatively, and even more simply, John Doe could do without anyone’s assistance by buying the stolen personal data of individuals from a hacker, and in place of a smurf, use their details in the guise that “they” are the donators to his charity organisation.

3.5.2 Online auctioneering

Albeit unknown to many, online auctioneering is a booming industry on the internet, not just for legitimate merchants, but criminals as well.\footnote{This is due to the large number of users of auction websites per month. They are now estimated at 16 million, and as a result of the concomitant side effects, 87% of fraud cases are believed to be related to auction websites. As far back as 1987, when the internet was still in infancy, consumer complaints of online auction websites being used as tools for fraud was estimated at 1280 per anum. This rose to an unsettling estimate of 10660 per anum in 1999. Today, the complaints are innumerable. Newman and Clarke (2003: 15). Cf Haney (2001: 26) and Messner (2000: 4).} Cyberlaunderers, in particular, find this avenue convenient for ‘washing’ dirty funds. An online auction website enables persons that are registered on
it to put up items or articles on the website for sale. Other users of the same website can bid for any item of choice. Just as one would find in auctions generally, the item, which is the subject of the sale, is sold to the person with the highest bid. Thereafter, the buyer would pay the agreed price to the bank account of the company, whilst, sometimes simultaneously, the seller sends the item to the buyer directly. Afterwards, behind the scenes, the company would pay the seller of the item and charge its own commission, if, according to the terms of sale, the buyer finds the product acceptable as advertised.\textsuperscript{307}

Given that online auctioneering companies are legitimate ones, in most instances, online auctioneering is often not considered a high-risk industry for a criminal enterprise. But the loophole is in the bidding process. A criminal could exploit this avenue by employing a smurf who could keep bidding continuously in high amounts until the item is sold to him or her, because in an auction sale without reserve, there is no limit to the bid made by a buyer.\textsuperscript{308}

3.5.2.1 Example of cyberlaundering through online auctioneering

The following serves as an example of how online auctioneering is used in practice for purposes of cyberlaundering:

Jack Sparrow is a drug dealer living in Turkey. He would like to convert the funds he has acquired from crime to legitimize his wealth. Jack Sparrow is registered on the auction site called Auction Express (www.AuctionExpress.com). In cahoots with

\textsuperscript{307} Filipkowski (2008:9).
Sally Shore - a smurf living in Cambodia, who is also registered on Auction Express - they agree to put up a very valuable relic for sale on Auction Express on a specific day and time. Jack Sparrow purchases a smart card, which he loads with the illegal funds. He sends the encryptions of the smart card to Sally Shore via email. She decrypts it and extracts the value in the smart card. At the time agreed, the relic is put up on the auction site. Sally Shore bids the highest for the relic, and it is sold to her. Thereafter, Sally Shores pays the money into the bank account of Auction Express, and, at the same time, Jack Sparrow sends the painting to Sally Shore. After this, the necessary verifications are made and the money is paid to Jack Sparrow. At this stage the money has been integrated fully into the commercial world, as it has been ‘cleaned.’ Note: Jack Sparrow could do this activity in multiple sequences, and several smurfs can be used for different items to further create the veneer of legitimacy.

3.5.3 Online gambling

Gambling is one of the few industries that have been transposed onto the internet successfully. Online gambling is a large part of the billion-dollar online gaming industry. By definition, online gambling refers to “the provision of opportunities to play games of chance or to obtain access to sports or race bookmaking via computer networks.” Statistics show that online gambling is fast becoming as buoyant as terrestrial casinos, if not

---

309 As at 2010, online gaming was estimated as having a world-wide worth of US$20 billion, with future estimations showing an increase to US$30 billion by 2012, and with online gambling constituting more than half of the gross. KPMG (2010: 4).
more.\footnote{In the period 1999 to 2001, the revenue derived from online gambling spiked from $651 million in 1999 to $2238 million in 2001 (See NUA (an undated website document) ‘Surveys’ available at http://www.nua.org> [accessed on 3 September 2011]). In Europe, Italy has the biggest online gambling market, which grew from €3.4 billion in 2009 to €4.8 billion in 2010. In Greece, also, online gambling rakes in an estimated €2 billion annually, and the government is currently considering taxing the industry and regulating it, considering that its annual revenue can go a long way in helping its crumbling economy. Despite the dwindling economies of these countries, this industry still thrives, and was unaffected by the recent recession that plagued several countries in Europe. See Online Poker News (an undated website document) ‘Italian Online Gambling worth €4.8 billion’ available at <http://www.onlinepoker.net/poker-news/poker-law-industry-news/italian-online-gambling-worth-48bn-rising-legislation/9394> [accessed on 3 September 2011]. See also Streak Gambling (an undated website document) ‘Online Gambling worth 2bn in Europe’ available at <http://www.streakgaming.com/forum/online-gambling–worth-2-billion-greece-t22194.html> [accessed on 3 September 2011].} It is common knowledge that terrestrial casinos are often warehouses for money laundering activities.

When judged side by side, online casinos are hardly different from terrestrial casinos. However, a very glaring fact is that online casinos are way more addictive, because one in every five persons that visits online gambling sites is deemed to be a pathological gambler, as compared to the same ratio of persons who visit terrestrial casinos.\footnote{Times (an undated website document) ‘Online Gambling’ available at <http://www.timesonline.co.uk/tol/news/politics/article620834.ece> [accessed on 21 July 2011]. Cf discussion in Schopper (2002: 309).} Several factors attest to this: First, just as with other activities performed on the internet, it is much more convenient to use online gambling than terrestrial casinos. One can gamble online from the comfort of one’s home, or from virtually anywhere, as long as one has access to the internet. Also, online gambling sites offer very attractive incentives that are very enticing, such as gambling for free for a stipulated number of minutes or hours, and, or, at very low rates. This is hardly the case with terrestrial casinos. Given the nature of competition on the internet,
where there are thousands of online gambling sites that sprout up every day, such incentives are a marketing strategy.\(^{313}\)

One may ask: How has online gambling become lucrative for purposes of cyberlaundering? Cyberlaundering can be accomplished through online gambling in two ways: A criminal could either use an existing online gambling service, which might appear legitimate, or set up one for the sole purpose of cleaning his/her ‘dirty’ funds.\(^{314}\) The latter would be a riskier method for the criminal, given that the existing online gambling website he/she seeks to exploit might or might not have strict internal regulations, laws and general oversight of the gambling activities. Also, with this method, the criminal would not have actual control over the gaming activities, and would stand a real chance of either winning or losing.\(^{315}\)

On the other hand, the former scenario, which involves establishing an online gambling site solely for the purpose of fostering a money laundering enterprise, appears more plausible for criminals. This method can be putative in nature, as it guarantees the criminal total control and, in most cases, a certain degree of anonymity. The very danger of online gambling inheres in this form. The following points explain this further:

\(^{313}\) In 2009, the number of online gambling sites was estimated at around 1800. This number was predicted to triple in the coming years. See The United States Government Accounting Office (2009: 1). Cf Financial Action Task Force (2009B: 2).

\(^{314}\) Bumeter (2001:2). Cf Schopper (2002: 310). A third form of online gambling, called live-based gambling, exists. It enables more interaction between players or participants in the gambling activity. However, it is not very significant for the purposes of this study, as compared to the other two forms.

\(^{315}\) With this option, however, a cyberlaunderer need not even play or engage in actual wagering activities, given the possibility that funds could be merely ‘dumped’ into one’s account at a casino, which could be recorded as ‘winnings’ and which, thereafter, could be moved to another account, without the fear that the casino might be monitoring the activities in question. Cf Gottfried (2004: 26).
(i.) Where a criminal creates an online gambling site solely for the purpose of laundering money, the most logical thing to do is to employ an army of smurfs to foster this objective. The illegal funds could be distributed among these smurfs to gamble on the site. It is immaterial whether the smurfs win or lose, for, in any case, it is the criminal who wins, simply because the proceeds will revert to him. This system is commonly known as “the drumming up business scenario.”

(ii.) Also, it is easy to set up an online gambling website. This can be attributed to the boundless boundaries and jurisdictional freedom of the internet, which are the main pillars supporting any online gambling enterprise. The method of online gambling for laundering money represents one of the negatives aspects of having a world of boundless boundaries on the internet. This feature of the internet makes the regulation and control of online gambling sites almost impossible. Especially where the laws of the relevant country permit online gambling, establishing an online gambling site is a hassle-free task for criminals. The regulation of online gambling remains a common problem amongst countries. At present, internet gambling is a legal activity in many countries. In very few countries, such as India.

---

317 This includes most countries in Europe, the Caribbean and North America. See KPMG International (2010: 23). In Africa, only South Africa has express provisions legalizing internet gambling, although these are subject to certain regulations under the National Gambling Act 7 of 2004.
318 The Bombay Wager Act IV of 1887 (Part 1).
and some parts of the United States (US), online gambling is illegal.\textsuperscript{319} In the US, whereas online gambling is not \textit{per se} deemed illegal in terms of federal law, the electronic transmission of betting and wagering activities is illegal in terms of The Wire Act of 1961; and\textsuperscript{320} (iii.) The feature of anonymity also rears its head within this discussion. As is typical with all money launderers, a person who devises an enterprise such as online gambling, for purposes of laundering money, seeks to cover his tracks and evade being traced. Luckily, the internet provides this feature, and an online gambling site can be created under such veil of anonymity. This can be amply possible if the criminal avoids the registration of his internet provider (IP) address. In countries or jurisdictions with very lax internet control policies or AML laws, this is often the case.

Moreover, the smurfs who are used by the criminal to play on the online gambling site can also enjoy anonymity. Even where the first scenario applies – where a legitimate online gambling site is exploited by a criminal – the principle still holds and the identity of the smurfs would not be determined. This is attributable to the fact that online gambling sites are not financial institutions; they are not required to

\begin{flushleft}
\textsuperscript{319} Some states in the US such as Illinois, Indiana, Louisiana, Montana, Nevada, Oregon, South Dakota, and Washington have strong laws against online gambling. Bluejay (2012: 1).
\end{flushleft}

\begin{flushleft}
\textsuperscript{320} The Federal Wire Act 87 of 1961 (popularly called ‘The Wire Act’). In the US, in a recent case of \textit{United States of America v. Scheinberg} et al 10 Cr. 336 (2011) three online poker companies were indicted for circumventing US laws that prohibit the operations of unlicensed online gambling websites that accept illegal funds for the purposes of gambling online. The rationale was reemphasized that the electronic transmission of betting and wagering activities is illegal under the laws of the Wire Act.
\end{flushleft}
observe customer verification (i.e. the KYC principle), neither are they under a similar obligation to report suspicious activities to law enforcement bodies.321

3.5.3.1 Example of cyberlaundering through online gambling

Below is an example of cyberlaundering through the method of online gambling, and, in particular, using the ‘drumming up business scenario:’

Jack Sparrow is a fraudster residing in New York City, US. He has US$1 million in criminal proceeds, which he wishes to launder. Jack Sparrow, therefore, opens an online casino (‘Caesar’s Casino’) in Pakistan through an acquaintance, John Doe, who is resident in Pakistan. Jack Sparrow intends to use John Doe and his friends as smurfs to ‘wash’ his ‘dirty’ funds for him. For this reason, Jack Sparrow obtains their e-mail addresses, and purchases several smart cards which he loads with varying amounts of the illegal funds. He then sends the details of these cards to the smurfs in Pakistan with encrypted software, along with their individual commissions on the encrypted cards. With the decrypted smart cards, the smurfs open an account at Caesar’s Casino. The smurfs then use the cards to gamble, but deliberately lose all the funds to the casino. These losses form part of the casino’s income, which reverts to Jack Sparrow (the owner of the casino) in monthly instalments. Alternatively, if John Doe is by chance the manager of the casino, he remits the money to Jack Sparrow.

Conversely, should it happen that the smurfs win at Caesar’s Casino, they then acquire the funds, which they send directly to Jack Sparrow in monthly instalments, or pay back to Caesar’s

Casino as a donation or as payment for a putative service rendered.

Note: This arrangement might well represent only one of numerous other possibilities, for Jack Sparrow could make similar arrangements with smurfs in various other countries simultaneously.

### 3.5.4. Online barter trade

According to the FATF, the reason for the advent of new e-payment systems, such as e-barter trading or digital payment systems is that it helps with certain key transactions on the internet, without reverting to traditional currencies, or having foreign exchange concerns. Although there are several e-barter trading companies such as WebMoney, Netpay and GoldMoney, this study will look more closely at E-gold Ltd and its operations as an example of e-barter trade, given that it is the only online e-barter trading company that has been most plagued with money laundering allegations amongst a slew of other criminal allegations. This is considered below in greater depth.

E-gold is an electronic currency created solely for the internet. It is issued by E-gold Ltd, and is backed 100% by gold bullion in allocated storage. One peculiarity of e-gold is that it is entirely unrelated to traditional currencies, such as the Dollar, the Euro, the Yen, the Rand etc. The system is account-based, which implies that only account holders can conclude transactions.

---

323 The resulting case of United States of America v. E-Gold Ltd, Douglas Jackson, Barry K. Downey, and Reid A. Jackson, 521 F.3d 411, 417 (D.C. Circuit) (2008), is discussed in detail in Chapter 6 below at paragraph 6.5.1.
with the e-gold currency by spending specified weights of gold of the e-gold currency with other account holders.\textsuperscript{325} It is a prerequisite, therefore, that e-gold trading is kept within the circle of account holders, and as a consequence of any barter trade, only ownership is exchanged. The holder or recipient of an e-gold currency could do whatever they want with the currency – it could be traded further with other persons or merchants accepting the currency, or it could be converted to cash.\textsuperscript{326} E-gold Ltd makes profits by charging a percentage of fees on each transaction conducted. In the 2005 fiscal year alone, transactions worth $1.5 billion were reported to have been conducted.\textsuperscript{327}

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.\textsuperscript{328}

This method of e-barter trade lends itself to be used to complete the full money laundering circle - placement, layering and integration. Also, e-gold

\textsuperscript{326} There are several ways in which e-gold can be converted to traditional cash. One can load a debit card with e-gold and cash it out at an ATM. However, the debit card must be anonymous in order not to leave a trail. Most anonymous debit cards do not require any form of identification and social security numbers, such as Cash Cards Internationals and RoboXchange Cards. Another method of conversion is through the use of some ‘electronic money merchants’ who accept e-gold currency. These types of merchants will accept e-gold for cash at commercial merchants. Also, some merchants trade certain products for e-gold. For example, a smart card company known as ‘gCard’ can be purchased with e-gold, which can be converted to cash through an ATM. In addition, e-gold currency can be converted to traditional cash, using the e-gold cirrus maestro ATM debit card, which is cashable at most ATMs. Cf Grow, Cady, Rutledge and Polek (2006) ‘Gold Rush: Online payment systems like e-gold Ltd are becoming the currency of choice for cybercrooks’ available at <http://www.businessweek.com/magazine/content/06_02/b3966094.htm> [accessed on 1 January 2011].
\textsuperscript{327} Grow, Cady, Rutledge and Polek (2006) ‘Gold Rush: Online payment systems like e-gold Ltd are becoming the currency of choice for cybercrooks’ available at <http://www.businessweek.com/magazine/content/06_02/b3966094.htm> [accessed on 1 January 2011].
\textsuperscript{328} Grow, Cady, Rutledge and Polek (2006) ‘Gold Rush: Online payment systems like e-gold Ltd are becoming the currency of choice for cybercrooks’ available at <http://www.businessweek.com/magazine/content/06_02/b3966094.htm> [accessed on 1 January 2011].
follows the peer-to-peer issuer model of e-payment, and as shown earlier, there are big risks associated with it.\textsuperscript{329}

E-gold poses a threat for the following reasons:

(i.) First, it is very easy to open an e-gold account. It has been structured in such a way that it is not cumbersome for potential customers. The process does not include a vetting process, which would naturally require a thorough verification of the customer’s identity. Just as with any system with little or no regulatory measures, it becomes very attractive to cyberlaunderers;

(ii.) Also, e-gold guarantees anonymity. As bees are attracted to a honeycomb, so, too, does anonymity attract criminals such as terrorists, hackers who steal and sell stolen identities, pornographers, and, above all, cyberlaunderers. This is evident in the following quotation:

Some of e-gold's customers have been unsavory. Omar Dhanani used e-gold to launder money for the ShadowCrew, a cybercrime gang with 4,000 members worldwide, according to an October, 2004, affidavit by a Secret Service agent. Based in a stucco house in Fountain Valley, Calif., Dhanani used his PC to hide the money trail from the sale of thousands of stolen identities, bank accounts, and credit-card numbers, the government said. Accomplices sent him Western Union (FDC ) money orders, which, for a fee, he filtered through e-gold accounts. On Oct. 4, 2004, Dhanani, 22, who used the nickname Voleur -- French for thief -- boasted in a chat room that he moved between $40,000 and $100,000 a week. He pled guilty in

\textsuperscript{329} See paragraph 3.3.2.4 above.
November to conspiracy to commit fraud and faces up to five years in prison.\textsuperscript{330} E-gold has been embroiled in many legal problems because of its very porous characteristics,\textsuperscript{331} which have attracted the scrutiny of several law enforcement agencies, leading to several investigations into its activities, and

(iii.) Given that e-gold does not fit the frame of a financial institution, as envisaged by regulatory instruments, such as the Bank Secrecy Act and the Money Laundering Control Act in the United States, it is not under any obligation to observe the Know Your Customer (KYC) principle, It therefore does not make any Currency Transaction Reports (CTRs), nor is it under any obligation to report suspicious activities. In addition, websites like e-gold are registered in jurisdictions with very lax law enforcement regimes. For this reason, it is not surprising to learn that e-gold Ltd has its server in Luxemburg.\textsuperscript{332}

\textbf{3.5.4.1. \textit{Example of cyberlaundering through online barter trade}}

For a better understanding of how online barter trading works, a hypothetical scenario in which e-gold is used as a currency is sketched below:

\begin{footnotesize}
\begin{enumerate}
\item Grow, Cady, Rutledge and Polek (2006) ‘Gold Rush: Online payment systems like e-gold Ltd are becoming the currency of choice for cybercrooks’ available at <http://www.businessweek.com/magazine/content/06_02/b3966094.htm> [accessed on 1 January 2011].
\item Cf discussion in Chapter 6, paragraph 6.5.1.
\end{enumerate}
\end{footnotesize}
Jack Sparrow is a drug dealer living in Luxemburg. Within one year he amassed $10 million in profits from the drug trade. Mindful of the risks involved in depositing the funds directly into his bank account, he goes online (www.e-gold.com) and opens an account with E-gold Ltd, where he uses the $10 million to purchase an equivalent value of e-gold (i.e. placement). He does this to avoid being subjected to the KYC and customer due diligence procedures which are typical for most banks. After placing the funds, Jack Sparrow purchases assets and financial products online from various companies that accept the e-gold currency (i.e. layering).

He also purchases a financial stake in a company listed on the stock exchange, and also resells some of the assets that he purchased for traditional cash (i.e. integration). Note: Jack Sparrow could, alternatively, have more than one e-gold account in which he could deposit portions of the illegal proceeds to feign legitimacy).

3.5.5 Virtual worlds

To date, the use of virtual worlds to launder money is certainly the most innovative and unassuming technique devised by criminals. Its uniqueness, which lies at the furthest end of Machiavellian tactics, makes the laws prescribed by the present AML regime look farcical. It is by far the most problematic, yet certainly one of the cleverest techniques used, and one without which any discussion on cyberlaundering would be incomplete.

---

333 This is an example of a real-life scenario involving e-gold Ltd. See Grow, Cady, Rutledge and Polek (2006) ‘Gold Rush: Online payment systems like e-gold Ltd are becoming the currency of choice for cybercrooks’ available at <http://www.businessweek.com/magazine/content /06_02 /b3 966094.htm [accessed on 1 January 2011].
A virtual world is part of online gaming, which is also known as Massively Multiplayer Online Role-Playing Games (MMORPG). As the name suggests, MMORPGs are internet-based games with attributes of a social network, and, in very colloquial terms, allow players to ‘live’ in a simulated environment that is very much akin to the real world. In other words, an almost exact replica of real life is represented in a virtual environment.\(^{334}\) In a virtual world, the players are represented by their avatars,\(^{335}\) with which they can conduct regular activities that mirror real life in its entirety. In practice, however, it is possible for an individual to create more than one avatar.\(^{336}\) The ‘gaming’ aspect of virtual worlds lies in the activities of players who are often competing with other players, particularly in an attempt to amass wealth by way of building virtual houses and buying virtual land. The innovation of virtual worlds is indeed the very apex of the continuously evolving genre of online gaming. Whilst certain virtual worlds are centred on a virtual-fictional world, others rely on user-generated content and the co-creation of digital objects by users, for example, the virtual world known as Second Life.

---

\(^{334}\) Cf Klimmt (2011: 1) and Bishop (2009: 5).

\(^{335}\) An avatar is a digital representation of an individual on the internet. An avatar can be created by the online gamer, who has the liberty of cloning this digital representation into any form or appearance he chooses. Given the highly developed state of graphic arts and designs at present, the idea of an avatar far exceeds merely a cartoon figure, as the semblance with reality is often uncanny.

\(^{336}\) In many cases, for individuals seeking to use the business aspect of participating in virtual worlds, this task is outsourced to certain skilled individuals. Every avatar in a virtual world has to undergo evolution and development of skills, which it can perform within the virtual economy. Given the painstaking nature of the required evolution, at present, this initial process is being outsourced to certain persons in India, China, Pakistan or to most other developing countries with developed cyber expertise, who are, in turn, paid a few dollars as remuneration. Once avatars are brought up to a certain standard, they are then passed over to their original creator, who could then use them to invest considerable sums of money into the online economy. These persons are also known as identity brokers, who invest hours in creating and building up avatars to perform specific tasks in these virtual worlds, after which they are auctioned. Demetis (2009: 11).
Virtual worlds can be sub-divided into three basic types: (a) MMORPGs, which are virtual worlds that are centred on a virtual fictional world, such as the World of Warcraft, where players, through their avatars, interact with thousands of other players, collecting digital objects of diverse kinds, resolving tasks and organizing themselves into groups to overcome certain challenges; (b) virtual worlds that rely on user-generated content that perpetuates the co-creation of digital objects by users, such as SL, Entropia Universe, Kaneva, Active Worlds and IMVU; and (c) virtual worlds that take on the character or features of social network sites, such as Facebook or Twitter. These virtual worlds host a virtual representation of many real individuals, without providing a virtual spatial environment which users can navigate through. Links between social profiles make social relationships visible and many modalities exist that create social dynamics and appeal, such as online groups and shared interests.

Virtual worlds are certainly good business and are gaining popularity by the day. Other than the appearance of the real world, virtual worlds also experience the same conditions and situations that exist in real life. This is due to the fact that they have their own functioning economies, political and social lives. In a recent report by the World Bank, the current worth of all

---

337 Klimmt (2011: 3).
339 Klimmt (2011: 3).
340 There are several other types such as Twinity, Fregger, PlayStaion Home and There, which are mostly social virtual worlds that exist permanently in three dimensional (3D) display, popularly called metaverses. See Cornelius and Hermann (2011: v).
virtual worlds combined stands at about US$18 billion\textsuperscript{343} with an average of 800 million users worldwide.\textsuperscript{344} In the year 2011, Entropia Universe had an annual turn-over of more than 1.5 billion PED – the virtual currency in the online space meaning ‘Project Entropia Dollar.’ By the end of 2012, virtual worlds might each have an average of approximately US$1 billion.\textsuperscript{345} One virtual world, Second Life, will be singled out here because of its popularity\textsuperscript{346} in order to better explain the nature of virtual worlds and how they are relevant in the cyberlaundering discussion.

SL was developed by Linden Labs in the United States in 2003. The players in SL are known as ‘residents,’ who, 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.”\textsuperscript{347} The currency used in SL is known as Linden Dollars (L$). Much like the real world, the activities of all residents revolves around money (i.e. the L$), as it is necessary to eke out a living and for the flow of commerce. Shrewd residents actually make profits from their inworld transactions. As a start-up, residents receive a stipend of L$300 a week, but are not limited to this amount because in SL, residents can convert real-world money, such as the US Dollar or the Euro, into L$. SL has a special currency

\textsuperscript{347} See Jamali (2009:32).
or money exchange service known as Xstreet, which makes it possible for such conversion to be done. With money in hand, residents can do virtually anything they wish, including creating virtual objects and purchasing real estate.\(^{348}\)

To conceive of virtual worlds as mere game sites would be to underestimate them, since unlike other online games, they transcend the virtual world into the real world, taking a heavy toll on it, with dire consequences. One such consequences is the window of opportunity it opens for criminals who wish to wash illegal funds. The potential of virtual worlds for money laundering is explored below, using SL as a sample case.

(i.) In virtual worlds such as SL, where attempts have been made to duplicate real life, apparently only the dazzling parts and pleasantries of the real world are imitated, not the daily grind of human life and the hard realities of the law. There are very few regulations or laws that control individual relations. AML laws are, consequently, non-existent. The existing laws in virtual worlds take the form of Terms of Service, which mainly serve to protect residents or players from harassment, disclosure, indecency, intolerance and assault.\(^{349}\) What a dreamland for money launderers! Innovators of virtual worlds possibly did not foresee this eventuality. So, the question that arises is this: Given SL’s limitless

---


capability to mimic real life, is it plausible to create virtual police or virtual law enforcement agencies to combat money laundering in the virtual world? Would the existence of a virtual criminal justice system not serve as a deterrent for potential money launderers desirous of escaping from the strictness of cumbersome regulations and red tape? The question is whether it is at all possible to enact laws in the virtual world which can, in fact, be aimed at combating money laundering in the virtual world. In other words, can we create a virtual world in which avatars can be arrested, tried and sent to prison?

The fact of the matter is that, even though a virtual economy operates like a real world economy, it is not as controlled as one. For instance, SL’s Xstreet creates the possibility for residents to change real-world money to L$ at often profitable rates. Conversely, the reverse is also the case. Similarly, in Entropia Universe, the virtual exchange rate is 10/1 (i.e. 10 PEDs to United States $1), with which to convert money back and forth into USD.\footnote{Demetis (2010: 9). Cf Spiegel (2007: 3.)} The conversion is done mainly through ATMs, which now accommodate virtual currencies.\footnote{Demetis (2010: 9).} Given the current statistics that approximately US $1.5 million change hands every day in SL,\footnote{Demetis (2010: 9). Cf Spiegel (2007: 3.)} the playing field is widened further for criminals. With the capability of Xstreet, if the exchange is done with illegal funds, integration would have occurred, as the dirty money, having been
washed, would be integrated into the real-world commerce. As a caveat, Xstreet is not a real financial institution; it is not under any obligation to comply with the reporting obligations, nor is it required to file CTRs, as is expected from terrestrial financial institutions in the real-world.

(ii.) Virtual worlds also create the possibility of tax evasion. In SL, by way of principle, only residents that live in countries which are considered part of the European Union may be charged value added tax (VAT).\(^{353}\) VAT is charged on all transactions conducted by the resident, using the L$ for which the resident pays Linden Lab,\(^{354}\) but not charged in transactions in L$ between residents. Due to the fact that residents do not have to disclose their source of income, and resident-to-resident transactions are not subject to taxation, it is easy for residents to evade payment of taxes, especially on goods or services which might be taxable in the real world. And given that tax evasion is but one of the many predicate offences for money laundering, it is also more convenient to ‘wash’ such illegal proceeds in such an environment.

(iii.) Also, anonymity is an advantage. Players in virtual worlds are very indistinct and vague, and the idea of a ‘resident’ could really be a veil

\(^{353}\)This principle originates from the Council of Europe: Council Directive 2002/38/EC on the value added tax arrangements applicable to radio and television broadcasting services and certain electronically supplied services, adopted by the Parliamentary Assembly on 7 May 2002 and which came into force on 1 July 2003. According to the Directive, VAT should be levied on the supply through electronic networks of software and computer services generally, and compliance is mandatory for all member countries of the European Union.

for anyone, saint or criminal. Other than the information a fellow resident puts into his profile, which is visible to other residents, and the representation of an avatar, residents know nothing about each other. This is further exacerbated by the fact that virtual worlds do not have to verify the identity of any player before joining the relevant community. Since one’s true identity cannot be ascertained correctly in anyway, such an environment is bound to propagate crimes such as identity theft and fraud, which are also predicate offences for money laundering.

What is more, in some virtual worlds such as SL, there are the so-called ‘virtual banks’ that house L$ or the relevant virtual currency which operates as real-world banks and where residents can open legitimate bank accounts. Also, here, the opening of a bank account is completely hassle-free, with no due diligence performed by the virtual bank. Thus, again, the true identity of the resident remains unknown. This is reminiscent of the problems identified earlier on online banking.\textsuperscript{355} The fact that basic banking laws are non-existent in virtual worlds has numerous repercussions for the real-world economy, one of which is the proliferation of money laundering activities.

(iv.) In addition, the act of smurfing thrives in virtual worlds. The idea that any person can become a player or resident in a virtual world as an anonymous entity, or with fake identification, after which he or she can go about his/her business in the community without raising an eye-brow,

\textsuperscript{355} See paragraph 3.5.1 above.
appears as a perfect plot to a smurf story. Innumerable ways exist in a virtual world in which a criminal can employ smurfs to layer illegal funds in the community, and because of the attribute of anonymity, the chances of getting caught are slim. This is further mitigated by the fact that Xstreet exists with which L$ can be converted to real-world money, and vice-versa.\textsuperscript{356} At the end of the process, the money is integrated into real-world commerce, appearing untainted.

3.5.5.1 Example of cyberlaundering using virtual worlds

Virtual worlds present an environment in which a criminal can weave and connive brilliant schemes through which his/her illegal funds can be placed, layered and integrated all at once, without leaving behind a single trail. An example is sketched below:

Jack Sparrow is a drug dealer living in South Africa. His annual turnover from his unlawful enterprise is about US$ 2 million. He learns about virtual worlds from a friend who is a game addict, and about the possibility of using such a novel method to launder his funds. Jack Sparrow, thereupon, joins SL as a resident. He buys a virtual land on which he later builds a big multi-purpose entertainment company called ‘The Lounge.’ The Lounge offers all sorts of social activities, ranging from night clubs to a diner and coffee shops. Jack Sparrow makes it a condition that visiting The Lounge is by invitation only. John Doe is an acquaintance of Jack Sparrow who often served as a middle-man in his drug dealings. Jack Sparrow employs John Doe as a smurf, together with several

\textsuperscript{356} Jamali (2009:45) and Klimmt (2011: 3).
other people who live on different continents in the world. For a commission, Jack Sparrow requires the smurfs to become residents on SL in order to clean his funds. Jack Sparrow buys several smart cards which he tops with varying value from his illegal funds. Thereafter, he sends the smart cards to all the smurfs. Jack Sparrow further invites the smurfs to The Lounge on an exclusive basis. Also, Jack Sparrow charges a membership or joining fee to the smurfs which is equivalent in value to the amount or value on each smart card in their possession. The money is paid to Jack Sparrow in L$. Thereafter, Jack Sparrow converts some of the monies back to real-world money, and further trades with the other smurfs with the remainder, after which, again, he converts the proceeds derived into real-world money.

3.6 WHAT THE FUTURE HOLDS FOR CYBERLAUNDERING

Years ago, one could have said that the development of this area of crime was still in its embryonic phase, but not so today. At present, cyberlaundering is well beyond its adolescent stage, but has certainly not reached the peak of its development. Just as this phenomenon was spawned by the realities of modern times, concomitantly, and in line with such trends, its growth and development can be foretold easily. Cyberlaundering is poised to develop in line with technological progress, and seeing that the latter is anything but static, one should anticipate criminals to be equally dynamic. Sadly, the future is anything but bleak for technologically-savvy criminals. This is evidenced by the development in certain key areas of electronic commerce and crime. This section investigates these areas by identifying some key
developments in the areas of e-payment systems, as well as some emerging crimes that represent predicate offences for cyberlaundering.

3.6.1 The advent of mobile payment systems

The World Bank identifies four basic mobile payment systems: (i) The mobile financial information services; (ii) mobile bank and securities account services; (iii) mobile payment services; and (iv) mobile money services. The latter two methods are more pertinent to this study, as they are characterized by having low regulation and supervision. Mobile payment services refer to the use of a mobile phone by non-bank account holders and non-securities account holders to make payments. Viewed objectively, the possibility exists that the payment service providers may have some security and regulatory measures in place, although this is unlikely as most are known to be unscrupulous. The mobile money services method appears more fascinating due to the fact that cellular network subscribers may store actual

---

358 This refers to the ability of online users to view general financial information held by their respective banks, but without the ability to conduct financial transactions. The FATF considers this method a low risk. Financial Action Task Force (2010D: 18). Cf World Bank (2008: 19). For a more detailed discussion on the risks that inhere in this method, see South African Reserve Bank (2008: 23).
359 This method is very much akin to internet banking. This is because financial transactions conducted via internet banking can be conducted similarly on a mobile device. The FATF is of the opinion that mobile service and security account services are likely to be regulated and supervised. Therefore, this method bears little risk. Financial Action Task Force (2010D: 18). Cf World Bank (2008: 21).
361 For example, in South Africa, a bank contracted a mobile phone service provider to provide a banking service that allows accounts to be opened with a mobile phone, without the need for personal contact between the account opener and the bank. To allay fears of irregularity, the South African Reserve Bank issued a guidance paper that sets the minimum criteria that should be met in the identification and verification process when such accounts are opened. See Financial Action Task Force (2010D: 52). Cf South African Reserve Bank (2008: 12).
value on their cell phones. This enables them to use phone credits or airtime as tender for payment at accepting merchants.\textsuperscript{362} Just as with mobile payment services, payment service providers are likely to be less prudent and lax about supervision and regulation.

Mobile payment systems, especially the latter two discussed, are burgeoning rapidly. They are projected to represent the bulk of future electronic payment commerce. It is reported that 1.4 billion people will use mobile phones to remit money by 2015.\textsuperscript{363} The mobile payments industry was said to be worth $100 billion in 2010, and projected to be worth between $200\textsuperscript{364} and $250 billion\textsuperscript{365} by 2012. What is worrying is the thought that mobile payments systems are fusible with e-payment systems which, on their own, are already plagued by numerous problems and loopholes.\textsuperscript{366} One of them is the possibility for mobile service providers to offer open-loop prepaid cards that can be linked to the accounts of their customers.\textsuperscript{367} This could guarantee trans-border services between multiple parties, and perpetuate anonymous illicit transactions.\textsuperscript{368}

Another key factor that explains this booming sector is the fact that mobile payment systems can facilitate peer-to-peer transactions. From the discussion

\textsuperscript{363} World Bank (2008: 14).
\textsuperscript{366} See the discussions in paragraph 3.3 above.
earlier, it is obvious that peer-to-peer model of e-payment systems is a fertile
ground for cyberlaundering operations to thrive solely because traditional
financial institutions, such as banks, which are governed by regulations, are
not involved. Another consequence of this system is the fact that withdrawals
can be made from ATMs without using ATM cards. This can be made
possible by using encrypted codes which can be transferred through mobile
payment services. This means that all that the receiving party needs to do to
obtain cash, is to type the key into the ATM.\textsuperscript{369}

Mobile payments systems are becoming so prevalent that they will become
indispensable. This creates a whole new level of convenience for consumers,
but the question is whether this is safe. Mobile payment services and mobile
money services would represent perfect laundering avenues for
cyberlaunderers, without adequate regulation and prudent control. The issue
of regulation and control is undoubtedly a recurring theme within the broad
discussion of cyberlaundering. Whether the law can keep pace with the
growth of technology is still an unsolved riddle in light of other social and
policy issues which are equally important, although extraneous to the subject
of cyberlaundering.

\subsection*{3.6.2 Growth in predicate offences for cyberlaundering}

Recalling the early years of the AML regime, when attempts were made to
grapple with the phenomenon of money laundering, one of the defining steps

taken was to expand the ambit of predicate offences for the crime as wide as possible, and this included all serious offences.\textsuperscript{370} This was done in order to ensure that there are no loopholes which criminals can exploit to evade liability for money laundering. Also, this was a necessary safeguard for prosecutors and law enforcement agencies.

However, as a caveat to the above, the concept of serious crimes or offences is far-reaching because presently, it has broken traditional boundaries. This is clearly shown by the advent of cybercrime, and cyberlaundering is unique in this respect. Aside from the traditional notion of physical illegal cash, cybercrimes with monetary dimensions are commonly the foundations upon which cyberlaundering is built.\textsuperscript{371} This fact feeds the emergence of what is today known as illicit e-money.\textsuperscript{372} Simply put, criminals are spared the trouble of converting the traditional cash to e-money through smart cards and the like. E-funds in their electronic state are better ‘washed’ in that state before they are integrated fully into the legal economy.

Currently, there is a spiralling growth in cybercrimes involving illicit e-money, chief of which is online piracy. Online piracy is a multi-billion dollar industry which is becoming a growing dilemma in modern times, and it represents one of the biggest predicate offences for cyberlaundering. A report


\textsuperscript{371} In a recent report by the FBI, almost 90\% of all reported crimes in the United States in 2010 were money-related crimes. Internet Crime Compliant Centre (2010) ‘2010 Internet Crime Report’ available at <http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf> [accessed on 9 September 2011].

\textsuperscript{372} Cf discussion in paragraph 3.3 above.
shows that by eradicating software piracy completely - which is only one aspect of online piracy - this would create about $142 billion in economic activity globally by the year 2013.\textsuperscript{373} Online piracy is growing simultaneously with the growth of several online activities such as online gaming and the online music industry. Income derived from the unlawful trade or activities in these industries yields illegal funds, which criminals would be more tempted to launder using the internet. In the United States, the online music piracy\textsuperscript{374} results in about “$12.5 billion dollars in losses to the U.S. economy as well as more than 70,000 lost jobs and $2 billion in lost wages to American workers.”\textsuperscript{375} This number is set to triple in the coming years, and, concomitantly, so would cyberlaundering.

According to the International Intellectual Property Association (IIPA), the issue of copyright piracy ranks number one on its list of key issues and challenges.\textsuperscript{376} Concerned bodies are battling with the dilemma, and much brain-storming is currently taking place on what kind of laws to enact and directives to promulgate to combat the problem. For instance, it is reported

that the European Commission will issue a directive by late 2012 which might propose solutions to the problem in Europe.\textsuperscript{377}

Online fraud is also on the rise, led chiefly by credit card fraud. It is uncertain how much this industry is currently worth, given that in the past 10 years its growth has peaked at over 1000%.\textsuperscript{378} In 2008, it was said to be worth about £4.5 billion.\textsuperscript{379} But the Federal Bureau of Investigation (‘FBI’) estimates its worth in tens of billions, and this is an estimate that has been increasing by at least 2% annually in the past ten years.\textsuperscript{380}

What this shows is that it is not only the proliferation of industries and markets through the internet that generate staggering amounts in profits for criminals, but also the growth of predicate offences for cyberlaundering, and by implication, money laundering. The potential that this creates for cyberlaundering is almost indescribable.

3.7 SUMMARY

In this chapter, the concept of cyberlaundering is deflated and explored thoroughly in order to demystify the aura of evasiveness around it. An

\begin{footnotesize}
\end{footnotesize}
understanding of cyberlaundering is the first step in finding a legal solution to the problem.

However, the importance of cyberlaundering goes beyond merely finding a solution for law enforcement bodies and guardians of the current AML regime. It is also not just another grey area of the law, which a mere perfunctory research can make clear. The issue of cyberlaundering is a legal concern that echoes across the board, and its unfavourable impact on commerce is but one of its many negative effects. Without adequately identifying these issues and bringing them to light, cyberlaundering will continue to be an evasive issue, and its future will remain as bright as it currently appears.
CHAPTER 4
THE PRESENT INTERNATIONAL AND NATIONAL LEGAL FRAMEWORK AGAINST CYBERLAUNDERING

4.1 INTRODUCTION

The stand against money laundering has come a long a way since ways were conceived on how to combat this kind of economic crime. More than ever before, there is a need to fortify existing barricades, and with the advent of cyberlaundering, create new ones.

This chapter embroiders on the legal relationship between money laundering and cyberlaundering, otherwise known as the ‘branch and stem’ relationship, discussed in the preceding chapter. To reiterate, cyberlaundering is an extension of money laundering and is thus not a separate or detached concept. With this in mind, a proper comprehension of the present anti-cyberlaundering (ACL) legal regime first calls for a basic understanding of the present anti-money laundering (AML) legal regime. Hence, one needs to consider closely the existing AML legal framework. This chapter discusses current AML laws and legal principles, the aim being to identify its deficits as regards cyberlaundering and conceive of solutions to curb its growth. Therefore, as a precursor, the current AML legal framework is set out in Part I of this study. Part II discusses the present ACL legal framework. To ensure a complete comprehension of the ACL legal regime, it is discussed at both

---

381 See discussion in paragraph 3.2.2, Chapter 3.
national and international levels. For the present ACL legal regime of local jurisdictions, this chapter samples certain countries such as the United States (US), the United Kingdom (UK), India, and Germany. The criteria used to determine these jurisdictions is that of relevance and prevalence – that is, on the one hand, the relevance of the ACL laws within such jurisdictions, and, on the other hand, the prevalence of the ACL laws within those jurisdictions. Additionally, in these jurisdictions, there is an increased awareness of the cyberlaundering problem, given the high chances of vulnerability that exist.\(^\text{382}\)

This chapter represents the basis for the proposed ACL legal regime that is discussed in subsequent chapters, for it identifies the inadequacies of relevant laws that are pertinent to fighting the problem of cyberlaundering.

\[\text{PART I}\]

\section*{4.2 AN OVERVIEW OF THE CURRENT ANTI-MONEY LAUNDERING REGIME}

\subsection*{4.2.1 General}

The AML legal regime began in a piecemeal fashion, starting locally in the US in the 1970s and gradually spreading internationally from the mid-1980s.\(^\text{383}\) Laws such as the Bank Secrecy Act\(^\text{384}\) (BSA) and the Money

\[^{382}\] Take Germany for example. It is greatly susceptible to money laundering because of its large economy and financial centre, as well as its international linkages; its strong position and strategic location in Europe. About €60 billion of criminal proceeds are generated in Germany alone. The fact that Germany shares the same Euro currency with other European countries only increases this propensity and its predisposition to money laundering activities. Financial Action Task Force

\[^{383}\] See the discussion in Chapter 2, paragraphs 2.2.2.1.
Laundering Control Act\textsuperscript{385} laid the foundation for a myriad of local and international laws that now represent the current AML legal regime.\textsuperscript{386}

The following discussion on the existing legal framework against money laundering is rooted in certain basic legal principles. Primarily, this study relies on relevant laws contained in treaties and conventions. The second legal basis for this study is the principle of customary international law,\textsuperscript{387} which is applicable where a codified law is lacking on the matter. Lastly, due to the fact that the current AML legal regime is comprised significantly of soft laws,\textsuperscript{388} which include principles, policies, directives and recommendations from certain non-governmental organisations and international private sector entities, such as the Financial Action Task Force (FATF) and the Basel Committee on Banking Supervision (BCBS), these soft laws form the third legal basis for the ensuing discussion. Over the years, these soft laws have become legally recognized standards that have been transplanted into the domestic legal systems of most countries. These laws carry much weight because, arguably, they have attained, or, for some, are

\textsuperscript{384} The Bank Secrecy Act of 1970, 31 United States Code 1051 (Public law number 99-570).
\textsuperscript{386} For discussions on the history and development of the AML regime, see paragraph 2.2.2 of Chapter 2.
\textsuperscript{387} Customary international law is a fundamental source of international law that derives from custom. In order for a principle to be welcomed as customary international law, it must satisfy the requirements of \textit{jus cogens} and state practice. That is, the principle must amount to something which the international community accepts as non-derogable rights which states have accepted as law, and the general practice of states. For more details see Cassesse (2005: 117). Cf Werle (2009: 51).
\textsuperscript{388} Soft laws are so-called quasi-legal instruments that are not legally binding, or which, as opposed to hard laws, might be have a weaker binding force in comparison. Cassese (2005: 161) and Evans (2010: 70) and Shaw (2003: 68).
attaining the status of customary international law in the field of AML law, due to the fact that they have become custom or practice for obligated states.

But one should not be naïve to think that the AML legal regime is comprised solely of laws. The essence of the AML legal regime encompasses all efforts made to combat the money laundering dilemma, and it includes the enactment of laws, the enforcement of such laws by relevant authorities, and the compliance with such laws by the concerned parties, persons and institutions alike. On this basis, one can argue that the current AML legal regime rests on three pillars: the prevention pillar; the enforcement pillar; and the compliance pillar. But some authors have argued that the current AML legal regime is comprised only of the first two pillars.389 This study holds the contrary. As is the trend of the current AML legal regime, compliance has proven to be just as crucial as prevention and enforcement.

This section is devoted to dissecting the various constituents of the three pillars in order to ensure a better understanding of later discussions on the current ACL legal regime. The constituents of the current AML legal regime that are discussed later on are premised on the standards set by the FATF in its Forty Recommendations390 and its Nine Special Recommendations.391 These recommendations are a significant part of the soft laws alluded to earlier. The FATF’s recommendations and standards laid the foundation upon

which the current AML legal regime stands today at both national and international levels. Thus, to comprehend the current AML legal regime properly, one needs to understand the existing standards. In addition, the ensuing discussion of the three pillars of the current AML legal regime is also crucial to the overall purpose of this study, as these pillars form the basis upon which a concrete ACL legal regime will be proposed.  

4.2.2 Pillar 1: Prevention

The prevention pillar of the current AML legal regime is comprised of the following: customer due diligence; reporting; regulation; supervision; and sanctions. These constitutive activities are discussed below.

4.2.2.1 Customer due diligence and record-keeping

The customer due diligence (CDD) and record-keeping standard is prescribed in Recommendations 10 and 11 of the FATF’s Forty Recommendations, now contained in its International Standards on Combating Money Laundering, the Financing of Terrorism and Proliferation. Given that most CDD measures often include record-keeping obligations, the term ‘CDD’ alone will be used in the discussion that follows. Generally, these CDD standards are a constellation of various strategies which primarily include a policy paper which was earlier adopted by the Basel Committee on Banking Supervision.

---

392 Cf discussions on the Regulation of Cyberlaundering in Chapter 5, paragraph 5.1, and the Prosecution of Cyberlaundering in Chapter 6, paragraph 6.1.
‘BCBS’), as well as several national laws. The CDD standards place an onus on financial institutions and on other third parties or intermediaries, such as correspondent banks, juristic persons and other non-financial institutions, as is disclosed below.

394 The Basel Committee on Banking Supervision is comprised of members from Argentina, Australia, Belgium, Brazil, Canada, China, France, Germany, Hong Kong Special Administrative Region (SAR), India, Indonesia, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, Russia, Saudi Arabia, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States, who foster cooperation on banking supervisory matters. The aim of the Committee is to promote understanding of banking supervisory issues and to improve the quality of banking supervision worldwide. See Bank for International Settlements (2012) ‘Basel Committee on Banking Supervision’ available at <http://www.bis.org/bcbs/> [accessed on 04 July 2012] and Basel Committee on Banking and Supervision (1988: 1).

395 These measures are generally reflective of United Kingdom guidance notes and the Swiss law. Cf Pieth and Aiofil (2003: 3).

396 For purposes of this paper, the term ‘financial institutions’ take on the meaning outlined by the FATF, which is any person or entity conducting as a business one or more of the following activities or operations for or on behalf of a customer (inclusive of private banking) entailing the following:

(i) Acceptance of deposits and other repayable funds from the public;
(ii) Lending [that includes, inter alia, consumer credit, mortgage credit, factoring, with or without recourse, and finance of commercial transactions (including forfeiting)];
(iii) Financial leasing, excluding financial leasing arrangements in relation to consumer products;
(iv) The transfer of money or value, which includes financial activity in both the formal and informal sector, for example, alternative remittance activity, excluding any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds;
(v) Issuing and managing means of payment (for example credit and debit cards, cheques, traveler’s cheques, money orders and banker’s drafts, electronic money);
(vi) Financial guarantees and commitments;
(vii) Trading in money market instruments such as cheques, compacts discs, and derivatives; foreign exchange; exchange, index and interest rates instruments; transferable securities, and commodity futures trading;
(viii) Participation in securities issues and the provision of financial services related to such issues;
(ix) Individual and collective portfolio management;
(x) Safekeeping and administration of cash or liquid securities on behalf of other persons;
(xi) Otherwise investing, administering or managing funds or money on behalf of other persons;
(xii) Underwriting and placement of life insurance and other investment related insurance, such that includes agents and brokers, as well as,
4.2.2.1.1 CDD for banks

With the advent of the AML legal regime, financial institutions, such as banks, were the first to be affected by the ‘purging’ caused by the enactment of strict AML measures. Undeniably, the adoption of AML measures revolutionised banking operations, and awakened lax banks that slept through the quiet operations of money launderers. But of course, as with any reaction to change, the new system did not sit well with the banks because they were the ones that bore the main burden of the AML legal regime. For a long time, financial institutions have served as the washing machine of money launderers, and it is only understandable that the current AML measures, especially those on CDD, place a heavier burden on financial institutions. This is because they can play a major role in clamping down on money laundering operations. Also called Know Your Customer (KYC) principles, the CDD measures exist to ensure that a bank’s reputation and integrity are protected. Such measures represent sound risk management for the banks. Conversely, non-adherence to the set CDD measures is sure to subject banks to legal and operational risks.

---

397 An example of this predates modern times. As far back as the mid-1970s, a group of banks in California were averse to the stringent provisions of the Bank Secrecy Act and had unsuccessfully contested the constitutionality of the Act in the case of California Bankers Association v. Schultz 39L ed 2d 812 (1974) n5. In rejecting their application, the United States Supreme Court noted that the right that is being protected in the Act outweighs the concerns and inconveniences caused to the banks as a result. See the discussion in paragraph 2.2.2.1, page 10, Chapter 2.


Banks are under an obligation to observe the following CDD measures or policies:

(a.) Policy on general preemptive measures

There are certain general preemptive measures that banks are required to observe before engaging in transactions with prospective and regular customers. First, banks should be able to draw a fine line between anonymity and confidentiality. While the latter represents a standard ethical banking principle, the former is often enveloped in illegality. Banks are urged to desist from opening accounts for persons who insist on anonymity. Customers often prefer numbered accounts, with an account number or a code name which is used in subsequent documentations to substitute the real name of the beneficial owner, who would be known to the bank. This notwithstanding, the Basel Committee on Banking Supervision (BCBS) and the Wolfsberg Group have proposed that the identity of the customer should be disclosed to a sufficient number of the bank’s personnel to ensure compliance with the

---


401 The Wolfsberg Group is a conglomerate of global banks that have adopted global standards in order to ensure that there is a unified front in the fight against money laundering. The Wolfsberg Group consists of Algemene Bank Netherlands and Amsterdam and Rotterdam Bank (also known as ABN AMRO); Banco Santander, Bank of Tokyo-Mitsubishi-UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, Hong Kong and Shanghai Banking Corporation (also known as HSBC), JP Morgan Chase, Société Générale and the Union Bank of Switzerland (also known as UBS). Established in the year 2000 at Chateau Wolfsberg in Switzerland, hence its name, the Wolfsberg Group of Banks has since issued various AML policy papers. For more information see the website <http://www.wolfsberg-principles.com/index.html> [accessed on 6 November 2011]. See also discussion in paragraph 4.3.2.4.2 below.
requisite due diligence procedure. As regards the essential due diligence steps, the Wolfsberg Group has proposed that banks should ascertain the purpose for opening the account, the expected account activity, the source of funds in relation to the economic activity that generated the net worth, the estimated net worth, the source of funds and references to other sources to corroborate other information where available.

(b.) Policy on customer acceptance

Banks have to develop clear-cut policies on customer acceptance. This requires a proper delineation of customer profiles in order to identify those customers that pose higher risks than the ordinary customers. Overall, the determining factors include the potential customer’s “background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators.” This information enables the bank to prescribe the necessary account opening requirements for the potential customer. Needless to say, the same account opening requirements for customers should not necessarily be the same as they vary, depending on the risk indicators.

---

403 A person’s net worth is simply the result derived from deducting one’s liabilities from one’s assets (put mathematically: Assets – Liabilities = Net Worth). For more details see Madinger (2012: 110).
(c.) Policy on customer identification

Recommendation 10 (a.) of the FATF Forty Recommendations provides that banks should undertake essential CDD measures, which include “identifying the customer and verifying that customer’s identity using reliable, independent source documents, data or information.” The BCBS has significantly expanded on this principle, which is deemed very crucial. For customers and those acting on their behalf, the BCBS recommends that policies should be documented and enforced in order to ensure proper identification. In this sense, non-resident customers who seek to open accounts in foreign jurisdictions should be earmarked as potential threats, as it is often difficult to subject them to the standard vetting procedures.

(d.) Policy on clients and beneficial owners

The CDD requirements for clients and beneficial owners must be clearly distinguished. Depending on the kind of client a bank has, whether a natural person, a corporation, a partnership, a foundation or a trust, recent and complete identity papers are mandatory.

---

409 Basel Committee on Banking Supervision (1999: 3).
410 Beneficial owners have been defined as natural persons who own or control a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates persons who exercise ultimate effective control over a legal person or arrangement. Financial Action Task Force (2012A: 12).
411 For a natural person, official identity papers may constitute sufficient proof; for corporations, partnerships, foundations, the bank will receive documentary evidence of the organisation and its existence. The Wolfsberg Group (2002: 2).
However, in the world of large-scale money laundering, the key players are often the smurfs who engage in transactions for the benefit of an instigating party. Therefore, with the policy on identifying beneficial owners, banks are not only required to consider first-party customers such as their clients, but also other parties who stand to benefit from the transaction between the bank and its client. This rationale is succinctly stated in Recommendation 10(b) of the FATF Forty Recommendations, which urges banks to take all necessary measures to ascertain the identity of the beneficial owners of the account.\footnote{Financial Action Task Force (2012A: 12). Cf Financial Action Task Force (2004B: 4).}

Given that beneficial owners could be natural persons, legal entities, trust and unincorporated associations, a more stringent kind of CDD is required.\footnote{Financial Action Task Force (2012A: 19). For example, with regard to natural persons, when the account is opened in the name of an individual, the private banker must establish whether such person is acting on his/her own behalf, and where there is doubt, the bank will need to establish the capacity in which the account holder is acting. As regards legal entities and unincorporated associations, the bank is obliged to understand the structure of the company and its control system as well as to identify the identity of the legal person or corporation and to obtain sufficient proof that the person acting on its behalf is so authorized. Also for trusts, it is prudent for banks to determine the source of the funds, those with control over it, and persons with the power to remove trustees. The Wolfsberg Group (2002: 2) and the Financial Action Task Force (2012A: 19). Cf Financial Action Task Force (2003: 4) and Basel Committee on Banking Supervision (1999: 3).}

Furthermore, Recommendation 22 states that the CDD measures are applicable to the following groups: casinos when they engage in transactions that are equal to or above the applicable designated threshold;\footnote{Recommendation 22(a), Financial Action Task Force (2012A: 19).} real estate agents who are engaged in transactions for their clients concerning the buying and selling of real estates;\footnote{Recommendation 22(b), Financial Action Task Force (2012A: 19).} dealers in precious metals and stones who engage in cash transactions with their clients equal to or above the applicable
designated threshold;\textsuperscript{416} lawyers, notaries, and other independent legal professionals and accountants who carry out transactions for their clients;\textsuperscript{417} trust and company service providers, when they carry out certain transactions for a client.\textsuperscript{418} Thus, there is no room for assumptions, and such measures should apply to every transaction, regardless of the regularity of the customer, or the pattern of transaction. Other than beneficial owners, it is equally important for CDD to be conducted in respect of other persons, such as money managers or intermediaries who hold accounts for the benefit of their clients.\textsuperscript{419}

(e.) Policy on obtaining outside information

Recommendation 10(d.) of the FATF Forty Recommendations suggests that banks should always take the necessary steps to obtain all required information from outside sources, such as third parties, depending on the

\textsuperscript{416} Recommendation 22(c), Financial Action Task Force (2012A: 19).
\textsuperscript{417} Recommendation 22(d), Financial Action Task Force (2012A: 19). Such transactions might include the buying and selling of real estates; management of bank, savings or securities accounts; management of bank, savings or securities accounts; creation, operation or management of legal persons or arrangements, and buying and selling of business entities and organisation of contributions for the creation, operation or management of companies. Cf Financial Action Task Force (2003: 7).
\textsuperscript{418} Recommendation 22(e.), Financial Action Task Force (2012A: 7). For trust and company service providers the following transactions could be performed on behalf of the respective clients: acting as a formation agent of legal persons; acting as a trustee of an express trust or arranging for another person to act as such; acting as a director or secretary of a company, partner of a partnership, or a similar position in relation to other legal persons, or arranging for another to act as such; acting as a nominee shareholder for another person or arranging for another person to act as such, and providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement. Cf Financial Action Task Force (2003: 16; 7).
\textsuperscript{419} The Wolfsberg Group (2002: 3). However, as a caveat, it is suggested that no due diligence would be required for holders of a power of attorney. The Wolfsberg Group (2002: 3).
nature of the relevant transaction.\textsuperscript{420} This CDD measure is a closed-list provision, which seeks to ensure that a bank is not confined to the truth or untruth of whatever information is provided by a customer. Conversely, this provision enables enforcing authorities to put relevant parties under an obligation to supply such information, as long as such request is made in good faith and the information requested is within the confines of the proposed transaction, and not in violation of any vested rights of the bank’s potential client.\textsuperscript{421}

(f.) Policy on conducting CDD on a regular basis

According to Recommendation 10 (d.) of the FATF Forty Recommendations, banks have a duty to conduct ongoing due diligence on the scrutiny of transactions taken and on the business relationship throughout the course of the relationship. This is done to ensure that the institution’s knowledge of the customer, the business and risk profile, and source of funds are consistent with the subsequent transactions.\textsuperscript{422} However, this does not imply that the initial CDD measures should be conducted repeatedly for every subsequent transaction with the customer. Where a full CDD was performed at the start of business with the customer, the financial institution is expected to rely on

\textsuperscript{421} The rights referred to include one’s right to privacy, and the confidentiality of personal information. A balancing exercise should normally be carried out by the relevant authority to ensure that a justifiable basis exists for which such request is made and, concomitantly, supplied.
the identification and verification steps, unless reasons exist that disprove the veracity of that information.423

The BCBS suggests that banks should develop clear standards on the kind of records to be kept on customer identification and individual transactions, as well as their retention period.424 The Wolfsberg Group adds to this rationale by indicating the applicability of the risk-based approach to the process. As recommended, the degree of on-going observance of CDD measures should depend on the respective categories of customers, and those posing a higher risk would naturally necessitate a higher degree of due diligence.425 This is essential in order for a bank to conduct CDD effectively on a regular basis.426 Conducting on-going CDD helps in discerning deviations and abnormalities in customer operations. It also highlights possible loopholes at the initial stage when the bank verifies the customer’s identity and the nature of the transaction.427

426 It is suggested that all identification papers should be retained for at least five years after an account is opened, and all financial transactions should be retained for at least five years after the transaction has taken place. Basel Committee on Banking Supervision (2001A: 7). Cf Recommendation 10(d), Financial Action Task Force (2012A: 14). Cf Financial Action Task Force (2003: 7).
427 Some indicators that might form grounds for reasonable suspicion include transactions that do not make economic or commercial sense, or transactions that involve large amounts of cash deposits which are inconsistent with the normal or expected transactions, with due consideration being given to potential risk variables. Basel Committee on Banking Supervision (2001A: 13). Cf Basel Committee on Banking Supervision (1999: 6) and Basel Committee on Banking Supervision (1997: 12).
Knowledge of when CDD should be performed is very crucial. However, this differs from understanding the kind of CDD required. As a general rule, CDD should be applied on a risk-sensitive basis, but this is not to say that it is not expected at certain stages in the client-bank relationship. The following examples are instances where CDD measures are expected to be applied:

(i.) At the start of business relations

When beginning transactions with customers, by virtue of Recommendation 10 (i), it is incumbent on financial institutions not only to verify the identity of the customer in question, but also the party benefitting from the transcation (also known as the beneficial owner) as well. This is part of the expansive nature of the FATF Recommendations, as an affront to the myth that financial institutions need only focus on their respective customers. However, the question to be answered is the meaning of the phrase - ‘start of business relations.’ A clear answer to this would depend on the circumstances of the relevant case and the operational practices of the relevant bank. The FATF suggests that financial institutions should conduct the CDD “as soon as reasonably practicable,” bearing in mind that the money laundering risks should be effectively managed and the normal course of business is not interrupted as a result.

---

428 This is discussed further in paragraph 4.2.3.1.5 below.
(ii.) For occasional transactions

According to Recommendation 10 (ii), and as regards ‘occasional customers,’ financial institutions should be required to conduct CDD when carrying out the following occasional transactions: (a.) Transactions that are above a designated threshold, which, as also recommended, should be US $15,000 (or €15,000). This situation foresees instances where the transaction involves a single operation or several operations that appear to be linked; (b) Transactions involving wire transfers in circumstances foreseen in the Interpretative Note to Special Recommendation VII to the FATF IX Special Recommendation; and under Recommendation 10 (ii) performing transactions at financial institutions, a designated threshold of US $15 000 or €15 000 per transaction is recommended.

434 Financial Action Task Force (2001A: 2) and Financial Action Task Force (2012A: 17). Special Recommendation VII (SR VII) is aimed at preventing criminals, and, specifically, terrorists from having unrestricted access to wired transfers to moving illicit funds. As provided in the Interpretative Note to Special Recommendation VII: Wire Transfers, in order to alleviate the possibility of criminal use of wire transfers, it ensures that the information on the originator of wire transfers is available to law enforcers, financial intelligence units and beneficiary financial institutions. See Financial Action Task Force (2001A: 16). In addition, Special Recommendation VII seeks to ensure that all wire transfers are traceable and it also seeks to minimise thresholds in order to prevent driving transactions underground. Financial Action Task Force (2001A: 18) and Financial Action Task Force (2012A: 17).
435 Financial Action Task Force (2003:18) and Financial Action Task Force (2012A: 19). As a caveat, transactions would be deemed to exceed the stated threshold where the transaction exceeding the amount is carried out in a single operation or where there are several transactions that appear to be linked.
(iii.) General suspicion

According to Recommendation 10(iii.), CDD measures should also be adopted where financial institutions have a general suspicion that there are money laundering or terrorist activities being carried out, and where such circumstances exist, financial institutions are required to take further steps, such as identifying and verifying “the identity of the customer and the beneficial owner, whether permanent or occasional, and irrespective of any exemption or any designated threshold that might otherwise apply.” Read with the FATF’s Recommendation 20, financial institutions should be required by law or regulation to file a suspicious transaction report (STR) to the necessary financial intelligence unit (‘FIU’), where there is a reasonable suspicion of money laundering and terrorist activities. To guarantee the efficacy of this provision, and as required in Recommendation 21, financial institutions, particularly their employees, such as directors and other officers, are prohibited from disclosing that an STR has been filed to an FIU. This is primarily meant to prevent ‘tipping off.’ Where customers are tipped off, this circumvents the work of law enforcers because it compromises future efforts to investigate and retrieve the illegal funds.

---

437 Financial Action Task Force (2003: 8) and Financial Action Task Force (2012A: 19). Cf the Egmont Group (2004E: 2) and Muller (2007: 87). The idea of an FIU is the brain-child of The Egmont Group, which is an informal body of government receiving agencies that share a common goal of providing a forum to enhance mutual cooperation and to share useful information in detecting and combating money laundering. Muller (2007: 87). The Egmont Group was established in Brussels, Belgium, in June 1995. For discussion on the meaning of an FIU, see paragraph 4.2.2.2.3 below. Cf the Egmont Group (2004B: 2) and Muller (2007: 88).
CDD measures is a very sensitive process, which could topple the overall AML process if criminal customers are aware, financial institutions, at the risk of such tipping off, are advised not to conduct any CDD, but only to file a STR to the relevant FIU.\textsuperscript{440} This is an exception to the general rule, as it is the only instance where CDD measures are not encouraged.

Financial institutions and their employees are no doubt put in a difficult situation because of their obligation to report a reasonable suspicion to an FIU. This is further compounded by the fact that there might be some legal constraints, such as the existence of a valid contract, which would prevent such an official from divulging information. But such a situation is foreseen in Recommendation 21(a.), which proposes that financial institutions and their employees should be “protected by legal provisions from any kind of civil or criminal liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision.”\textsuperscript{441} As a crucial caveat, the STR should be filed in good faith to the FIU, and the whistleblower is not required to know or understand fully the relevant underlying criminal activity (i.e. the predicate offence) or whether or not such criminal activity actually occurred.\textsuperscript{442}


(iv.) Inaccuracy of customer information

Recommendation 10 (iv.) also foresees a scenario where a financial institution already possesses inaccurate customer information. In other words, where a financial institution fails to conduct proper CDD at the start of business relations, all hope is not lost, for Recommendation 10 (iv.) says that a CDD should still be performed. This means that the bank would have the option of terminating the contractual relationship with the customer or simply just proceeding with the filing of an STR to the relevant FIU. Again, the caution against tipping off the customer needs to be heeded.

4.2.2.1.2 CDD for correspondent banks

Financial institutions have an obligation to observe CDD towards other financial institutions with which they have a correspondent relationship. Correspondent banking is a situation where one bank (the ‘correspondent bank’) conducts business with or provides banking services for another bank (the ‘respondent bank’), which the latter is not otherwise able to offer directly. The rationale that underlies this is the expansive approach to the prevention of money laundering that the current AML legal regime requires,

---

445 Basel Committee on Banking Supervision (2001A: 12). However, it is noted that the principle of correspondent banking is not limited to banks alone but also to broker-dealers, mutual funds, unit trusts, investment services firms, hedge funds, introducing brokers, money service businesses, pension funds, credit card providers, commercial credit card companies, household fiancé companies, mortgage banks, building societies and leasing companies. The Wolfsberg Group (2002: 1).
given that banks are now required to be scrupulous in all transactions, whether in relation to customers directly or fellow financial institutions.

In principle, the general CDD measures set out in Recommendation 10 of the FATF Forty Recommendations should be applied equally to respondent banks in a correspondent relationship with a corresponding bank. However, given the uniqueness of this relationship, Recommendation 13 raises the bar by prescribing additional measures to be observed. It states that financial institutions should take reasonable steps in order to ascertain the respondent bank’s AML controls, and they should gather adequate information about the respondent institution in order to understand fully the nature of its business, the reputation of the institution, the quality of supervision and whether such an institution has been subject to a money laundering investigation or regulatory action. Moreover, it is necessary to know who owns and the respondent bank. Banks should also be wary of the possibility that the respondent bank might be a ‘downstream correspondent clearer.’ In particular, banks should refuse to engage in relations with shell banks. The Wolfsberg Group defines a shell bank as:

---

446 Financial Action Task Force (2012A: 16). Cf Basel Committee on Banking Supervision (2001A: 12) and Financial Action Task Force (2003: 6). In this context, a regulatory action implies an action that is imposed on a bank for failing to comply with a relevant regulatory law. The form of CDD measures to be conducted on respondent banks include ascertaining the bank’s domicile and organisation; client ownership and executive management; the respondent bank’s business; its products and services offered; its regulatory status and history; its existing AML controls. See The Wolfsberg Group (2002: 3).

447 A downstream correspondent clearer is a respondent bank that receives correspondent banking services from an institution while it provides corresponding banking services to other financial institutions. This relationship often portends a lot of troubles, necessitating strict AML laws. Wolfsberg Group (2002: 4).
a) A bank that does not conduct business at a fixed address in a jurisdiction in which the shell bank is authorised to engage in banking activities;
b) A bank that does not employ one or more individuals on a full-time business at this fixed address;
c) A bank that does not maintain operating records at this address; and
d) A bank that is not subject to inspection by the banking authority that licensed it to conduct banking activities.\textsuperscript{448}

As a cautionary procedure, a representative of the correspondent bank should endeavour to visit the respondent bank at their premises within a reasonable period after establishing a relationship with it in order to confirm that it is not a shell bank.\textsuperscript{449} Also, financial institutions are obliged to obtain the prior approval of senior management before establishing new correspondent relationships. They must document the respective responsibilities of each institution and must be able to perform the required CDD measures on customers that have direct access to accounts of the correspondent bank, otherwise known as ‘payable through accounts.’\textsuperscript{450} The latter presents the risk

\textsuperscript{448} The Wolfsberg Group (2002: 3). Cf Basel Committee on Banking Supervision (2001A: 12). It should be added that the only exception to the rule that banks that meet these requirements are shell banks are banks that are regulated affiliates, which are banks that are owned, directly or indirectly by a financial institution that is licensed in a jurisdiction that has not been deemed as uncooperative by the FATF and which is subject to the banking authority of that jurisdiction. The Wolfsberg Group (2002: 3).

\textsuperscript{449} The Wolfsberg Group (2002: 3).

that third parties might use correspondent accounts to transact business on their own behalf.  

4.2.2.1.3 CDD for mutual funds and pooled investment vehicles

There are money laundering risks associated with mutual funds and pooled investment vehicles (otherwise called ‘PV’ or ‘PVs’). PVs is a collective term used to refer to hedge funds, private equity funds, unit investment trusts and funds-of-funds, and they can assume legal forms such as corporations, trusts, partnerships and contracts. PVs are often overlooked as not posing money laundering threats due to the fact that they usually have measures and controls which serve as a barricade for money laundering purposes. They are also ignored as a potential threat because they are commonly used for long-term investment purposes with high turnovers that make short-term investment – which money laundering schemes tend to fit – very unusual. 

As part of basic CDD measures to be undertaken, PVs should be able to identify and verify the identity of the investor and the beneficial owner, understand the purpose of the investment and conduct ongoing due diligence.

---

451 Basel Committee on Banking Supervision (2001A: 12). Where there is such a risk, it is advised that such a case should no longer be deemed as correspondent banking but an ‘introduced business’ scenario which is usually a tripartite relationship involving an outside party (i.e. third party) who instigates the business relationship. The Basel Committee on Banking Supervision strongly recommends that such third parties be subjected to stringent CDD measures, as is the case with regular bank customers. Basel Committee on Banking Supervision (2001A: 9).

452 The Wolfsberg Group (2006: 1). Other than the legal forms they share, PVs are also characterized by their varying investment objectives, the jurisdictions in which they are organized, the level of regulation to which they are subject, the type of investor they solicit, and the way in which their units or interests and shares are distributed. The Wolfsberg Group (2006: 1).

453 The Wolfsberg Group (2006: 1). In addition, a PV is likely not to be involved in money laundering activities because assets that flow into PVs are sourced from financial institutions which are regulated for AML purposes. The Wolfsberg Group (2006: 2). Cf Lilley (2003: 34).
on their investors as well as scrutinise their transactions.\textsuperscript{454} The policies on identification of banking customers and policies on beneficial ownership apply equally to PVs.

However, not all PVs have a direct relationship with their investors. Some investors could use intermediaries to funnel their investments to PVs, hence, establishing an indirect link with the investors, but a direct one with the intermediaries. PVs in such indirect relationships with investors thus create more risks of money laundering. Therefore, it is prudent to always consider existent regulatory supervision to which intermediaries are made subject, as this would determine the level of CDD measures that should be applicable.\textsuperscript{455} Generally speaking, where intermediaries are found to be regulated, there might not be a need to adopt measures which might require the PVs to conduct CDD on the customers of such intermediaries. Logically, the contrary would hold for unregulated intermediaries.\textsuperscript{456}

\textbf{4.2.2.1.4 CDD for wire transfers}

Wire transfers, otherwise called funds transfer, refer to “any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution, \textit{known as the ‘ordering financial institution’} (italics my own), by electronic means with a view to making an amount of money available to a beneficiary at another financial institution, \textit{known as the


\textsuperscript{455} Intermediaries could either be regulated or unregulated. Regulated intermediaries are those that are subject to the AML provisions or local law. The contrary holds for unregulated intermediaries.

\textsuperscript{456} The Wolfsberg Group (2006: 12).
‘beneficiary institution’ (italics my own).”457 In addition, there might be intermediary financial institutions that process wire transfers between the ordering financial institution and the beneficiary financial institution. Also, wire transfers can be done either domestically (where the ordering financial institution and the beneficiary financial institution are in the same jurisdiction) or internationally (where the ordering financial institution and the beneficiary institution are in different institutions). The risk that inheres in the phenomenon of wire transfers is that information on the originator458 of such wire transfers always eludes law enforcement or prosecution authorities, financial intelligence units, financial institutions and beneficiary financial institutions.459

As a starting point, financial institutions are required to set a threshold for all wire transfer transactions.460 For international wire transfers that exceed the set threshold, the information accompanying the wire transfer should always contain the name of the originator, the account number, where there is one, or a reference number in the absence of an account number, as well as the

---

458 An originator of wire transfers can either be an account holder, or where there is none, the party who gives an order with the financial institution to make the transfer. An originator can either be a natural person or legal person.
460 Financial Action Task Force (2004B: 17) and Recommendation 16, Financial Action Task Force (2012A: 17). For international transfers, the FATF stipulates, however, that a threshold of USD $1000 or €1000 should be used as the maximum basis. As a general rule, for transactions falling below this threshold, ordering financial institutions would not be required to provide the originator information for identification or verification purposes, even though such information can be requested where there is a pressing need for such. Financial Action Task Force (2004B: 17) and Recommendation 16, Financial Action Task Force (2012A: 17).
address of the originator.\textsuperscript{461} Realizing that international wire transfers are more prone to use by money launderers, there has been a clarion call for transparency in the wire transfer system, which has always seemed opaque. In spite of its opaqueness, there is a well standardized payment system known as the Society for Worldwide Interbank Financial Telecommunication (SWIFT) tries to enable information on the originator and the beneficiary to be always included.\textsuperscript{462}

The same requirement holds for domestic wire transfers, except that a threshold is generally not required. Also, the requisite originator information might not need to accompany the wire transfer where such information can be made available to the beneficiary financial institution and appropriate authorities by other means, in which case an account number or a reference number would suffice in order to ensure the possibility of tracing the account back to the originator.\textsuperscript{463} Given the possibility that financial institutions might be lethargic in their cooperation with other financial institutions, a maximum period of three business days is prescribed within which an ordering financial institution must make originator information available. Thus, ordering

\begin{footnotesize}
\footnotesize\textsuperscript{461} Financial Action Task Force (2004B: 18) and Recommendation 16, Financial Action Task Force (2012A: 17). There is a caveat to the requirement of an address, which is that a national identity number, customer identification number or date and place of birth could be provided as a substitute for an actual address. Also, where there are several individual transfers from a single originator sent in a bundle or batch file to a beneficiary in another jurisdiction, full originator information would not be required, so long as the originator’s account number or unique reference number is included, as well as the batch file containing the full originator information. Financial Action Task Force (2004B: 18) and Recommendation 16, Financial Action Task Force (2012A: 17).

\footnotesize\textsuperscript{462} The Wolfsberg Group (2007: 1). The Wolfsberg Group considers it prudent and expedient for all financial institutions to be a member of SWIFT, which could facilitate easier regulations. The Wolfsberg Group (2007: 1).

\end{footnotesize}
financial institutions have the obligation to ensure that wire transfers contain complete originator information.\textsuperscript{464} Intermediary financial institutions, on the other hand, have an obligation to ensure that all originator information accompanying a wire transfer is retained with the relevant transfer. Also, unless not practically possible, intermediary financial institutions have an obligation to ensure that a record of originator information received by the ordering financial institution is kept for a period of five years after the transfer.\textsuperscript{465}

However, there are certain cases where the aforementioned measures on the CDD for wire transfers would not apply. This includes cases where a transaction is carried out using a credit or debit card,\textsuperscript{466} and where the financial institutions involved in the transfer as ordering and beneficiary institutions are one and the same entity, acting on their own behalf.\textsuperscript{467}

In addition to the above measures, financial institutions are enjoined to observe four crucial standards when dealing with wire transfers in general. These include (i) an obligation not to delete or alter information in payment messages or orders for the purpose of avoiding detection of that information by any other financial institution in the process of payment; (ii) the obligation not to use any particular payment messages for the purpose of avoiding

detection of information by any other financial institution in the payment process; (iii) the obligation to cooperate in line with applicable laws with other financial institutions in the payment process when requested to provide information about the parties involved; and (iv) the obligation to urge their respective correspondent banks to observe these principles. 468

4.2.2.1.5 CDD and the risk-based approach

As an overarching principle, the FATF recommends that the CDD measures should be applied on a risk-sensitive basis, taking into account the nature of money laundering, and, or terrorist activities, depending on the relevant context. 469 Thus, in cases where a high risk exists, financial institutions are required to perform enhanced due diligence, whilst, on the other hand, where there is low risk, simplified or reduced CDD measures should be adopted. 470 This method of assessment is known as the risk-based approach. It is one that is largely convened by the Wolfsberg Group, which asserts that institutions should follow a reasonably designed risk-based approach by identifying the criteria to measure potential money laundering risks, with every case to be judged on its own merits. 471

More often than not, for the purpose of making a well-informed risk analysis, three risk criteria are always involved, and they are country risk, customer risk and service risk.472

(i.) Country risk

When determining what constitutes country risk, some factors have to be taken into account, which might help to establish the existence or nonexistence of a potential money laundering risk. Examples are where countries are subject to United Nations-issued embargoes, sanctions or similar measures;473 where countries are recognized by reliable sources as having significant levels of criminal activities such as terrorist activities and corruption,474 or as being generally uncooperative in the global fight against money laundering.

(ii.) Customer risk

The methodology behind determining customer risk is somewhat blurred as it is entirely up to each institution to assess whether a customer poses a higher risk.

---

473 As a necessary addition, where some countries are subject to such sanctions which are not universally recognized, such countries may be given credence by the financial institution as a result of the standing of the issuer and the nature of the measures. The Wolfsberg Group (2006: 4).
474 Transparency International is an organisation that plays a major role in this regard, as it spearheads the global anti-corruption campaign. Also noteworthy is the regulatory practices of the FATF which formerly used to classify countries in the black-list of Non-Cooperative Countries and Territories (NCCTs). However, the FATF has substituted this approach for another which monitors the progress and compliance of each country with present AML standards through its FATF Styled Regional Bodies (FSRBS). The work of other supra-national or institutional bodies such as the World Bank, The Organisation for Economic Co-operation and Development (OECD), the International Monetary Fund and the Egmont Group of Financial Intelligence Units are also essential to making a similar determination.
risk, using its own criteria. The Wolfsberg Group generally identifies the following categories of customers having potentially high money laundering risks: weapons or armament manufacturers and dealers; money service businesses such as currency exchange services, casinos and gambling houses; charities and international non-profit organisations that are largely unregulated; dealers in high-value precious metals such as jewellery, diamonds and precious stones; accounts for the so-called ‘gatekeepers,’ such as lawyers, accountants and other professionals who hold accounts for undisclosed persons; the use of undisclosed intermediaries in the bank-customer relationship; and customers deemed to be Politically Exposed Persons (PEPs). With respect to PEPs, the FATF also emphasizes the importance of following a risk-based system. Recommendation 12 of the FATF Forty Recommendations states that financial institutions should obtain senior management approval prior to establishing business relations with the PEPs, and should take reasonable measures to establish the source of wealth and source of funds, and they must also conduct an enhanced ongoing monitoring of the business relationship with them. Another important type of customer in respect of which banks are urged to adopt the risk-based approach is the respondent bank, in a correspondent banking relationship, which serves as a client to the correspondent bank. As

---

part of the risk indicators to be considered, the respondent bank’s domicile or jurisdiction, its ownership and management structure and its business and customer base should be scrutinised.\textsuperscript{478}

As a general recommendation, higher CDD standards should also be applied to persons (legal and non-legal) who have funds that are sourced from other jurisdictions that are known to have inadequate AML laws, as well as to persons (legal or non-legal) who are known to engage in certain business activities known to be susceptible to money laundering.\textsuperscript{479}

(iii.) Service risk

The third common risk criterion identified by the Wolfsberg Group is service risk. This simply means that financial institutions must assess the services offer in order to identify those services which might pose a higher risk of money laundering in the overall money laundering risks posed.\textsuperscript{480} This is crucial, given the competitive nature of banks today, which drives them to adopt certain innovative services not necessarily offered by other financial institutions, but which pose a high risk for money laundering. Some of these services include international correspondent banking services, services involving banknotes, and precious metal trading and delivery, as well as international private banking services.\textsuperscript{481} The latter is particularly dangerous,

\begin{flushright}
\textsuperscript{478} The Wolfsberg Group (2002: 2).
\textsuperscript{479} The Wolfsberg Group (2002: 4).
\textsuperscript{481} The Wolfsberg Group (2006: 6).
\end{flushright}
as it often uses accounts involving a large measure of confidentiality,\(^{482}\) which can be opened by both legal and non-legal entities.

4.2.2.1.5.1 Specific risks criteria for PVs

There are specific risk criteria for PVs. First, PVs are obliged to consider the type of investors with which they deal, as some may be more regulated than others. Thus, for example, the same CDD measures that apply to financial institutions that are investors should not be different to those applicable to complex and more transparent investors such as trusts and foundations.\(^{483}\)

Also, other than the applicable rationale of country risk, which generally requires that the AML laws of domestic institutions be considered, with PVs, one has to consider that multiple investors from foreign jurisdictions would create a greater risk than investors from the same jurisdiction.\(^{484}\) Moreso, the individual characteristic of the relevant PV and the amounts of any investments are equally important in the general assessment of risk.\(^{485}\)

4.2.2.1.5.2 Risk variables and further measures

In addition to the three categories of risk discussed above, there are certain risk variables that institutions should consider which might further help to assess the risks posed by the customer or transaction, depending on the

\(^{482}\) Basel Committee on Banking Supervision (2001A: 7). This type of service necessitates a great deal of internal control, as it should be open to review by compliance officers and auditors, as well as the involvement of a bank official who is not necessarily part of the private banking relationship. See paragraph 25 of the Basel Committee on Banking Supervision (2001A: 7).


particular case at hand, and eventually determine the kind or level of CDD measures to be taken. Amongst these are: the level of assets to be deposited by the particular customer or the size of the transaction involved; the level of regulation or oversight of the relevant AML legal regime to which the customer is subject; the regularity and length of the business relationship between the customer or client and the financial institution and the client’s familiarity with the existent jurisdiction and its relevant laws and regulations; and a client’s use of certain intermediary corporate vehicles that are fictitious or phantom-like, whose operations are not entirely transparent to the financial institution.\(^{486}\)

After financial institutions have assessed the inherent risks posed by customers or transactions, immediate, albeit reasonable, actions would be required where the customer or transaction poses a high risk of money laundering. Some of the necessary actions required from the financial institution are, firstly, that in such a situation, there should be an increased awareness by the institution of higher risk situations for similar transactions falling within the business lines across the institution.\(^{487}\) Secondly, the financial institution needs to increase its CDD measures or its KYC policies.\(^ {488}\) A necessary consequence is that the financial institution should not easily approve the relevant transactions or establish the requested

\(^{486}\) The Wolfsberg Group (2006: 3).
business relationship with the customer.\textsuperscript{489} Lastly, an increased monitoring of transactions, ongoing controls, and review of relationships are essential steps required of the relevant financial institution.\textsuperscript{490} The aforementioned measures are not necessarily relevant for a particular risk criterion, but are applicable to all three risk criteria, such as country risk, customer risk, and service risk. Each institution has the discretion to attach whatever weight it wants to the three risk criteria.

Financial institutions are also expected to conduct training and development exercises on a regular basis in order to keep employees abreast of their role in the fight against money laundering. Recommendation 18 of the FATF Forty Recommendation requires financial institutions to develop programmes against money laundering and terrorist financing. They must also have an ongoing employee training programme, internal policies, compliant management systems,\textsuperscript{491} efficient screening procedures for prospective employees, as well as a functioning audit system.\textsuperscript{492} Such programmes should bear in mind the level of money laundering risk inherent within the relevant jurisdiction and the size of the relevant financial institution.\textsuperscript{493}

\textsuperscript{489} The Wolfsberg Group (2006: 4).
\textsuperscript{491} Financial Action Task Force (2012A: 18). In order to ensure this, it is recommended that a compliance officer be appointed at the management level to oversee the proper compliance management programmes.
\textsuperscript{493} Financial Action Task Force (2012A: 18). Cf Financial Action Task Force (2003: 22). The role of training in the prevention of money laundering activities is also accentuated by the Wolfsberg Group, which asserts the need for employees of financial institutions to be aware of the legal and regulatory environment in which they operate. See the Wolfsberg Group (2006: 6).
4.2.2.1.5.3 High measure CDDs versus simple measure CDDs

An effective risk-based system requires a judicious study of every case in order to ascertain the right type of CDD measure to be applied. Thus, other than the cases involving high-risk customers identified above, equal consideration should be given to cases that would require simplified CDD measures as well.

In general, simplified CDD measures apply to financial institutions which are themselves customers of another bank, as they too are equally required to observe the same AML standards observed by the service-providing financial institution. Simplified CDD measures would also apply to public companies that are subject to regulatory disclosure requirements and to government departments and enterprises. Such measures apply to certain kinds of transactions such as life insurance policies, insurance policies for pension schemes, or a typical pension scheme providing benefits to employees. These measures also apply regardless of the fact that the customer might be from another jurisdiction. However, this is subject to the knowledge that such other jurisdiction has well-grounded AML policies. Ultimately, the yard-stick remains the suspicion of money laundering or

---

496 This would apply where the annual premium is no more than US $1000 or €1000 or a single premium does not exceed US $2500 or €2500. Financial Action Task Force (2003: 21) and Financial Action Task Force (2012A: 63).
where a higher risk scenario applies, and applicability of simplified CDD measures would be an irrelevant discussion, as in the case of the former.

4.2.2.2 Reporting

Other than having well-entrenched CDD measures as part of the institutional and policy framework of every financial institution, another obligation prescribed by the current AML legal regime is the duty to report suspicious activities. Several questions have to be answered, such as who should report to whom, when and on what grounds.

4.2.2.2.1 Grounds for reporting

Recommendation 20 of the FATF Forty Recommendations states that where a financial institution suspects that funds are derived from criminal activity, or related to terrorist financing, a report must be made immediately to the relevant financial intelligence unit (FIU). Therefore, suspicion that funds relate to criminal activity or its relatedness to terrorist financing is a ground upon which reporting should be done. One important issue to be determined is whether the traditional notion of a crime is sufficient to constitute a criminal activity. This conjures up the topic of predicate crimes for money laundering. Countries are urged to criminalize money laundering on the basis of the United Nations Convention against Illicit Traffic in Narcotic Drugs

---

and Psychotropic Substances, 1988\(^{500}\) (the ‘Vienna Convention’) and the United Nations Convention against Transnational Organized Crime, 2000\(^{501}\) (the ‘Palermo Convention’), and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (the ‘Warsaw Convention’)\(^{502}\) to include “all serious offences, with a view to including the widest range of predicate offences.”\(^{503}\) Thus, by definition, predicate offences include the following:

- a) All offences (i.e. the general approach); or
- b) A threshold linked to a category of serious offences, or to a penalty of imprisonment applicable to the predicate offence, or a list of predicate offences, or a combination of these approaches (i.e. the threshold approach).\(^{504}\)

As regards the general approach, at a minimum, countries are expected to adopt those offences falling under the general canopy of serious offences in their local jurisdictions.\(^{505}\) Given the fact that the threshold approach could be problematic. It touches on one of the most enigmatic problems that the current AML regime is encountering, namely the jurisdictional barriers caused by the lack of universal uniformity of predicate offences. In order to circumvent a foreseeable problem where an offence constitutes a predicate offence in one country but not in another, it is also recommended that predicate offences for money laundering should extend to offences that are committed in another country which are not deemed predicate offences in that

---

\(^{500}\) The Convention was adopted by the General Assembly of the United Nations on the 7\(^{th}\) of December 1987, and it came into force on 11 November 1988.

\(^{501}\) The Convention was adopted by the General Assembly of the United Nations on the 15 November 2000, and came into force on 29 September 2003.

\(^{502}\) Adopted by the Council of Europe on 16 May 2005, and came into force on 1 December 2009.


\(^{505}\) Subject to interpretation, this approach could be problematic. It touches on one of the most enigmatic problems that the current AML regime is encountering, namely the jurisdictional barriers caused by the lack of universal uniformity of predicate offences. In order to circumvent a foreseeable problem where an offence constitutes a predicate offence in one country but not in another, it is also recommended that predicate offences for money laundering should extend to offences that are committed in another country which are not deemed predicate offences in that
evasive, as it is left to the determination of any set threshold, the FATF recommends that ‘serious offences’ should include those offences that are punishable by a maximum penalty of more than a year’s imprisonment, or, alternatively, those countries having a minimum threshold system with a penalty of more than six months imprisonment.\textsuperscript{506} Also, in ascertaining the requisite elements of the relevant predicate offence, particularly the mental element, the FATF urges countries to ensure that the knowledge and intent requirement needed to prove the offence can be inferred from the relevant factual circumstances.\textsuperscript{507} In founding liability for the predicate offences for money laundering, juristic persons are not absolved of possible criminal, civil or administrative liability.\textsuperscript{508}
Therefore, depending on the circumstances of the relevant case, what constitutes a ground upon which reporting is mandatory is a reasonable suspicion that the transaction relates to any form of predicate offence for money laundering. As a cautionary note, given the practice that money launderers often try to boycott a financial institution’s duty to report by often stating that their transactions relate to tax matters, financial institutions still have the obligation to report regardless of the relatedness of a transaction to matters of taxation.\textsuperscript{509} It should be noted that the duty to report suspicious activities also covers transactions relating to correspondent banks\textsuperscript{510} and PVs.\textsuperscript{511}

Also, another ground upon which reporting should be made is when financial and non-financial institutions engage in domestic and international transactions that exceed the prescribed threshold.\textsuperscript{512} As compared to the other ground that requires a risk-sensitive approach in ascertaining whether a transaction relates to a criminal activity, this ground is more straightforward and easily ascertainable, and one can easily determine when it is surpassed.

\textsuperscript{511} The Wolfsberg Group (2002: 5).
\textsuperscript{512} The Wolfsberg Group (2006: 8).
4.2.2.3 The obligation to report

Unlike the CDD standards that are tailor-made for financial institutions, there is a much wider approach adopted as regards the duty to report. By virtue of Recommendation 22(d) of the FATF Forty Recommendations, the FATF also places a duty to report suspicious transactions on non-financial institutions such as lawyers, notaries, other independent legal professionals and accountants who act for a real estate transactions; management of client money and other assets including securities; managing of bank, savings and securities accounts; creating, operating or managing of legal persons or arrangements; buying and selling of business entities; and organizing contributions for the creation, operation or management of companies.\(^\text{513}\)

However, as a caveat, the obligation upon these professionals to report suspicious transactions does not supersede the relevant duty upon such professional to observe professional secrecy or privilege.\(^\text{514}\)

In order to further solidify this requisite duty to report, and according to the safeguard clauses of the FATF’s Recommendation 21, it is expedient to have in place legal, regulatory or administrative provisions to protect whoever files a suspicious transaction report (STR) to the FIU in good faith, in order to shield them from any possible criminal and civil liability that could result

---


\(^{514}\) Every case should be judged on its own merit, and it is up to each jurisdiction to determine the kind of matters falling under professional privilege. In principle, for lawyers, legal privilege covers the information received from or obtained through a client either in performing the task of representing or defending the client in judicial, administrative, arbitratrative or mediation proceedings, or in the course of ascertaining the legal opinion of that client. Financial Action Task Force (2003: 23) and Financial Action Task Force (2012A: 34). Cf Thanki (2011: 301).
from such conduct.\textsuperscript{515} Moreover, the one who files an STR to the relevant FIU is prohibited by law from disclosing such fact to third parties.\textsuperscript{516}

The obligation to file STRs applies also to other non-financial entities or institutions, such as dealers in precious metals and precious stones (when they engage in a cash transaction with a client that is equal to, or exceeds the applicable designated threshold) as well as to trust and company service provider, when in acting on behalf of a client(s), performs one or more of the following functions:

a) Acts as an agent of legal persons;

b) Acts as (or arranges for another person to act as) a director or secretary of accompany, a partner of a partnership, or a similar position in relation to other legal persons;

c) Provides a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;

d) Acts as (or arranges for another person to act as) a trustee of an express trust; and

e) Acts as (or arranges for another person to act as) a nominee shareholder for another person.\textsuperscript{517}


4.2.2.2.3 **To whom reporting should be made**

According to the FATF’s Recommendation 20 and 23, STRs should be filed with the relevant FIU. An FIU is a “central, national agency responsible for receiving (and as permitted, requesting), analyzing and disseminating to the competent authorities, disclosures of financial information: (i) concerning suspected proceeds of crime and potential financing of terrorism, or (ii) required by national legislation or regulation, in order to combat money laundering and terrorism financing.”\(^{518}\) Simply put, an FIU obtains an STR, processes and discloses it to the relevant government authority as part of the general national AML strategy. FIUs are thus able to ensure a rapid exchange of information between law enforcement agencies, financial institutions and prosecutorial authorities, while simultaneously protecting the interests of innocent persons contained in their data. Thus, an FIU is necessary in every jurisdiction, where it should serve as a focal point for the exchange of financial intelligence on money laundering and terrorism in order to foster international cooperation between governments to combat money laundering. FIUs take on different models, depending on the relevant jurisdiction. Some are established alongside existing law enforcement systems,\(^{519}\) while others are created as a single office that receives and analyzes the financial

---


\(^{519}\) This model is known as the Judicial, Law Enforcement, or Hybrid model. See Muller (2007B: 90) and Forget and Hocevar (2004: 44).
information, after which the resulting information is sent to the competent authorities.\footnote{This model is known as the Administrative or Hybrid model. See Muller (2007B: 90) and Forget and Hocevar (2004: 44).}

As regards their functions, FIUs are mandated to receive financial disclosures of STRs filed by both financial institutions and non-financial institutions. In very unique instances, apart from the STR filed, some FIUs query the financial information supplied by financial and non-financial institutions.\footnote{Such situations are quite rare, as it generally depends on the nature or model of the FIU and the nature of the STR report that is filed. FIUs, however, cannot exercise this discretion arbitrarily. The Egmont Group (2004B: 3). Cf Forget and Hocevar (2004: 28).}

The most important function of an FIU is to analyze the information it renders, for the kind of analysis conducted always determines what action that the FIU will take. Several FIUs have developed analytical software to aid them in following trends in money laundering. These are useful to law enforcement agencies.\footnote{The Egmont Group (2004B: 4). Cf Forget and Hocevar (2004: 28).}

FIUs further have a disseminative function. This means that they are obliged to disseminate the financial disclosure that they have obtained. The Egmont Group\footnote{The Egmont Group is an informal body of government receiving agencies that share a common goal of providing a forum to enhance mutual cooperation and to share useful information in detecting and combating money laundering. See discussion in paragraph 4.3.2.4.4 below.} has recommended that FIUs should share the relevant information with domestic authorities, after which they are required to share it with the other FIUs.\footnote{The Egmont Group (2004B: 4).} Caution is advised when disseminating information, and unless
the relevant information obtained by an FIU is publicly available, such information should be treated as strictly confidential and sensitive.\(^{525}\)

4.2.2.3 Regulation and supervision

Another important aspect of the prevention pillar is the concept of regulation and prevention. Adequate oversight is crucial in order to ensure the sustainability of the present AML mechanisms. The approach here requires a constant analysis of the present safeguards in order to block existing loopholes in the system which money launderers would readily exploit for their illicit purposes. The current AML policy on regulation and supervision targets ordinary money laundering vehicles, which are financial and non-financial institutions, and, particularly, their control structure.

The FATF’s Recommendation 26 urges countries to take the necessary legal or regulatory steps to ensure that criminals or their associates are not holders or beneficial owners of a controlling interest or holding management function in a financial institution.\(^ {526}\) As opposed to a system of regular review of licensing of financial institutions, the FATF emphasizes the appropriateness of controlling shareholders in financial institutions with a view to ascertaining their relevance for money laundering purposes.\(^ {527}\) To this end, countries are

---

\(^{525}\) The Egmont Group (2004B: 5).
required to adopt comprehensive guidelines in applying national AML measures.\textsuperscript{528}

Given that non-financial institutions are more prone to becoming effective money laundering vehicles, as they are not as well-defined as financial institutions, there are certain strict regulatory and supervisory measures which are recommended for them. For example, casinos should be licensed, and they should have in place effective controls in order to prevent criminals and their associates from being operators, or being the beneficial owners or from holding a management function of the casino.\textsuperscript{529} The same applies to other categories of designated non-financial businesses and professions such as real estate agents, dealers in precious metals and stones; lawyers, notaries and accountants, as well as trust and company service providers.\textsuperscript{530}

**4.2.2.4 Deterrent measures**

There are several other deterrent measures that should be entrenched domestically in order to ensure the prevention of money laundering activities. According to the FATF’s Recommendation 35, at a minimum, countries are required to ensure that effective, proportionate, and dissuasive sanctions, which could be of a criminal, civil or administrative nature, are available in order to deal with natural or juristic persons who fail to comply with the basic

FATF AML standards.\textsuperscript{531} Thus, each country should have adequate AML laws, particularly as regards the CDD measures and reporting requirements that dictate appropriate sanctions against non-compliant persons or entities. Also, to compliment the discussion on shell banks above,\textsuperscript{532} countries should be expected to exercise prudence by refusing to engage in relationships with shell banks, either by way of establishing them, or by entering into a correspondent banking relationship with them.

\textbf{4.2.3 Pillar 2: Enforcement}

The enforcement pillar of the current AML legal regime tackles the root of the money laundering dilemma. As opposed to the essence of the prevention pillar, the enforcement aspect embodies more proactive measures against money laundering. This pillar entails several important phases such as identifying the predicate offences underlying the crime of money laundering; investigating and prosecuting, as well as confiscating, or, preferably termed, recovering the assets.\textsuperscript{533} The ensuing discussion does not re-visit the notion of predicate offences, as this has been discussed above.\textsuperscript{534} The discussion now focuses on the other elements.

\textsuperscript{532} Paragraph 4.2.2.1.2 supra.
\textsuperscript{533} See Reuter and Truman (2004: 47), where these are distinguished succinctly.
\textsuperscript{534} See paragraph 4.2.2.2.1 supra.
4.2.3.1 The principle of mutual legal assistance: a binding chord

The term ‘mutual legal assistance’ refers to the general cooperation needed between states, either express or implied, which is necessary in the fight against money laundering. The principle of mutual legal assistance is the spine of the current AML legal regime and the vehicle that drives it. Together with the provisions of the Vienna and Palermo Conventions, this principle is also well-enunciated under the Warsaw Convention. International cooperation remains crucial in order to combat the transnational crime of money laundering effectively. This applies especially to the enforcement pillar of the AML legal regime. Mutual legal assistance is crucial to ensuring the effectiveness of investigations, prosecutions and judicial proceedings in money laundering cases. There should be reciprocity between the requesting country and requested country. Mutual legal assistance may be required on an ongoing basis – from the investigation stage to the conviction stage. The kind of assistance required can be wide-ranging, depending on the circumstances of the case at hand.


Mutual legal assistance can be sought for various reasons that may include, but not limited to taking evidence or statements from persons; effecting service of judicial documents; executing searches, seizures and freezing; examining objects and sites; facilitating the voluntary appearance of persons in the requesting country, providing information, evidentiary items and expert evaluations; identifying or tracing proceeds of crime, property, instrumentalities’ or other things for evidentiary purposes, and providing originals or certified copies of relevant documents and records, including
One of the recurring themes of mutual legal assistance is the concept of disclosure. Whenever a country has some information that could assist the authorities of another country in criminal proceedings on money laundering, that country has an obligation to disclose such information to the other country, irrespective of whether the latter country has made a request for such information or not.\(^5\) Also, depending on the nature of the relevant request, disclosure might also mean that the requested country would have to supply certain documents such as copies of government records or information which might not be confidential in nature.\(^6\)

The principle of mutual legal assistance also envisages the scenario where the need exists for persons to be transferred from one country to another in order to provide assistance in on-going proceedings involving the offence of money laundering. The country in which such proceedings are being held may request the presence of a person who is being detained or serving a sentence in the territory of another (the requested country) for several purposes, such as identification, testifying, obtaining evidence for investigations, prosecutions or judicial proceedings.\(^7\) Upon transfer, and unless it is agreed

---

\(^5\) Government, bank, financial, corporate or business records. Article 18 (3) of the Palermo Convention. Cf Article 7(2) of the Vienna Convention and Article 7 of the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime.

\(^6\) Article 18(4) of the Palermo Convention. As a caveat, it should be added that inquiries and criminal proceedings in the country providing such information would be unaffected as a result of transmitting such information. See Article 18(5) of the Palermo Convention. Cf Article 15(1)-(4) Warsaw Convention.

\(^7\) Article 18(29) of the Palermo Convention.

\(^7\) Article 18(10) of the Palermo Convention. Cf Article 7 (18) of the Vienna Convention. However, the free and informed consent of the person for whom transfer is sought is requested, and both countries must be in agreement as regards every term and condition relating to the transfer. Article 18(10)(a)(b) of the Palermo Convention. Cf Article 7(18) of the Vienna Convention and Article 15(1)-(4) of the Warsaw Convention.
upon otherwise, the country to which a person is transferred is obliged to keep the person in custody,\(^{540}\) and is equally obliged to return the person to the custody of the requested country from which the person was transferred.\(^{541}\) The latter would not require an extradition proceeding in effecting the person’s return.\(^{542}\) For the period that the transferred person is within the territory of the requesting country, the time served in that country’s territory is credited to him/her for the service rendered. For example, if the transferred individual was serving a sentence in the requested country prior to his/her transfer, the individual shall receive credit for service for the sentence being served in the territory of the requested country. The rendered service could be deemed an extension of sentence served or, alternatively, it could be deemed as a separate service that could be awarded to his credit. Also, unless otherwise agreed, the person transferred from the requested country should not be prosecuted, detained, or punished in the territory of the requesting country for acts crimes, offences, or convections prior to such person’s departure from the territory of the requested country.\(^{543}\)

Where the person transferred is a witness or an expert witness in respect of crimes and offences committed prior to his/her transfer from the territory of the requested country, such a person would be immune from being

\(^{540}\) Article 18(11)(a) of the Palermo Convention.

\(^{541}\) Article 18(11)(b) of the Palermo Convention.

\(^{542}\) Article 18(11)(c) of the Palermo Convention.

\(^{543}\) Article 18(12) of the Palermo Convention.
prosecuted, detained, and punished for such crimes or offences while he/she is in the territory of the requesting country.\textsuperscript{544}

4.2.3.1.1 \textit{Grounds upon which mutual legal assistance may be refused}

The principle of mutual legal assistance embodies the concept of dual criminality, which serves as a bar to mutual legal assistance. Dual criminality means that the underlying crime or predicate offence for money laundering should be recognized in both countries (i.e. the requesting and requested countries). The concept of dual criminality represents the exception that underscores the blanket obligation to render mutual legal assistance.

Although mutual legal assistance can be refused on this basis, within the context of rendering any other possible assistance to the requesting country, the requested country is not excused from providing any such assistance, provided it is within its capacity to do so.\textsuperscript{545} Overall, it becomes a matter of discretion and the existence or non-existence of the political will on the part of the requested country.

Interestingly, the Vienna Convention does not explicitly use the term ‘dual criminality’. However, an implied reading of the principle comes by way of the provisions of Article 15(c) and (d) of the Convention, which provides that the mutual legal assistance should be refused where the authorities of the requested country would be prohibited by its domestic law from carrying out

\textsuperscript{544} Article 18(27) of the Palermo Convention. Cf Article 7(18) of the Vienna Convention.

\textsuperscript{545} Article 18(9) of the Palermo Convention. Cf Article 7 (15) (c) and (d) of the Vienna Convention where it is elaborated further.
the required action had it been under its jurisdiction, or if such request is contrary to the legal system of the requested country. Although the Palermo Convention also has similar provisions, these provisions only reiterate the underlying rationale that underscores the concept of dual criminality.

In principle, countries may not refuse mutual legal assistance for reasons falling outside the scope of the above. However, it is imperative that the requested country provide reasons for any refusal to render mutual legal assistance. It must also consult with the requesting country in order to consider the option of rendering the assistance subject to such terms and conditions as it may propose. Also, bank secrecy is not a ground upon which one country can refuse mutual legal assistance to another.

---

546 Article 7 (15) (c) of the Vienna Convention. This does not deviate far from the concept of dual criminality, as it can be justified by the underlying rationale. Simply put, a lack of criminality of the action in the domestic law of the requested country factors as an impediment to the ability of the authorities of the requested country from carrying out the requested action.

547 Article 7 (15) (d) of the Vienna Convention. The concept of dual criminality also applies here because the legal system of the requested country might be one that does not entail the criminality of the relevant offence for which extradition might be refused.

548 Article 18 (23) (c) and (d) of the Palermo Convention.

549 Certain other reasons may justify the refusal of mutual legal assistance, for example, if the request might likely prejudice the sovereignty, security or the general interests of the country, or if the request runs contrary to general principles of mutual legal assistance. See Article 18(21) (a) and (b) of the Palermo Convention. Cf Article 7 (15) (c) and (d) of the Vienna Convention.

550 Article 18(23) of the Palermo Convention. Cf Article 7 (16) of the Vienna Convention.

551 Article 18(26) of the Palermo Convention.

4.2.3.1.2 *Formalities*

Reasonableness and exigency are required for the handling of any request for mutual legal assistance.\(^{553}\) The requested country should execute the request as soon as possible, and should be able to inform the requesting country of the status and progress of the request.\(^{554}\) The following are basic elements and essential characteristics of a request for mutual legal assistance:

a) The request must be made in writing;\(^{555}\)

b) The request has to be made in a language that is acceptable to the requested country;\(^{556}\)

c) The identity of the state and its relevant authority making the request must be revealed;\(^{557}\)

d) The subject-matter or nature of the investigation, prosecution and judicial proceeding to which the request relates must be stated clearly;\(^{558}\)

e) The request must state that the investigation shows a *prima facie* evidence, pointing to the existence of a material element of the alleged crime of money laundering within the territory of the requested country;

f) The name and functions of the authority conducting the investigation, prosecutions or judicial proceeding should be stated\(^{559}\)

---


\(^{554}\) Article 18(24) of the Palermo Convention.

\(^{555}\) Article 18(14) of the Palermo Convention. Cf Article 7 (9) of the Vienna Convention.

\(^{556}\) Article 18(14) of the Palermo Convention. Cf Article 7 (9) of the Vienna Convention.

\(^{557}\) Article 18(15)(a) of the Palermo Convention. Cf Article 7 (10)(a) of the Vienna Convention.

\(^{558}\) Article 18(15)(b) of the Palermo Convention. Cf Article 7 (10)(b) of the Vienna Convention.
g) A concise summary of the relevant facts must be provided;  

h) The type of assistance sought must be stated clearly, as well as details of any precise procedure that the requesting country requires from the requested country;  

i) The identity, location and nationality of any concerned individual must be provided,  

j) The purpose for which the mutual legal assistance is sought should be stated for example, the mutual legal assistance could be required for seeking evidence, requesting information or requiring action.

Depending on the nature of the relevant request for mutual legal assistance, the requested country may require other information in addition to what is outlined above, in order to facilitate an effective execution of the request. Also, given that a request for mutual legal assistance has to be properly addressed, one must also determine to whom such a request must be addressed. To this end, countries are obliged to establish central authorities to facilitate requests for mutual legal assistance, which should facilitate the proper execution and transmission of requests received. Whatever

---

559 Article 18(15)(c) of the Palermo Convention. Cf Article 7 (10)(c) of the Vienna Convention. This should be read with point (iii.) above, though a more precise requirement.

560 Article 18(15)(c) of the Palermo Convention. Cf Article 7 (10)(b) of the Vienna Convention. This would not be required for requests relating to service of judicial documents.

561 Article 18(15)(d) of the Palermo Convention. Cf Article 7 (10)(d) of the Vienna Convention.

562 Article 18(15)(e) of the Palermo Convention. Cf Article 7 (10)(e) of the Vienna Convention.

563 Article 18(15)(f) of the Palermo Convention. Cf Article 7 (10)(f) of the Vienna Convention.

564 Article 18 (13) of the Palermo Convention. Cf Article 7(8) of the Vienna Convention. The FATF lays a more practical approach by suggesting that, amongst a host of its other duties, FIUs should be the central authority to which requests for mutual legal assistance should be addressed. See

The Legal Regime for Anti-Cyberlaundering / Daniel Leslie 

194
information is transmitted to the requesting country must not be used arbitrarily but discretely, for the original purpose intended.\textsuperscript{565} Where the information will be needed for another purpose, the prior consent of the requested country is required.\textsuperscript{566}

In addition, the request for mutual legal assistance borders on the very salient principle of state sovereignty, which is an important principle of international law. Countries have the incumbent responsibility to respect the existing laws and principles of others countries, and should not willy-nilly circumvent such laws in order to satisfy private interests. Therefore, the requested country need not step out of the jurisdictional bounds when executing a request for mutual legal assistance. Such a request must be executed in accordance with its domestic law.\textsuperscript{567}

The initiation of requests for mutual legal assistance might be costly. However, ordinary costs should be borne by the requested country.\textsuperscript{568} Depending on the implications of the relevant case, the manner in which any extraordinary costs will be borne, may be determined in the request for mutual legal assistance or a separate agreement.\textsuperscript{569}

\footnotesize

\textsuperscript{566} Article 18(18) of the Palermo Convention. Cf Article 7(13) of the Vienna Convention.
\textsuperscript{567} Article 18(17) of the Palermo Convention. Cf Article 7(3) of the Vienna Convention.
\textsuperscript{568} Article 18(28) of the Palermo Convention. Cf Article 7(19) of the Vienna Convention.
\textsuperscript{569} Article 18(28) of the Palermo Convention. Cf Article 7(19) of the Vienna Convention.
4.2.3.2 Investigation and prosecution of money laundering

The principles of mutual legal assistance are of particular relevance to the investigation and prosecution of money laundering. How could law enforcement agents possibly begin to untie the knot and fathom the evasive trail of money launderers? Where should they start? These are questions with which law enforcers and prosecutors always face. The quality of the investigation conducted for alleged money laundering cases, depending on the nature of the investigative techniques adopted, determines the success of the outcome of the case. In other words, the effective enforcement of AML laws does not stop with the provenance of numerous principles and guidelines, but with the role of key actors such as investigators and prosecutors, who must prove that the proceeds of the crime exist. The Warsaw Convention particularly highlights the significance of the mutual legal assistance with respect to investigations. Other than the general obligation upon states parties to assist one another, the importance of mutual legal assistance especially for requests for information on bank accounts and transactions, for the monitoring of banking transactions and for spontaneous information is also emphasized for the investigations on money laundering operations, conducted by the relevant authorities.

570 Article 16 of the Warsaw Convention.
571 Articles 17 and 18 of the Warsaw Convention.
572 Article 19 of the Warsaw Convention.
573 Article 20 of the Warsaw Convention.
Money launderers are characterized by three main traits: their behaviour, their finances and their business.\textsuperscript{574} It is the task of investigators to gather any, and all relevant data revolving around these traits, for this helps in understanding not just the criminal, but the crime itself.\textsuperscript{575} The overall investigative framework includes the following seven primary steps:\textsuperscript{576} (i) The initial information stage, where law enforcement officers have acquired information on money laundering operations, either from financial sources such as through suspicious transaction reports (STRs) or informants, or through the specified unlawful activity (SUA) sources such as witnesses and informants; (ii) the basis for the investigation, in terms of which assets or transactions are traced or linked to the SUA; (iii) case organisation, which involves developing an investigative plan, and general administration and organisation; (iv) evidence collection; (v) evidence analysis; (vi) presentation which occurs at the trial stage where the money laundering offence is often prosecuted along with the underlying criminal activity, and (vii) the forfeiture stage of the process.\textsuperscript{577}

Given that prosecutors rely on the outcomes of investigations, such outcomes must show that a given transaction is not genuine.\textsuperscript{578} The process of proving the existence of money laundering could entail assembling extensive data

\textsuperscript{574} Put otherwise, they are known by what they like to do (i.e. their behaviour), what they can afford to do (i.e. their finances) and their business (i.e. the financial vehicles they have access to). Turner (2011: 169).
\textsuperscript{575} Cf Article 7 of the Warsaw Convention.
\textsuperscript{576} Madinger (2012: 303).
\textsuperscript{577} See paragraph 4.2.4.4 below.
from different sources or ascertaining the source of the recipient of funds.\textsuperscript{579} Several accounting tools are used to collate the data.\textsuperscript{580} The point of collating relevant data is to identify inherent inconsistencies through an analytical assessment model. Other than relevant data, investigators are required to set their sight on other individuals who might be in a position to either prove or disprove the suspect’s statements and documentations. These associated parties may range from family members to fellow business partners or abstract parties.\textsuperscript{581}

However, the overall investigative task is limited by stringent privacy laws. Gone are the days when one could simply gain access to data by simply unlocking an office cabinet. Nowadays, with the advancement of technology, electronic storage is the standard norm. Ever since its advent in the early 1990s, when internet banking started gaining popularity, the government’s ability to obtain electronic data has become painstakingly difficult.\textsuperscript{582} This

\textsuperscript{579} The very divergent sources of data which investigators often have to scour include the following: Certain documents captured by virtue of a search warrant used for the investigation of the underlying crime, which may have substantive corroborative evidence, or, for the actual money laundering process; certain other documents such as brokerage records, financial records, telephone records, open loans, etc; databases of law enforcement which might include suspicious transaction reports (STRs), currency transaction reports (CTRs), and currency or monetary instrument report (CMIR); databases records from the financial sector such as the suspect’s personal account details, loan accounts, and past account history; certain court filings, such as criminal, civil, and bankruptcy records, together with business entities involved, as well as other public records such as official permits and press articles. Turner (2011: 160). Cf Madinger (2012: 84, 311), and Evans (2000: 208).

\textsuperscript{580} Investigators could make use of different accounting tools such as comparative net worth analysis, income and expense comparison, and bank deposit analysis. These tools are used for the same purpose, which is to ‘compare the claimed activity with the visible record and evaluate value of the missing data, if any.’ Tuner (2011: 161). Cf Madinger (2012: 317).


\textsuperscript{582} At some point the United States government proposed that the idea of online banking should incorporate a feature known as the Clipper chip, which is an 80-bit encryption system meant to ensure that the government would be able to decrypt data if needed. This was, however, met with great opposition from the general public and banking sector. Presently, online banking uses a
problem is further compounded by the advent and increasing use made of electronic payment systems. These systems are the gateway to a very elusive world where data cannot be always traced nor collated successfully.\(^{583}\) This is one facet of cyberlaundering, and one of many investigative problems that come with it.

In order for a prosecution’s case to be admissible in court, the relevant state or territory must determine which jurisdiction is to try the case. Amongst several principles of jurisdiction that exists in international law,\(^ {584}\) given the nature of the money laundering offence, the subjective territoriality principle is the most suitable, as it is based on the rationale that a nation can exercise jurisdiction over a money laundering offence where the property, person, conduct or effects of the conduct fall within its territory.\(^ {585}\) A state may claim such jurisdiction regardless of where the predicate offence might have taken place.\(^ {586}\) Also, given that money laundering is in no way a result offence but a protocol known as the Transport Layer Security (TLS) which does not grant any leeway for third party access. Turner (2011: 161).

---

\(^{583}\) See Chapter 3, paragraph 3.2.2.

\(^{584}\) The main principles of jurisdiction include the nationality principle, in terms of which a nation can prescribe laws with regard to its nationals either inside, or outside its territory; the objective territoriality principle which guarantees jurisdiction because the action had actual or intended effects on the state’s territory without the action occurring in that state; the universality principle which ascribes the notion that any state should assert jurisdiction on the basis that crimes are so serious and threatening to international peace, human rights and integrity that they affect all states and all people, and the passive personality principle, according to which jurisdiction can be established on the basis of the fact that state’s nationals are part of the victims of the relevant crime. Stessen (2000: 199). Cf Koh (2006: 57).


\(^{586}\) Article 6(2) of the Vienna Convention, and Article 6(2) of the Palermo Convention. An important caveat to this principle is the concept of dual criminality which might serve as a bar to founding jurisdiction. Essentially, where a predicate offence is an offence in one country but not in another, the former country cannot punish the offence or offences based on the money laundering offence.
conduct offence, for it is the conduct that incurs criminal liability, the offence of money laundering is deemed to have taken place as soon as a constituent element of the crime is present within that country or territory.\textsuperscript{587}

The prosecution of money laundering itself depends on the nature of the money laundering offence. Other than prosecuting money laundering as a separate offence, very often, money laundering is charged with the underlying predicate offence, which often makes it easier for the prosecutor to prove the alleged money laundering offence. The prosecution can also prove that the accused committed the predicate offence of the alleged money laundering offence (i.e. money laundering of ‘own proceeds’), or all that needs to be proved is that the accused committed the money laundering offence.\textsuperscript{588} The latter applies where money laundering is the only chargeable offence. In principle, the accused person does not have to be convicted of the predicate offence to the relevant money laundering offence. Thus, the prosecution need not prove the conviction, but only the three major elements, namely that a transaction involving property took place; that the property is the proceeds of crime; and that the accused has knowledge of the fact that the property derives from a crime, or, at the very least, has that suspicion.\textsuperscript{589} In the end,

\begin{footnotesize}
\begin{itemize}
  \item \textsuperscript{587} This is because it would be tantamount to governing into another sovereign states’ territory and jurisdiction, which is contrary to the principle of international law.
  \item \textsuperscript{588} Consequently, the crime of money laundering can create multi-jurisdictional claims over the same money laundering scheme, as it is not focused on whether the crime has an effect or result in that territory, but on whether an essential part of the conduct took place there.
  \item \textsuperscript{589} Basel Institute on Governance: Assets recovery Knowledge Centre (2007) ‘Anti-Money Laundering’ an internet article available at <http://www.assetrecovery.org/kc/node/82bce589-7805-}
\end{itemize}
\end{footnotesize}
there must be a domestic AML law upon which the prosecution can ground and found its case. Such legislation is not only essential to the disclosure of information needed by the prosecution, but also needed as a complementary tool to the relevant domestic criminal procedural laws.

It goes without saying that the successful investigation and prosecution of a transnational crime such as money laundering depends on international cooperation. This fact remains a recurring theme which shows the importance of an effective mutual legal assistance.

4.2.3.4 Assets recovery

Assets recovery\textsuperscript{590} comes to play after the deed has been done – where money has been laundered successfully – and the need arises to find a remedy to the situation. Within the framework of the global AML legal regime, given its complexity, the subject of assets recovery comes across as a Herculean task, being always an uphill climb for law enforcers.\textsuperscript{591} Tracing stolen assets is

\textsuperscript{590}The term ‘assets recovery’ is often understood in the plural as also including assets confiscation or assets forfeiture. Assets recovery is a common feature of the two broad but often intertwined areas of money laundering and corruption. As regards the latter, Chapter V of the United Nations Convention against Corruption (which was adopted in terms of the General Assembly Resolution 58/4 of 31 October 2003 and enforced on 15 December 2005) is entirely dedicated to the subject. However, given that corruption is itself a predicate crime for money laundering, the ensuing discussion on assets recovery, although relative to corruption, is not exclusive to it, but generic within the confines of money laundering.

\textsuperscript{591}In spite of its apparent difficulty, history unveils an underlying optimism to the process. For example, by the year 2005, Nigeria had recovered a total of $1.2 billion that had been stolen by its former military dictator, General Sani Abacha. The country was able to recover the stolen funds by requesting assistance from multiple jurisdictions such as Liechtenstein, Switzerland and Jersey, and by designating the Abacha family a criminal organisation, in order to circumvent the need for a conviction. Ivory (2008: 1) and Pieth (2008: 5). Cf Theleskaf and Pereira (2011: 14) and Smith, Pieth and Jorge (2007: 1).
very much akin to finding a needle in a haystack, especially when these assets have been commingled with legitimate funds that have become properly integrated into the legitimate world of commerce. The ensuing discussion assesses the basic principles of assets recovery as entailed in international laws and policies.\textsuperscript{592}

As a general rule, countries have an overall mandate to confiscate proceeds of predicate crimes or property equivalent to the value of such proceeds, or instrumentalities used in, or destined for use in the commission of predicate crimes.\textsuperscript{593} In order to do this, countries are under an obligation to adopt measures which include enacting national laws that ensure the identification, tracing,\textsuperscript{594} freezing/seizure\textsuperscript{595} (hereinafter known as the assets recovery

---

\textsuperscript{592} From a sociological perspective, the issue of assets recovery rests on a very poignant reason. According to the World Bank, an estimate of the cross-border flow of illegal funds is at an estimated $1.6 trillion, half of which is derived from developing economies. The United Nations Office on Drugs and Crime / The World Bank (2007: 9).

\textsuperscript{593} Article 12(1)(a) and (b) of the Palermo Convention and Article 23 of the Warsaw Convention. Cf Article 5(1)(a) of the Vienna Convention.

\textsuperscript{594} Tracing of stolen assets refers to the causal element which must be established between the relevant asset and the relevant criminal activity. This spells much difficulty for law enforcement authorities because usually, they are engrafted into an unfathomable maze of diabolically layered funds. However, very rarely, authorities are saved the trouble of trailing every path that leads to the loot, because evidence might exist that leads directly to the relevant asset. For example, Ferdinand Marcos, the former authoritarian president of the Philippines, had looted billions of dollars from the nations coffers whilst in power from 1965 to 1986, and when this was investigated, authorities were led easily to the funds because of his bank records that were easily accessible at his presidential villa. Asian Development Bank / Organisation for Economic Cooperation and Development (2007: 83). Cf Pieth (2008: 23). Aside from this fact, the cat and mouse system that the process involves, through the STRs that are often filed with financial intelligence units (FIUs), certain necessary connections can also be uncovered.

\textsuperscript{595} Freezing or seizure of stolen assets becomes essential after identification in order to prevent the criminal from further hiding such assets. Beneficiaries of stolen assets would, in most cases, try to make such assets unreachable or untouchable. This is why the notion of confidentiality is key to the concept of assets recovery. This is because criminals who become aware of the operation of authorities who know of the stolen assets are likely to keep moving such assets. Central to this subject is the role of financial institutions, which are key actors in the process. The case of Tommy Suharto, the former President of Indonesia, is an example. In 2002, Suherito’s bank, Banque Nationale de Paris (BNP) Paribas, refused to transfer funds that were beneficially controlled by Suharto, due to the fact the bank had reasonable suspicion of the illegal origins of such funds. King, P
measures) of stolen assets.\textsuperscript{596} However, before assets recovery measures can be initiated, there should be an enabling law on the part of countries that authorizes their relevant authorities to perform such tasks.\textsuperscript{597} Different governmental bodies or agencies are often tasked to perform such duties.\textsuperscript{598} The assets recovery measures will apply to all stolen assets regardless of the fact that they might be:

a) Proceeds of crime that have been transformed or converted, in part or in full, into other property, the value of which is the same as that of such proceeds;\textsuperscript{599}

b) Proceeds of crime that have been intermingled with property acquired from legitimate sources, which shall be liable to confiscation up to the assessed value of the intermingled proceeds;\textsuperscript{600}

c) Income or other benefits derived from proceeds of crime, or from property into which proceeds of crime have been transformed or


\textsuperscript{597} Article 12(6) and Article 5(3) of the Palermo and Vienna Conventions respectively. Cf Article 23-25 of the Warsaw Convention.

\textsuperscript{598} For example, in the United States, the Federal Bureau of Investigation (FBI) and Drug Enforcement Agency (DEA) are specially tasked for this purpose. In the United Kingdom, the Assets recovery Agency (ARA) has this mandate. Also, in South Africa, Nigeria and Colombia, the Office of Serious Economic Offences (OSEO), the Economic and Financial Crimes Commission (EFCC), and the Administrative Securities Department (ASD) are the respective relevant bodies. In its recent report on tracing stolen assets, the Basel Institute on Governance highlighted the significance of information technology, which could help authorities to a great extent with the tracing of stolen assets. See Mulukutlah and Rüegg (2009: 71).

\textsuperscript{599} Article 12(3) of the Palermo Convention.

\textsuperscript{600} Article 12(4) of the Palermo Convention.
converted, or from property with which proceeds of crime has been intermingled, or 
d) Property, equipment or other instrumentalities used in the commission of the relevant predicate offences. 601

As a general rule, the rights of bona fide third parties to the categories of assets above are unaffected, 602 and, in a criminal trial, the onus to prove the lawful origin of the property is on the accused. 603

As a golden thread that runs through the entire money laundering discourse, the concept of mutual legal assistance 604 is a constant. The Palermo and Vienna Conventions both require countries to cooperate in the confiscation of stolen assets. Cooperation often entails exchange of relevant information, and, in certain instances, the extradition of the suspect. 605 In general terms, when a country with jurisdiction to prosecute the crime of money laundering (the requesting country) makes a request for confiscation to another country within whose territory the criminal has placed the stolen assets (the requested country), the latter is obliged to request its authorities to obtain an order of

---

601 Article (12)(1)(b) and Article 5(2) of the Palermo and Vienna Conventions respectively. Cf Article 23 of the Warsaw Convention. This provision is extremely broad, as it encompasses what might otherwise be termed ‘tools’ of the crime. This tool of the crime refers to what has been used to commit the crime. The phrase can be interpreted widely or narrowly, depending on the facts and circumstances of the relevant case, and the relevant laws governing the local jurisdiction.

602 Article 12(8) and Article 5(8) of the Palermo and Vienna Conventions respectively.

603 Article 12(7) and Article 5(7) of the Palermo and Vienna Conventions respectively. However, this provision remains subject to the principles of the relevant domestic legal system. For the greater part, the nature of the legal recovery mechanism that is adopted also plays a major role.

604 Broadly, within the context of money laundering, the concept of mutual legal assistance refers to the multilateral and international cooperation expected from countries in the global fight against money laundering.

605 See Article 16 and 18 of the Palermo Convention, as well as the Article 7 of the Vienna Convention.
confiscation or, alternatively, to give effect to such an order. It is important for the relevant request to be clear and to be accompanied by the relevant information. The request should be written in the national language of the requested country. Depending on the relevant case, the requested country may have to give effect to such a request by adopting the relevant assets recovery measures.

4.2.3.4.1 Methods of confiscation

There are several avenues through which a court judgment can be obtained to freeze or to confiscate the proceeds of crime or property. These are criminal proceedings (in personam), civil proceedings (in personam), civil proceedings against property (in rem), and civil actions for damages in a criminal court (accion civil resarcitoria).

a) Criminal proceedings

Criminal confiscation as an avenue refers to the confiscation of assets based on the conviction of the accused for the crime of money laundering (otherwise called Conviction-Based Asset Forfeiture or ‘CBF’). The fact that this form of confiscation relates to the person tells why it is referred to as

---

606 See Article 13(1) of the Palermo Convention, and Article 7 (3) of the Vienna Convention. In this instance, it should be noted that a request based on mutual legal assistance is often based or governed by an existing treaty between both countries (e.g. the Palermo Convention or the Vienna Convention), or any form of mutual agreement that might exist between them.

607 See discussions in paragraph 4.2.3.1 above.

in personam. In order to ensure an effective criminal confiscation, the confiscation must be based on an enforceable confiscation order. Within the overall context of international assets recovery, as a fundamental rule, a legal basis must exist between countries to justify the act of confiscation. Bilateral or multilateral agreements concluded between countries form such a legal basis, which serves the desired purpose. For example, by virtue of Article 13(2) of the Palermo Convention, in the absence of any other agreement, signatories to the Palermo Convention may use the Convention itself as a legal basis to enforce confiscation orders that have been obtained in a foreign jurisdiction. Hence, signatory countries cannot absolve themselves from this obligation on the basis that there is no arrangement or agreement with the requesting country.

In addition, criminal confiscation contains the principle of dual criminality. As it relates to money laundering, the principle means that the relevant predicate offence must be recognized as a crime by both the requesting and requested countries.

b) Civil proceedings in personam

Another possible method of confiscation is by way of civil proceedings (in personam). Where the proceeds of crime or property are situated in foreign jurisdictions, a civil action can be initiated in foreign courts. Within a local

---

609 The Latin term ‘in personam’ means ‘of relation to the person’ in English.
610 Similarly, as regards the UNCAC, Article 54(1)(A) of the Convention contains a similar provision.
611 See Article 18(9) of the Palermo Convention. Although not stated expressly in the Vienna Convention, a close reading of Article 7(150)(d) expresses the underlying principle.
jurisdiction, private persons and juristic persons can use this avenue as well in order to recover stolen assets.\textsuperscript{612} This method is a better alternative due to the fact that a criminal conviction might be impossible to obtain, whereas in the case of civil action the absence of the defendant would not halt proceedings.\textsuperscript{613} Also, the fact that the burden of proof required in a civil proceeding is proof on balance of probabilities makes it more advantageous, as opposed to criminal proceedings where proof beyond a reasonable doubt is required. In practice, there is no hindrance to instituting civil proceedings together with criminal proceedings, as the latter often complements the former.\textsuperscript{614}

c) Civil proceedings \textit{in rem}

Another very viable method of confiscation is to institute civil proceedings against property (\textit{in rem}), as opposed to instituting the action against the person (\textit{in personam}). Assets can be recovered directly via this means, which is also known as Non-Conviction Based Asset Forfeiture (NCBF). Thus, a civil or criminal conviction against a person is not necessary to

\begin{flushleft}
\textsuperscript{612} Pieth (2008: 76).
\textsuperscript{613} In the case of \textit{The Federal Republic of Nigeria v Joshua Chibi Dariye [2007] EWHC 708 (Ch)} in which the Federal Republic of Nigeria instituted civil proceedings in the English Courts for the recovery of stolen assets by its former state governor, Joshua Dariye, the Court noted that serving a notice to the lawyer of a defendant who is not present, would suffice to justifying the continuance of proceedings. Cf Maton, J (an untitled internet article) ‘Recovery of Assets Case Study: The Dariye Proceedings in the United Kingdom’ Available at the Assets recovery Knowledge Centre <http://www.assetrecovery.org/kc/resources/org.apache.wicket.Application/repo?nid=62ba6a53-c5fb-11dd-b3f1-fd61180437d9> [accessed on 14 December 2011].
\textsuperscript{614} Pieth (2008: 80). For such overlap, see the discussion in point (d.) of the same discussion below. However, this is not to say that, with civil proceedings \textit{in personam}, it would not be possible to freeze assets in order to prevent dispersal; circumvent bank secrecy; to order seizure or search orders, or issue the so-called gag orders to third parties in order to prevent breach of confidential information.
\end{flushleft}
confiscate the proceeds of crime or property. What is required, however, is to prove that the property in question was involved in a criminal activity; hence, guilt is assigned to such property.\footnote{Greenberg, Samuel, Grant and Gray (2009: 33). Cf Pieth (2008: 80).} This is often reflected in the citation of cases such as the “United States of America v. $124,700 in U.S. Currency.”\footnote{United States of America v. $124,700 in U.S. Currency, 05-3295 (8th Cir. 2006). The case concerns civil proceedings \textit{in rem} against the amount of $124,700. Civil proceedings \textit{in rem} against third parties are common in the United States, the United Kingdom and Australia, to name a few.} In such a case the owner of the property bears the onus of proving that the property in question was not involved in the crime.\footnote{Greenberg, Samuel, Grant and Gray (2009: 59).}

\textbf{d) Civil actions for damages}

This is an action that is common in civil law jurisdictions. It is a hybrid between CBF and NCBF. It takes place within the criminal court, and it cannot be initiated unless a concurrent criminal investigation is underway, otherwise referred to as \textit{accion civil resarcitoria}. In essence, it is a civil proceeding in a criminal court. The purpose is primarily to find redress for victims of the criminal offence, as it recognizes damages with monetary compensation.\footnote{Larguire (1965: 687). Cf Pieth (2008: 89).} In the case of international assets recovery, the recoverable damage would be the proceeds of crime or the property. An interesting feature of this option is that the civil action is not dependent on the criminal conviction of the individual. Thus, when the criminal process reaches the trial stage, the civil action continues separately, which often leads to the forfeiture of the property.
4.2.3.4.2 Repatriation

The question of repatriation often crops up after the proceeds of crime have been confiscated. It is important to tread softly in this case. Countries usually have guiding laws or administrative procedures with which to deal with such a case. However, should there be none, as a general rule, countries are under obligation to return such assets to the requesting country. The underlying rationale for this principle is to ameliorate the consequences of the criminal act by compensating the victims of the crime or returning the proceeds or property to their legitimate owners.\footnote{Article 14(2) of the Palermo Convention and Article 8 of the Vienna Convention, respectively.} In unique instances, there might be supplementary agreements or arrangements between the relevant countries, which allow the requested country to share in the confiscated assets or utilize the funds in its fight against money laundering.\footnote{The World Bank plays a crucial role here as a neutral third party that ensures that the assets are channelled into development efforts and needful sectors such as education and health.} Within the broad framework of repatriation, the claim of legitimate third parties has to be taken into account.

In general, assets recovery is one aspect of the global AML legal regime, and one that requires continuous capacity development and training efforts, especially when there is a need to pursue assets in countries lacking the adequate institutional framework for assets recovery.\footnote{Currently, several international organisations have diverted attention to addressing this challenge. Some of these are the United Nations Office on Drugs and Crime (UNODC); the World Bank (with its StAR initiative) and the International Centre for Assets recovery (a Centre for Assets recovery at the Basel Institute on Governance in Basel, Switzerland).} Such continuous efforts help to solidify the compliance, prevention and enforcement pillars upon which the current AML legal regime rests.
4.2.4 Pillar 3: Compliance

Unlike in the past, the present AML legal regime places a heavy emphasis on the notion of compliance. It is one thing to have in place a myriad of AML laws and policies, but another to ensure that they are put into effect. This study identifies the issue of compliance as the principal third pillar of the modern AML legal regime, without which the other two pillars would be merely theoretical. Compliance represents the binding chord connecting all pillars. Parties who have a duty to comply are today paying a hefty price for failing to comply with these laws. The importance of this rationale is stressed extensively in international norms and policies. In its Recommendations, the FATF identifies certain measures to facilitate compliance with established laws and standards. This involves a proactive involvement of various state actors, such as effective Financial Intelligence Units (FIUs); adequately empowered law enforcement bodies and competent authorities, which means being properly endowed with the requisite financial, human and technical resources; competent supervisors who can ensure that the relevant organisation and institutions are able to

---


comply with the set laws and standards, as well as establishing set measures to ensure that legal professionals are not exploited for laundering purposes.

Although the issue of compliance is peculiar to the aforementioned parties, it is one that really does echoes generally. There is an obligation to comply and to ensure compliance. Thus, this obligation is two-fold: on the one hand is the targeted group, which are persons and entities with the duty to comply with set AML laws and policies, such as financial institutions, their clients and beneficial owners; mutual funds and pooled investment vehicles such as hedge funds, private equity funds, unit investment trusts, corporations, trusts and partnerships, and other designated non financial businesses such as lawyers, notaries, accountants, dealers in precious metals and stones, and real estate agents. On the other hand, there are the so-called guardians that are meant to ensure compliance, such as governments and their respective agencies. Apart from the individualised efforts on the part of governments to ensure compliance, which mostly boils down to the existence of non-existence of political will, or lack of adequate means, several international

---

627 See discussion in paragraph 4.2.3.1.1 below.
628 See discussion in paragraph 4.2.3.1.3 below.
629 See discussion in paragraph 4.2.3.1.1 (d) below.
agencies, institutions and organisations have also made attempts at ensuring effective compliance.\(^{630}\)

As it pertains to cyberlaundering, the two distinct arms of compliance are better understood in subsequent discussions in the chapter that follows.\(^{631}\)

**PART II**

4.3 THE ACL LEGAL REGIME: A SURVEY OF EXISTING RELEVANT LAWS, POLICIES AND INITIATIVES

4.3.1 General

Cyberlaundering is current and adapts to technological advancement. This compounds the already complex problem of money laundering.\(^{632}\) It is important to reiterate that the notion of cyberlaundering grows out of the traditional concept of money laundering, which is why an understanding of the current legal regime against money laundering is crucial for the proper comprehension of the existing legal regime against cyberlaundering. This part of the study is therefore an extension of the previous part. This section studies the legal strategies currently in place to combat cyberlaundering. However, a concrete and well-structured legal regime has yet to be established to combat cyberlaundering. This does not mean that the current AML legal regime is completely ineffective against cyberlaundering; it is only inadequate. This section identifies some attempts against cyberlaundering made at both the

---

\(^{630}\) Amongst others, in the forefront are the World Bank, the Basel Institute on Governance, the FATF and the FATF-Styled Regional Bodies, the Egmont Group and the Wolfsberg Group of Banks.

\(^{631}\) See Chapter 5, paragraph 5.6.

\(^{632}\) See Chapter 3 for a discussion of the concept of cyberlaundering.
national and international levels. The section also focuses on one key aspect of the compliance pillar of money laundering, which has to do with parties (i.e. ‘guardians’) bearing the obligation to ensure compliance with AML laws – which in this case would be anti-cyberlaundering (ACL) laws.

4.3.2 Present international legal framework against cyberlaundering

4.3.2.1 General

Cyberlaundering is still a very evasive phenomenon which, until now, has not been properly conceptualized. This is one of the principal challenges facing its regulation and control, for it is a phenomenon which has proven extremely difficult to grasp, let alone one with which to come to grips. In fact, at present there is no international ACL legal regime. This section tries to unravel and explore some related issues that justify the rationale behind this study’s attempt to establish an appropriate ACL legal framework. It will look at the relatedness of the current ACL legal regime to the AML legal regime, and at the link between international cybercrime laws and cyberlaundering. This section also discusses how much of cyberlaundering is known internationally, and what attempts have been made to remedy it.

4.3.2.2 The relationship between the AML and ACL legal regimes

The relationship between the current AML and ACL legal regimes is traceable to the roots of both concepts. It has been said that cyberlaundering is not a separate crime from money laundering, irrespective of its deep
rootedness in cybercrime. Thus, proceeding from the standpoint that cyberlaundering is indeed money laundering that appears in another form, it goes without saying that the legal basis governing money laundering is the same as that for cyberlaundering. Upon close consideration, it also becomes apparent that an analysis of the present legal regime or construct for money laundering is tantamount to that of cyberlaundering. However, there is a caveat to this rationale, being that the current legal framework for money laundering is not sufficient to gauge and contain the dilemma of cyberlaundering. This is because there are presently no AML laws that directly cater for the problem. The fact that the present AML laws are inadequate, distinguishes the present AML legal regime from the ACL legal regime which this study proposes. The latter builds on the former, and in essence, justifies the rationale for this study.

4.3.2.3 Cyberlaundering and the Council of Europe Convention on Cybercrime

Given that there are currently no laws, rules or regulations governing cyberlaundering in the international sphere, the question is whether

633 See discussion in Chapter 3, paragraph 3.2.3.
634 The following chapters set out the legal ramification and legal construction for the prosecution of cyberlaundering. They also outline possible solutions to the problem. By so doing, this study attempts to establish a concrete ACL regime for the problem.
635 One might find some laws that touch on some aspects of cyberlaundering, such as electronic payment systems, for example. For instance, as regards electronic payment systems, there is the Council of Europe Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions, adopted by the Parliamentary Assembly on 16 September 2009 and which came into force on 30 October 2009. This is discussed further in Chapter 5, paragraph 5.5.2.3.2.
cyberlaundering can be regulated under the first and only international cybercrime convention - the Council of Europe Convention on Cybercrime (the ‘Budapest Convention’). The Convention came about as a response to the disharmony of cybercrime laws across various jurisdictions in Europe. This was an obstacle to the international prosecution of cybercrime offences across European countries. The Budapest Convention aims to harmonize national cybercrime laws and to improve investigative techniques, with the principal objective of fostering cooperation amongst states parties. The Budapest Convention does not expressly define cybercrime. This is due to the fact that the Convention tries to foster harmony in cybercrime laws by abstaining from prescribing a definition, and not propounding one which might be restrictive in nature. Rather, the Convention sets out measures to be taken at the national level to combat cybercrime. It describes certain types of conduct which national authorities should criminalize, such as offences against the confidentiality, integrity and availability of computer data and systems; offences related to the infringement of copyright and related

---

636 The Convention was drawn up by the Council of Europe in Strasbourg, with participation of the Council of Europe, observer states Japan, Canada and China. The Convention was adopted by the Committee of the Ministers of the Council of Europe at its 109th session on 8 November 2001. On 23 November 2003, it was open for signature in Budapest, and on 1 July 2004, it came into force. As at 26 September 2012, the Convention had been ratified by 37 states parties. For more information see the Treaties Office of the Council of Europe at <http://conventions.coe.int/> [accessed on 26 September 2012].

637 On 7 November 2002, the Council of Europe Committee of Ministers adopted an additional protocol to the Convention (Additional Protocol to the Convention) which came into force on 1 March 2006. In addition to the cybercrime offences set out in the Convention, the Protocol criminalises the dissemination of xenophobic or racist materials through computer systems.

638 In addition to the conduct to be criminalized, measures are also put forth for ancillary or incidental liability. See Title 5 (Article 11 to 13) of the Convention.

639 See Title 1 (Articles 2 to 6) of the Convention.
rights;\textsuperscript{640} computer-related offences such as computer-related forgery and fraud,\textsuperscript{641} and content-related offences such as offences related to child pornography.\textsuperscript{642} The Convention says nothing about the conduct of cyberlaundering.\textsuperscript{643} This is evidence that cyberlaundering does not fit solely into the frame of cybercrime.

However, this should not be construed to mean that the Convention bears no relation to the concept of cyberlaundering. In fact, it does. Viewed from the ambit of predicate offences, all categories of offences listed under the Convention can be predicate offences for cyberlaundering, together with a list of other serious offences.\textsuperscript{644} The technological dimension that cyberlaundering has with other kinds cybercrimes makes it much easier for these cybercrimes to become predicate offences for it, as it is only logical for illicit funds derived from the internet to be laundered through it. Many cyberlaundering activities fly under the radar simply because the concept of cyberlaundering is still not understood by investigators, and when other comprehensible cyber criminal activities are involved, as is often the case,

\textsuperscript{640} See Title 4 (Article 10) of the Convention.
\textsuperscript{641} See Title 2 (Article 7 and 8) of the Convention.
\textsuperscript{642} See Title 3 (Article 9) of the Convention.
\textsuperscript{643} The conduct of cyberlaundering manifests through its basic elements, which are the presence of a computer, an activity and illegal funds (i.e. \textit{actus reus} elements) together with knowledge of the illegality of the funds, and its associative intention (i.e. \textit{mens rea} element). See Chapter 3, paragraph 3.2.4.
\textsuperscript{644} Chapter 6 below, which deals with the prosecution of cyberlaundering, dwells extensively on explaining this link. For a detailed discussion on predicate offences of money laundering, see Chapter 2, paragraph 2.2.1 above.
investigators and prosecutors only focus on those cybercrimes, ignoring the elusive manifestations of cyberlaundering.\textsuperscript{645}

Another upshot of the Budapest Convention is that it does not have universal application. Although being a European Convention which most European countries have ratified, only very few other non-European countries are parties to it.\textsuperscript{646} The fact that the Convention is the only major international instrument, which itself does not have a global reach, shows the gross inadequacy of laws, and as regards cyberlaundering, it shows the need to found a concrete ACL legal regime.

\textbf{4.3.2.4 Present attempts to regulate cyberlaundering through international policies}

There have been certain efforts undertaken by certain non-governmental organizations and international private sector entities to understand the concept of cyberlaundering. These take the form of policies and recommendations. Yet, a pedantic interpretation of these laws, policies and recommendations, would not amount to a ‘legal framework’ \textit{per se}, given that they lean more to the side of soft laws, as opposed to hard laws.\textsuperscript{647} However, as alluded to earlier,\textsuperscript{648} most of these laws, practices and recommendations (i.e. soft laws) have become legally recognized standards which have been

\begin{itemize}
\item \textsuperscript{645} Cf discussion in Chapter 6, paragraph 6.5.
\item \textsuperscript{646} These include Canada, Japan, South Africa and the US.
\item \textsuperscript{647} Within the ambit of international law, hard law is a binding legal instrument that gives rights to and imposes obligations on parties upon which it is binding. Cassese (2005: 160). Cf Evans (2010: 71) and Shaw (2003: 67).
\item \textsuperscript{648} See paragraph 4.2.1 above.
\end{itemize}
transplanted into the domestic legal systems of most countries. Given the interwoven nature of both the AML and ACL legal regimes, and the latter being practically not yet existent, it is thus important to consider the present attempts made at combating cyberlaundering in the international sphere. Although the conceptual phrasing - ‘cyberlaundering’ - is not found in these soft laws, reference is made to some of its operations and manifestations. Much of these attempts have been undertaken by inter-governmental organisations and private state actors such as the Wolfsberg Group, the Basel Committee on Banking Supervision, the FATF, the World Bank, the Egmont Group, and, for the enforcement ambit, the International Police Organisation (‘Interpol’).

4.3.2.4.1 The FATF

In Recommendation 15 of its Recommendations (‘International Standards on Combatting Money Laundering and The Financing of Terrorism and Proliferation’), the FATF preempts the danger of cyberlaundering. It cautions financial institutions to pay special attention to money laundering threats that may arise from new and developing technologies which might favour anonymity. The FATF also warns that these new technologies can be used for money laundering schemes, and it highlights those risks associated with non-face-to-face business transactions. With the increasing manifestation of these threats, the FATF has tried to follow these trends closely. This

---

resulted in its 2006 New Payment Method Report\textsuperscript{651} and its 2010 Report on Money Laundering Using New Payment Methods.\textsuperscript{652} From several case studies conducted, the latter report identifies the laundering capabilities of New Payment Systems (NPSs), such as prepaid cards and internet payment systems. Some these case studies indicate how illicit funds, of both high and low values, are being laundered using NPSs.\textsuperscript{653} The FATF elucidates the fact that certain key features of modern technology have helped to foster the attractiveness of NPSs for money laundering purposes. One of these is the anonymity of the internet. Others are the high utility of funds, as well the global access via automatic teller machines (ATMs).\textsuperscript{654} Given its currency, there is presently no uniformity across jurisdictions on the classifications and regulatory measures for such NPSs. In addition, Special Recommendation VII (SR VII) of the FATF’s Special Recommendations on Terrorist Financing\textsuperscript{655} sets out measures to prevent money laundering and terrorist financing possibilities by way of wire transfers, which is incidental to the problem of online banking. These challenges, loopholes and proposals put forward by the FATF are discussed under solutions to the cyberlaundering problem in Chapter 5 of this study.

\textsuperscript{652} Financial Action Task Force (2010D: 3).
\textsuperscript{654} Financial Action Task Force (2010D: 7). These are salient features of money laundering that are discussed in detail in Chapter 3 of this research.
4.3.2.4.2 The Wolfsberg Group

In October 2011, the Wolfsberg Group issued a guidance paper on the risks of prepaid and stored value cards.\textsuperscript{656} This comes with the advent of cyberlaundering, and the steady migration from a paper-based payment system to the now predominant electronic payment system. The latter is largely monopolized by the non-bank service providers (NBSPs) who do not necessarily fit the respected frame of a financial institution that is typically controlled and regulated.\textsuperscript{657} NBSPs are often private entities (i.e. companies or corporations) that distribute electronic payment instruments such as smart cards, prepaid or stored value cards. Although NBSPs are often badly tainted for their predisposition to cyberlaundering, some have played more positive roles, such as serving as outsourcing agents for financial institutions, by providing certain specialist services to financial institutions, or, in their capacity as financial service providers, acting as competitors to financial institutions.\textsuperscript{658} Given the fact that NBSPs also need to be controlled, the Wolfsberg Group follows a risk-based approach in prescribing control measures for the use of prepaid and stored value cards. This represents a good promise of what should be expected in the near future.

\textsuperscript{656} The principles and recommendations outlined in this guidance paper are discussed further in Chapter 5.

\textsuperscript{657} With growing awareness of the dangers they harbour, more and more of these NBSPs are becoming regulated. While some may be regulated to a lower standard as banks, some are regulated to the same standard, or only regulated for business in a specific country. The Wolfsberg Group (2011: 2).

\textsuperscript{658} The Wolfsberg Group (2011: 2).
4.3.2.4.3 The Basel Committee on Banking Supervision

The Basel Committee on Banking Supervision addresses the issue of cyberlaundering from the angle of online banking, which proves problematic because for banks that are solely internet-based, without an actual physical presence anywhere, customers are not subjected to the same rigid verification process that a terrestrial bank would ordinarily use for prospective clients.\(^{659}\) With the advent of telephone banking, which is now complementary to online banking, the matter is not remedied. Although the possibility exists that an independent third party could readily conduct such identification and verification, there are still doubts about the veracity and credibility of such third party or agency. The proposals made by the Basel Committee are analysed critically in Chapter 5 which considers how cyberlaundering can be regulated.\(^{660}\)

4.3.2.4.4 The Egmont Group

The effort made by the Egmont Group is a more practical one. It is meant to empower the FIUs. Given the technological prowess of cyberlaunderers who are able to exploit some technological avenues for their illicit operations, and in order to foster the work of the FIUs, the Egmont Group took the initiative of establishing an Information Technology Working Group (ITWG). In October 2010, the ITWG and the International Monetary Fund (IMF) held a workshop entitled the IMF-Egmont Group IT Workshop, which assessed best

---

\(^{659}\) Basel Committee on Banking Supervision (2001A: 9).

\(^{660}\) Cf discussion in Chapter 5, paragraph 5.5.2.1.1.
practices in IT developments within FIUs. It was held in Brazil, and 15 countries in Central and Southern America participated.\footnote{The Egmont Group (2011: 25).} This was a crucial step forward, especially given the fact that FIUs serve as an intelligence centre where information on money laundering operations are collated, exchanged and processed. With an increase in its technological capabilities, cyberlaundering operations would not easily elude FIUs, for they would be detected with relative ease.\footnote{On a complementary note, the Egmont Group also pilots certain other IT innovations. An example is a recently completed development paper entitled ‘FIU IT System Maturity Model’ (FISMM), which is a hightech self-evaluation tool meant to aid the operations of FIUs. Also, there is a system called Data Standards Set which allows FIUs to use uniform documents and fields when requesting information from other FIUs. The Egmont Group (2011: 25).}

4.3.2.1.5 The World Bank

The World Bank, in conjunction with the IMF, has a more radical approach towards fighting cyberlaundering. Recently, it introduced an innovative program known as the Financial Sector Assessment Program (FSAPs),\footnote{See <http://www.imf.org/about/projects/worldbank> [accessed on 13 August 2010].} which is meant as a solution to the problems caused by electronic payment systems, particularly as regards the non-bank issuer model and the peer-to-peer model.\footnote{See discussion in Chapter 3, paragraphs 3.2.2.3 and 3.2.2.4. Cf Kellerman (2004: 3).} The World Bank identifies threats posed by the use of such systems. It has also launched the Global Systems Mapping Project in order to monitor the flow or movement of money in complex financial systems.\footnote{Kellerman (2004: 16).} In the long run, this will enable governments and their respective
local authorities to better safeguard their monetary policies from threats such as cyberlaundering.\textsuperscript{666}

In addition to these initiatives, the Bank outlines the need for the establishment of cyber-threat analysis centres across all financial institutions, either in a national or international jurisdiction. Much like the functions of FIUs, the cyber-threat analysis centres would enable financial institutions to share intelligence on cyber-threats with other financial institutions. While studies show that financial institutions already have such system in place, it takes uniformity to work, as such cyber-threat centres need to be properly networked to work. In essence, all financial institutions must have one such cyber-threat centre in order for realize its advantages. In the US, there is a similar service known as the Financial Services Information Sharing and Analysis Centre (ISAC). The ISAC functions like the proposed cyber-threat centre. Although it is an internet-based third party service provider, it gives alerts upon detection of threats in banking transactions, and serves as a real time information sharing system.\textsuperscript{667} The rationale here is simply to coordinate and harmonize cyber entities against cyberlaundering. The significance of cyber forensics should hence not be underestimated, especially within financial institutions, given that the ability to detect and preserve the minutest electronic evidence is the minimum required in order to contain the problem of cyberlaundering adequately.

\textsuperscript{666} Kellerman (2004: 16).
4.3.2.4.6 International Police Organisation

The International Police Organisation (Interpol)\textsuperscript{668} has a mandate to foster operational support in the global challenge of fighting crime by ensuring cooperation between police from various jurisdictions. This is to ensure the enforcement of laws and the prevention crimes.\textsuperscript{669} For the enforcement aspect of the global ACL legal regime, Interpol is key. Interpol exhibits characteristics of an adequately equipped organisation with the right resources to fight cyberlaundering.

In the fight against cybercrime in the international sphere, Interpol plays a key role. It collects, preserve, analyzes, and shares information on cybercrime with all its member states.\textsuperscript{670} Interpol has since spearheaded some initiatives geared towards this purpose, such as the setting up of the National Central Reference Point Network. The latter is a designated network of investigators in national cybercrime units, who are meant to be on the alert and to identify imminent threats, and to facilitate cybercrime investigations.\textsuperscript{671} Interpol also established the Interpol Working Parties on IT Crime, which is a working group that continually works on developing strategies on the latest cybercrime methods, and it also conducts an International Cybercrime

\begin{itemize}
\item Interpol is the world’s largest police organisation. It is comprised of 190 member states. It has its General Secretariat in Lyon, France, with other several regional offices around the world. It operates 24 hours a day, 365 days in a year. For more about the organisation, see <http://www.interpol.int/Crime-areas/> [accessed on 11 February 2011].
\item Interpol (an undated webpage) ‘About Us’ available at <http://www.interpol.int/about/> [accessed on 11 February 2011].
\end{itemize}
Conference every two years. This conference creates a forum for the exchange of knowledge and expertise in fighting cybercrime.\textsuperscript{672}

In the next chapter, these initiatives are considered more closely as they are pertinent to cyberlaundering.

\section*{4.3.3 Present national legal framework for cyberlaundering}

\subsection*{4.3.3.1 General}

An international canopy for the ACL legal regime would only be as strong as the tent poles erected locally. Apart from a consideration of the present ACL legal regime on the international plane, it is also imperative to examine the situation at the national level. This section samples four different countries through which to juxtapose efforts made locally in the ACL legal campaign. These are Germany, the UK, India and the US. These countries are selected because of their level of awareness of the crimes of money laundering and cybercrime, as well as their vulnerability to it. This section seeks to create an understanding of the situation of the ACL legal regime in local jurisdictions by analyzing those relevant laws against money laundering and cybercrime that might or might not pertain to cyberlaundering. This exercise is crucial in order to identify the common issues that exist amongst these countries, given that an identification of the basic issues is extremely crucial to proposing a solution. To this end, the relevant cybercrime and money laundering laws of the aforementioned countries are considered closely.

4.3.3.2 Germany

Money laundering is an offence regulated under section 261 of the German Criminal Code of 1998 (Strafgesetzbuch – StGB), the Anti-Money Laundering (AML) Act of 2008 (Gesetz zur Ergänzung der Bekämpfung der Geldwäsche und der Terrorismusfinanzierung - GwBekErgG) as well as the Banking Act of 1998 (Gesetz über das Kreditwesen Kreditwesengesetz - KWG).

Section 261 of the German Criminal Code forms the basis of the country’s AML legal regime. Liability for the crime of money laundering can be founded if the constituent elements of the crime of money laundering are satisfied, as set forth in the section. The elements contained therein, however, are elements of the traditional concept of money laundering which, by way of implication, exclude cyberlaundering, given that its constituent elements are not the same, even though the latter is embedded in the former. Consequently, the concept of cyberlaundering is not contained in the money laundering provisions outlined in section 261 of the German Criminal Code.

---

673 Other related provisions of the Criminal Code include sections 257, 258, 259, 260, 260(a) and 262.
675 Otherwise known as the ‘Kreditwesengesetz in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2776).’
676 The elements of the crime of money laundering are discussed in Chapter 3, paragraph 3.2.4.
677 For a detailed discussion on the relationship between money laundering and cyberlaundering, see Chapter 3, paragraph 3.2.3.
The AML Act of 2008 created Germany’s financial intelligence unit (FIU) within the Federal Criminal Police Office (Bundeskriminalamt - BKA). The Act also provides detailed customer due diligence (CDD) obligations on financial institutions, and also requires them to submit suspicious transaction reports (STRs) to the competent authorities. The AML Act does not contain provisions regulating cyberlaundering.

The Banking Act of 1998, however, is relevant to the regulation of cyberlaundering. Article 2 of the Act requires prepaid service providers to observe KYC principles when conducting business with customers. This means that customers, amongst other requirements set out, would need to provide proof of their identities to prepaid service providers. Also, under the same provision, prepaid service providers are required to conduct thorough KYC procedures and file STRs where the prepaid or smart card in question is topped with amounts that exceed €100.

The German laws dealing with cybercrime include the Freedom of Information Act of 2005 (Informationsfreiheitsgesetz) the Federal Data Protection Act of 2001 (Bundesdatenschutzgesetz - BDSG) and the Telecommunications Act of 2004 (Telekommunikationsgesetz - TKG). A regulatory framework for cybercrime is also outlined in the German Criminal...
Code, which governs aspects of cybercrime such as cyberfraud, data tampering, crimes against the computer, violation of privacy, data espionage, and phishing. None of these laws describes the conduct of cyberlaundering expressly. At the moment, there are no proactive steps being taken against cyberlaundering in Germany. The exception is Article 2 of the Banking Act. But the German police continue to fight money laundering and cybercrime.

4.3.3.3 United Kingdom

The UK operates a very strong AML legal regime. Its AML legal regime is governed by the Terrorism Act 2000, the Anti-Terrorism, Crime and Security Act of 2001, the Serious Organized Crime and Police Act 2005, the Money Laundering Regulations 2007 and the Proceeds of Crime Act 2002. The latter is the primary AML legislation in the UK, and it evidences the exceedingly wide nature of the UK AML laws. The far-reaching nature of the UK’s AML laws is its most distinguishing characteristic. For instance,
handling or dealing with the proceeds of a criminal activity, be it represented in money or assets,\textsuperscript{693} incurs liability of the accused. However, in spite of the wide breadth of these laws, the AML laws of the UK do not cover the notion of cyberlaundering. Juxtaposed to the UK’s cybercrime laws, are other laws meant to fight cybercrime. These are the Computer Misuse Act of 1990,\textsuperscript{694} the Privacy and Electronic Communications (EC Directive) Regulations of 2003,\textsuperscript{695} the Police and Justice Act of 2006,\textsuperscript{696} and the Serious Crime Act of 2007.\textsuperscript{697} The conduct that criminalizes cybercrime does not fit that for cyberlaundering.

In February 2012, the UK renewed its campaign against cybercrime by establishing regional cybercrime hubs across the UK. These are meant to help in the identification of cyber threats.\textsuperscript{698} Perhaps by having effective detective mechanisms, the problem of cyberlaundering will become more visible, which is a first step to combating it effectively.

\textsuperscript{693}Money laundering in the UK is deemed an ‘acquisitive crime,’ one which merely requires the accused person to have obtained a pecuniary advantage. As gleaned from its AML laws, the money laundering offences in the UK are not confined to the proceeds of serious crimes. There are also no monetary limits, and it is not a requirement that there be a money laundering design or purpose to an action for it amount to a money laundering offence. See the International Monetary Fund (2011: 7). Cf Padfield (2004: 270).

\textsuperscript{694}Chapter 18, Act of 1990.

\textsuperscript{695}Act No. 2426 of 2003.

\textsuperscript{696}Chapter 48, Act of 2006.

\textsuperscript{697}Chapter 27, Act of 2007.

\textsuperscript{698}These units which will help battle online threats were established in Yorkshire and the Humber, the Northwest and the East Midlands. See Evans, S (2012) ‘UK launches Regional Cybercrime Hub’ available at <http://security.cronline.com/news/uk-launches-regional-cybercrime-hubs-100212> [accessed on 13 February 2012].
4.3.3.4 India

The AML legal regime in India is governed primarily by the Prevention of Money Laundering Act, 2002. As the title suggests, this Act has provisions that reflect the prevention pillar of the present AML legal regime. It lays down very stringent CDD measures for financial institutions in particular. This law does not contain provisions that regulate cyberlaundering. On the other hand, cybercrime in India is regulated in two ways. Criminal activities of a traditional nature, such as theft, forgery, fraud, defamation, amongst others, are regulated under the Indian Penal Code. Other types of cybercrimes, such as computer-related crimes are dealt with under the Information Technology Act 2000. The latter also addresses the legal recognition of electronic documents and legal recognition of digital signatures. These laws, too, only cater for crimes under the cybercrime family. They exclude cyberlaundering.

The Indian Income Tax Department is the main AML law enforcement body in the country for enforcing AML laws. This department and the Financial Intelligence Unit (FIU) of the Indian Police Service are yet to come to grips with this growing phenomenon of cyberlaundering.

700 Act No. 45 of 1860.
701 Act No. 21 of 2000.
4.3.3.5 United States

The US is a good example of a local jurisdiction that has highly fortified preventive and enforcement strategies against cybercrime and money laundering. The reality of cyber criminality in the US prompts its dedication to fighting the problem. This speaks to why the US is one of only three non-European countries that has signed the Budapest Convention, and one of just two that has ratified it.\footnote{The US signed the Budapest Convention on 23 November 2001; it ratified it on 29 September 2006, and enforced it on 1 January 2007. Japan signed the Convention on 23 November 2001, and ratified it on 3 July 2012. As at time of writing, South Africa and Canada are the only other countries that have signed the Convention, but are yet to ratify it.}\footnote{Earlier citation at footnote 3 above.} Much of the provisions of the Convention have been domesticated into Title 18 of the United States Code,\footnote{Crimes and Criminal Procedure Act of 1948, 18 United States Code 645; 683.} which is the criminal and penal code of the federal government of the US. The latter deals with federal crime and procedure.

The US does not have laws that cater for cyberlaundering explicitly. However, the crime of money laundering is a federal offence in the US and is regulated under a slew of anti-money laundering laws, such as the Bank Secrecy Act,\footnote{Act 18 of 1986, codified in Title 31 United States Code and 31 Code of Federal Regulations.} the Money Laundering Control Act,\footnote{US PATRIOT ACT of 2001. The AML provisions in this Act are contained mainly in Title III of the Act.} and the Uniting and Strengthening America by Providing By Providing the Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (‘US PATRIOT ACT’).\footnote{Earlier citation at footnote 3 above.} These laws are all federal laws. Several states have their own AML laws which mirror these federal laws. The aforementioned AML laws are a
clear depiction of the current AML legal regime discussed in Part 1 of this paper. But here, too, the laws do not cater for cyberlaundering.

Also, as regards cybercrime, the US has a federal law entitled Fraud and Related Activity in Connection with Computers Act. This law prohibits the unauthorized use of computers to commit crimes such as espionage, accessing unauthorized information, accessing non-public government’s information by computer, damage to computer, extortionate threats to damage a computer, and trafficking in passwords. Other relevant laws include the Computer Fraud and Abuse Act of 1984, the Electronic Communications Privacy Act of 1986, the National Infrastructure Protection Act of 1996, the Digital Millennium Copyright Act of 1998, the US PATRIOT Act of 2001, and the Cyber Security Enhancement Act of 2002. Nowhere is the conduct of cyberlaundering prescribed in any of these laws. In spite of its increasingly glaring manifestations, cyberlaundering is not as yet a legal concept under US law.

However, unlike most other local jurisdictions, the US is unique for the fact that it has extremely well-resourced agencies which have the capacity to regulate cyberlaundering. These are the Federal Bureau of Investigation (FBI), the Financial Crimes Enforcement Network (FinCEN), and the Drug

---

708 These categories of cybercrime are detailed extensively in Act.
714 See discussion in Chapter 6 below, paragraph 6.5.
The FBI is a multi-tasked law enforcement agency in the US. It has highly specialized investigative techniques with which to combat high profile crimes, such as money laundering and cybercrime. Although cyberlaundering activities are known to it, given that the concept is yet to be categorized legally under federal law, the FBI’s response to it has been somewhat loathed. Certain divisions of the FBI, such as the Internet Fraud Complaint Centre (IFCC) and the National White Collar Crime Centre (NWC3) are dedicated to unravelling the phenomenon of cyberlaundering. However, the FBI is yet to publish a concrete report on its various investigatory surveys on cyberlaundering, as well as its reports on cyberlaundering cases.

4.3.3.5.2 The Financial Crimes Enforcement Network

The Financial Crimes Enforcement Network (FinCEN) is a specialized enforcement agency under the US Department of Treasury. It provides specialist intelligence on financial crimes, and enforces the set regulatory measures set out in the Bank Secrecy Act and the Money Laundering Control Act. Thus, the FinCEN monitors the observance of CDD standards required

---

for most financial institutions in the US, and other concerned parties.\textsuperscript{716} After 9 September 2011, with the enactment of the US PATRIOT Act, the mandate of the FinCEN was broadened to include monitoring terrorist financing initiatives related to money laundering activities. Just like the FBI, the FinCEN is still trying to come to grips with the phenomenon of cyberlaundering. In its Strategic Plan for the Fiscal Years of 2008-2012, there is a blueprint for research into ways of combating internet-based money laundering activities (i.e. cyberlaundering).\textsuperscript{717} However, the FinCEN is yet to issue an actual report on the subject.

4.3.3.5.3 The Drug Enforcement Administration

The DEA is an enforcement agency tasked with controlling the sale and distribution of illegal drugs in the US, as a response to the fact that the US has since been a haven for such activities.\textsuperscript{718} Today, this business also uses tools for cyberlaundering. Realizing the many dangers that electronic payment systems create, as a composite part of the cyberlaundering concept, the DEA has in recent times delegated its focus on this area to its special division known as the National Drug Intelligence Centre (NDIC).\textsuperscript{719}

\begin{itemize}
\item Financial Crimes Enforcement Network (2008B: 4).
\item Though a US-based agency, the DEA has 86 offices in over 62 countries, due to the transnational nature of the illicit drug trade business. Recent studies show that the illicit drug trade in the US is worth around $65 billion. See <http://www.justice.gov/dea/programs/money.html> [accessed on 30 January 2012].
\item See <http://www.justice.gov/dea/programs/money.html> [accessed on 30 July 2010].
\end{itemize}
Given a scenario where a drug dealer is caught with prepaid cards, the question arises whether the seizure of such cards would ordinarily hinder the business of the suspect, as opposed to the seizure of hard cash. Given the fact that a single prepaid card can be accessed by more than one party, this becomes a danger, as the electronic funds on the card can still be accessed by the accused person’s accomplice.\textsuperscript{720} With the DEA’s bringing this issue to light, a new law was enacted in the State of Nevada called the SB-82,\textsuperscript{721} which came into effect on 1 July 2009. This law allows law enforcement officers to investigate suspicious pre-paid card transactions and cases of fraud that occur within the State of Nevada. In order to prevent criminals from removing funds from a prepaid card after seizure, with the requisite warrant, funds on the prepaid card can be frozen for up to 10 days after such seizure. In certain instances, the SB-82 allows authorities to seize without a warrant funds loaded onto a pre-paid card.\textsuperscript{722} Although not of a federal character, this legislative initiative is a good ACL legal measure that will help in the prosecution of cyberlaundering. The viability and legal ramifications of this law are considered closely in Chapter 5 of this study.

\textsuperscript{720} This scenario and its legal ramifications are considered more in depthly in Chapter 6 of this study.\textsuperscript{721} NV Senate Bill 82-75th (BDR 14-266).\textsuperscript{722} National Drug Intelligence Program (2010: 61).
4.4 SUMMARY

Apart from all its other intricate complexities, cyberlaundering is a conceptual problem. There is no current ACL legal regime because a legal comprehension of the concept and an understanding of its convoluted legal ramifications are presently lacking. Investigators and prosecutors therefore cannot identify it properly, which, in turn, means that it cannot be effectively prosecuted.

The present AML legal regime is well-established, with properly entrenched international laws and policies that have been transplanted properly into most local jurisdictions. However, lawmakers and enforcers constantly negate the fact that money laundering is not a static type of crime, for unlike other crimes, it continues to evolve. The current AML laws remain behind the ever-changing nature of cyberlaundering. The laws are therefore unsuited to combat cyberlaundering at both the national and international level. This problem can be described metaphorically as an old wine in a newly-shaped wine bottle, which cannot fit into the old wine cellar. Hence, there is a pressing need to ‘reconstruct the wine cellar’ in order to accommodate this new phenomenon, failing which cyberlaunderers will remain beyond the reach of law enforcers.

This study also prompts the question as to why the present laws regulating money laundering and cybercrime cannot work against cyberlaundering.723

As in the game of dart, these laws only shoot around the base, and not

723 See Chapter 6 for a detailed discussion of this rationale.
directly at the red dot. A proper regulatory legal framework needs to be established, and concrete laws are needed to match this new phenomenon. The next two chapters of this study seek to do just that.
CHAPTER 5
REGULATING CYBERLAUNDERING

5.1 INTRODUCTION
Regulation is a critical and highly relevant factor in establishing a legal framework to combat cyberlaundering. The need for regulation forms the crux of the anti-cyberlaundering (ACL) legal regime. This chapter is dedicated to finding appropriate regulatory measures for cyberlaundering.

As a starting point, it outlines the rationale that underscores the task of regulating cyberlaundering, after which it discusses certain issues that pose as barriers to its regulation. The chapter looks at how cyberlaundering can be combatted by adapting some of the existing apparatus that exists to deal with money laundering. This approach is employed for founding the necessary pillars for the ACL legal regime, such as the prevention, enforcement and compliance pillars. These pillars, which presently make up the current anti-money laundering (AML) legal regime, can be adapted to suit purposes of the needed anti-cyberlaundering (ACL) legal regime. However, in this chapter, the regulatory possibilities in relation to the prevention and compliance pillars alone are considered. The enforcement pillar, which concerns prosecutorial issues related to cyberlaundering, is discussed separately in the next chapter of this study, along with certain technicalities involved in establishing an

---

724 See Chapter 6 that follows.
In addition to examining the existing AML pillars, where applicable, certain anti-cybercrime (ACC) principles are also considered as possible solutions.

### 5.2 RATIONALE FOR REGULATION

Several questions brew beneath the campaign for a solid ACL legal regime. One might ask: Do we really need new laws against cyberlaundering? Are not existing laws sufficient to deal with the problem? These questions all point to the importance of regulating cyberlaundering, as they call into question the need for regulation. These questions have been answered in part in preceding chapters that show that there are currently no national and international legal frameworks for combating cyberlaundering. However, the other part of the equation, which stems from the inadequacy of present laws, is the very essence of this current study, being an investigation into how present laws can be modified to cater for cyberlaundering, failing which new laws become necessary. It follows that an adaptive approach is necessary for erecting a strong regulatory pillar for the ACL legal regime, together with the task of fashioning out new regulatory measures.

It is important to state at this outset that the regulatory framework against cyberlaundering set out in this study does not pertain to laws and law-makers alone, but also to single and collaborative efforts of individuals upon whom a

---

725 See Chapter 6, paragraph 6.6.
726 See detailed discussions in Chapter 4 of this study, dealing with the present national and international legal framework for cyberlaundering.
duty exists to report suspicious transactions. This also includes law enforcement authorities and other natural as well as juristic persons to which the issue relates. Indeed, the AML legal regime is incompatible with the concept of cyberlaundering. This is because there is a mismatch between the AML laws and the phenomenon of cyberlaundering.

The rationale of this study is premised on the notion that the regulation of cyberlaundering is needed in order to stem its growth, which is not only taking a heavy toll on the economy, with rippling effects on both local and international commerce, but which also undermines the global AML legal regime.

---

727 See the AML principles set out in Chapter 4, paragraph 4.2.3.2. Recommendation 23 of the Forty Recommendations of the Financial Action Task Force provides that, other than financial institutions, the duty to report is also incumbent on lawyers, notaries, other independent legal professionals and accountants who engage in the activities of their clients, such as real estate transactions; management of client money and other assets including securities; management of bank, savings and securities accounts; creation, operation or management of legal persons or arrangements; buying and selling of business entities, and the organisation of contributions for the creation, operation or management of companies. See Financial Action Task Force (2012A: 20). Cf Financial Action Task Force (2003: 8). Also, the obligation is incumbent upon non-financial entities, such as dealers in precious metals or stones, as well as trust and company service providers. Financial Action Task Force (2012A: 20). Cf Financial Action Task Force (2003: 16).

728 To put this into further perspective, for example, the customer due diligence and reporting standards ensconced in the current AML legal regime (see Recommendations 5 to 12 of Forty Recommendations plus Nine Special Recommendations, Financial Action Task Force (2004: 12)) cannot be adopted wholly for cyberlaundering purposes. Given the reality of terrestrial banking, for instance, where customers are required to be present at the place where transactions are conducted, the problem is not only whether certain online banks can adhere to these reporting and record-keeping requirements, but also whether the information provided by the customer or user, which they might be required to keep, is true and viable. This further makes it difficult, if not impossible to enforce the Know Your Customer (KYC) principle. Cf discussions in Chapter 3, paragraph 3.5.1 and Chapter 4, paragraph 4.3.2.1.

729 When illicit funds are eventually integrated into the legal economy, the entire commercial sector is tainted with illegality, meaning that traceability of such funds becomes impossible, and measures set in place to maintain the stability of the economy also become undermined. As this forms one of the driving factors forcing countries into recession, in the end, the integrity and stability of financial institutions and systems are affected negatively; international investment is discouraged and international capital flows are distorted. Presumably, over $4 trillion in illicit funds are laundered on an annual basis, and, even more frightening, about 5% to 7% of the world’s gross domestic product (GDP) is laundered annually [Schott (2006: 12) and Unger (2007: 151)]. In fact, the scale has reached such an enormous magnitude that the Financial Action Task Force chooses not to
5.3 REGULATORY ISSUES AND CHALLENGES

The regulation of cyberlaundering is not without certain issues and concerns that hinder its effectiveness and realization. Some of these issues, which will be discussed here, include corporate concerns, the fluidity of the cyberlaundering problem, enforcement challenges and general regulatory problems associated with the roots of cyberlaundering.

5.3.1 Corporate concerns

The regulation of cyberlaundering demands a traversing of certain corporate interests. This is attributable to the fact that most websites that perpetuate cyberlaundering operations are actually profit-driven businesses and enterprises.\(^{730}\) This is evidenced by the preponderance of the e-commerce industry and its unprecedented growth over recent years, propelled by the exponential increase in the use of electronic payment (e-payment) systems, which are, in turn, also fostered by activities of prepaid card companies.\(^{731}\)

\(^{730}\) Good examples are the websites E-gold Ltd and Megaupload Ltd. Cf discussion in Chapter 6, paragraph 6.5.

\(^{731}\) E-commerce is steadily gaining dominance within the global financial sector, representing a significant part of overall commerce. For example, in the United States (US), e-commerce represents about 10.8% of the total economy, jumping from $185 billion dollars in 2008 to $205 billion dollars in 2009. See Javelin Strategy & Research ‘Online Retail Payments Forecast 2010 – 2014: Alternative Payments Growth Strong but Credit Card Projected for Comeback’ 03 June 2011 <https://www.javelinstrategy.com/research/Brochure-171> [accessed on 4 March 2012]. Cf detailed discussion in Chapter 3, paragraph 3.3.1.
Law enforcement bodies are thus engaged in a power struggle with big corporations that thrive on these businesses. Other than websites and prepaid card companies, such corporate concerns are echoed by financial institutions that also need to also implement new measures against cyberlaundering. However, lessons from the past suggest that this task is not an easy one, especially on the part of banks.  

Corporate fears can be allayed by setting the two opposing interests on a scale: On the one hand is the public interest that government and law enforcement authorities seek to protect by putting in place strict ACL measures, and on the other hand, is the potential loss of profit that corporations might lose by implementing such measures, if such risk exists at all. In the end, the fact that the scale is tipped in favour of implementing such ACL measures would not really be an issue. The problem is having such laws approved in by the legislature, where lawmakers representing diverging interests are represented. Fears escalate when one considers the current widespread nature of corporate bribery, where corporations try to ‘grease

---

732 In the early days of the AML legal regime in the United States, with the advent of the Bank Secrecy Act of 1970 (PubL 91-508; 841114), most financial institutions opposed the law, due to allegations that it undermines their corporate interests. In the case of California Bankers Association v Schultz 39L ed 2d 812 (1974) n5, the Supreme Court upheld the constitutionality of the law. Cf previous discussion in Chapter 2, paragraph 2.2.2.1.

733 Corporate bribery, also known as corporate graft, is alarmingly commonplace amongst thriving corporations today. These corporations continue to use the advantage of their position and influence in commerce to derive gains and benefits from government officials, both at home and abroad. For example, in the US, the Foreign Corrupt Practices Act of 1977 (Title 15, United States Code, Public Law 95-213) bars American companies and foreign companies, whose securities are traded in the US, from paying bribes to government officials abroad. Recently, about 78 American corporations were under investigations for violating the provisions of the Act. The corporations include Alcoa, Goldman Sachs, Avon, Pfizer, Hewlett-Packard, and Wal-Mart stores and Kellog Brown & Root (also known as KBR). The latter company is the only one currently facing criminal charges under the Act. See Leslie, W (2012) ‘Hits and Misses in a War on Bribery’ An internet article dated 10
the palms’ of lawmakers to ensure that the laws passed in the end are in their ‘corporate favour.’ This is the heart of the regulatory issue. It is a steep barricade to the regulation of cyberlaundering.

5.3.2 Fluidity of the cyberlaundering process

As long as the internet exists, the potential of it being used as a weapon for criminals will continue to exist. It would be totally wrong to think that the demerits of the internet exceed its merits, and most absurd to suggest that the internet should be banned or outlawed in order to stop internet criminality. This notion is very unrealistic, given how the internet has grown to become an essential part of daily living. Hence, the only logical resolve would be to cut the branch (i.e. cyberlaundering) without necessarily rooting out the tree (i.e. the internet). But how does one regulate a growing problem without reaching to its roots? This is another principal challenge facing the regulation of cyberlaundering. Cyberlaundering is a moving a target, changing shape, guises and adapting with increasingly new technological features. A good example of this is the concept of virtual worlds, which is probably the most dynamic cyberlaundering avenue to date, given its mystifying nature. Where, for instance, virtual worlds have become properly regulated, chances are that

---


734 Cf discussion on the computer element, under the elements of cyberlaundering in Chapter 3, paragraph 3.2.4.2.

735 Cf discussions on virtual worlds in Chapter 3, paragraph 3.5.5.
cyberlaunderers could sniff out other diabolically innovative avenues for their operations. This study nevertheless attempts to grapple with the problem as it presently exists, in the belief that the proposed regulatory measures would become thresholds for other potential regulatory measures, where other cyberlaundering avenues emerge in the future.

5.3.3 Enforcement challenges

It is commonplace that newly enacted laws take time before they gain currency and become established firmly within society. This is so where such laws differ radically from existing norms. The efficacy of any law depends entirely on whether the right systems exist to enforce such laws effectively. Enforcing the law is a challenge when one looks to see what mechanisms already exist to enforce such laws. This is not a problem when existing enforcement mechanisms work.

Given that the enforcement mechanisms needed for cyberlaundering are put in place by governments, the problem arises where governments and their respective authorities are wholly incompetent or incapable of enforcing the needed regulatory measures against cyberlaundering because of a lack of political will and the resources. When it comes to fighting crime, countries have diverging priorities. Based on what was stated in Chapter 4 above, a strong international standard is yet to be forged against cybercrime, as is evidenced by the nonexistence of a concrete international treaty or convention.

736 See Chapter 4, paragraph 4.3.2.3.
on cybercrime. The Council of Europe Convention on Cybercrime\textsuperscript{737} (the Budapest Convention) is worth noting, even though it has a regional effect. Countries have such diverging priorities, not because cybercrimes are generally more prevalent in some countries than others, but because the shoe pinches them from other sides. These countries consider other issues to be more pressing, such as crimes that threaten national security.\textsuperscript{738} Also, some countries lack the capacity. This is the case especially in developing countries. The fact that it is difficult to solicit and obtain the requisite cooperation from such countries, makes regulation almost unfeasible. Such countries cannot be relied upon to regulate cyberlaundering. However, ignorance of the crime of cyberlaundering blinds many to the countless dangers it harbours. The massive impact that it has on the economy is unfathomable, and this is happening when countries are struggling to stabilize their economies. The unfortunate thing is that ignorance of the crime blinds one to its effects, for comprehending the effects first demands an understanding of the crime.

\textsuperscript{737} The Convention was drawn up by the Council of Europe in Strasbourg, with participation of the Council of Europe, as well as the observer states Japan, Canada and China. The Convention was adopted by the Committee of the Ministers of the Council of Europe at its 109th session on 08 November 2001. On 23 November 2003, it was open for signature in Budapest, and on 1 July 2004, it came into force. As at 9 March 2012, the Convention had been ratified by 32 states parties. \textit{In tandem} with the Convention is the Council of Europe Convention on Cybercrime: Additional Protocol to the Convention adopted by the Council of Europe on 7 November 2002 and came into force on 1 March 2006. For more information see the Treaties Office of the Council of Europe at <http://conventions.coe.int/> [accessed on 9 February 2012]. Cf discussion in Chapter 4, paragraph 4.3.2.3.

5.3.4 Problems associated with the roots of cyberlaundering

At the beginning of this study, the issues of money laundering and cybercrime were identified and explored as the main roots of cyberlaundering.\textsuperscript{739} The discussion also pointed out that these concepts are not without their individual regulatory problems.\textsuperscript{740} Given this fact, these problems have been transposed onto the notion of cyberlaundering, further convoluting the phenomenon and making the issue of its regulation more complicated. For example, as regards cybercrime, the field of computer forensics has not reached a state of full-fledged development. This fact impacts on the overall regulation of cybercrime\textsuperscript{741} which, in turn, impacts on the regulation of cyberlaundering, further suppressing potential regulatory measures against it.

Given the concepts of money laundering and cybercrime, as roots of cyberlaundering, and building on the premise that these two roots are discordant concepts that are each burdened with separate regulatory challenges, the principles that will be discussed explain how cyberlaundering can be regulated by means of adapting existing measures against money laundering and cybercrime. This will be called the ‘adaptive approach’ in the discussion below.

\textsuperscript{739} See Chapter 2, paragraphs 2.2 and 2.3 for detailed discussions on these concepts as the two pillars on which the cyberlaundering rests.
\textsuperscript{740} See Chapter 2, paragraphs 2.2.5 and 2.3.4.2.
\textsuperscript{741} American Academy of Forensic Sciences (2011: 14). Cf Reyes, Brittson, O'Shea, and Steele, (2007: 33). The other glaring fact is that cybercrime laws are not commonly uniform across major countries. This is due partly to the fact that there is currently no one true international legal framework umbrella addressing the problem, and the fact that the few that exist are not fully incorporated into national laws. Cf discussion in Chapter 6, paragraph 6.6 and Chawki (2003: 49).
5.4 AN ADAPTIVE APPROACH TO REGULATING CYBERLAUNDERING

The adaptive approach to regulating cyberlaundering is tied to the central tent pole established by the current anti-money laundering (AML) legal regime, which is upheld by the compliance, prevention and enforcement pillars. Also, as a necessary scaffold required for supporting this tent pole, certain anti-cybercrime (ACC) principles are also adapted, particularly for the enforcement pillar. This approach is desirous because the loopeholes created by cyberlaundering can be filled easily, laying a strong foundation for a formidable anti-cyberlaundering (ACL) legal regime. In keeping with the adaptive approach, the current ACL legal regime could stand on the existing pillars forming the current AML legal regime without faltering. With this in mind, the following discussion reflects various measures that are needed to adapt the pillars of the current AML legal regime to suit the purposes of a developing ACL legal regime. Therefore, possible regulatory measures against cyberlaundering through all three pillars of the present AML legal regime are assessed below by identifying what can be done in each pillar to regulate the problem. As noted earlier, the enforcement pillar, which is the third pillar of the current AML legal regime, entailing prosecutorial issues of cyberlaundering, is only discussed in the next chapter of this study. The prevention and compliance pillars are discussed here.

742 See Chapter 4, paragraph 4.2.
5.5 PREVENTION PILLAR FOR THE ACL LEGAL REGIME

Prevention represents an important regulatory phase within the broad ACL discussion. As part of the adaptive approach employed for the regulation of cyberlaundering, with a pragmatic approach, this section sets out ways in which cyberlaundering and its growing manifestations can be legally curtailed in policy wise. In this section, the ACL prevention pillar is discussed under two broad categories: a general approach to cyberlaundering regulation, and a target approach to cyberlaundering regulation. While the latter is more specific, in that it addresses those thorny issues that continue to make cyberlaundering so complicated, the latter deals with regulatory measures from a more general perspective.

5.5.1 General preventive measures against cyberlaundering

There are certain general measures that can be put in place to ensure the prevention of cyberlaundering. These are discussed below.

5.5.1.1 Threshold consideration: Premise for regulation

Cyberlaundering and its relatedness to money laundering and cybercrime leads to the fact that some problems associated with both concepts become transposed automatically to cyberlaundering. In the same way, the regulatory rationale for both concepts should be transposed onto cyberlaundering, where applicable. In other words, the inextricable link between cyberlaundering and its two root concepts, which are money laundering and cybercrime, should
serve as a foundation to regulate it. By constantly taking measures to combat the ‘mother crimes,’ invariably, cyberlaundering is attacked at the roots, even though such measures are not entirely sufficient. Although it is not the purpose of this study to explore all the present regulatory mechanisms against money laundering and cybercrime, as they are separate fields, the discussion now turns to legal measures that are essential to the regulation of cyberlaundering from a broad or general perspective.

5.5.1.1.1 Conceptualizing cyberlaundering legally for regulatory purposes

The first step towards regulating a problem is defining it. This is the primary aim of Chapter 3 of this study, which attempts to conceptualize cyberlaundering into a legal frame.\footnote{See discussion in Chapter 3, paragraph 3.2.3.} The legal conclusion reached was that cyberlaundering is essentially money laundering, although the playing field (i.e. the internet) where the process takes place is different.\footnote{See discussion in Chapter 3, paragraph 3.2.3.3.} Therefore, a person who commits cyberlaundering might be deemed to have committed money laundering, although this is hardly the case in practice.\footnote{This issue intertwines with the subject of prosecuting cyberlaundering and particularly detection. The fact that, currently, authorities are unable to detect cyberlaundering explains why it has not been prosecuted as money laundering. This in itself is due to the fact that there is not yet a legal framework in place upon which prosecutors can rely to institute criminal proceedings. For further details, see discussion in Chapter 6, paragraph 6.5.} However, the same could not be readily said for cybercrime, given that cybercrime itself has numerous sub-categories of cybercrimes.\footnote{See discussion in Chapter 3, 3.2.4.1.} The reason why little is known about cyberlaundering, and the reason why the concept has remained
elusive, is simply because policymakers do not understand the problem. This is the root problem of cyberlaundering, which demands urgent redress.

Thus, as a fundamental first step to regulation, this study holds the position that cyberlaundering should be expressly included into the definition of money laundering. It should also be included into the rubric of cybercrime, but as a separate category within it. In other words, cyberlaundering should be criminalized as money laundering and cybercrime. This proposal is supported further by the fact that the elements of cyberlaundering fit well into the elements of the crimes of money laundering and cybercrime.\(^747\)

This approach has the advantage that the problem would be addressed from the two legal sides of money laundering and cybercrime. It implies that the present legal measures against both these two subject areas can be harnessed against cyberlaundering as well. And where the legal remedies available against one of the ‘mother crimes’ prove insufficient for the regulation of cyberlaundering, especially with the likelihood that cyberlaundering will

\(^{747}\) As pointed out in Chapter 3, paragraph 3.2.4.2, the elements of cyberlaundering include a predicate offence, illegal funds, an activity, a computer (\textit{actus reus}); the knowledge of the illegal funds and an associative intention with the illegal funds (\textit{mens rea}). These elements also constitute the elements of the crime of money laundering, save for the requirement of a computer. The object of the crime of money laundering is the same as that of cyberlaundering. The object of the crime here includes the violation of government or state activities and its management system by causing instability in its financial sector. It also includes obstructing the normal activities of the judicial investigation of crime, as well as the objective aspect of the performance which entails the disguise and concealment of the proceeds of the relevant criminal activity. The purpose of criminalising money laundering is, in the first place, to safeguard certain protected interests, such as the health of the economy and the judicial process. By criminals succeeding with their money laundering operations, these protected interests are violated. For cybercrime, on the other hand, given that the minimum requirement here is for the violation of a right or interest to have occurred with the instrumentality of information technology or a computer, the ambit is wide enough to accommodate the concept of cyberlaundering. See Chapter 3, paragraph 3.2.4.2 for more details.
evolve into newer forms in the future, one can always rely on the legal remedies available to the other against cyberlaundering. As such, the legal frameworks for each of these separate concepts would target the problem, with better hopes of curbing it.

5.5.1.1.2 Fighting predicate offences

The rationale that underlies money laundering is that a crime must have been committed from which a criminal derives funds. The purpose of laundering the funds is to conceal or disguise the illegal proceeds in order to create a veneer of legality. Given the premise that cyberlaundering covers the nature of money laundering, just as with money laundering, the crime is predicated on an earlier offence committed. In other words, the proceeds in question must have been derived from a crime committed previously in order to constitute cyberlaundering. Therefore, it follows that combating the respective predicate offences is tantamount to fighting cyberlaundering.

As established previously, with predicate offences, an expansive approach is followed, as the norm is to cast the net as wide as possible in order to cater

---

748 Cf discussion in Chapter 3, paragraph 3.6.
749 Cf Chapter 6, paragraph 6.6 below for discussion on how this can be effected in practice. Where cyberlaundering becomes part of the current AML and anti-cybercrime (ACC) legal regimes, in consequence, it will fall under the legal regulatory umbrellas of these two legal regimes. Interestingly, recently, a proposal was made for the establishment of an International Criminal Court or Tribunal for Cyberspace (ICTC) which shall have jurisdiction to hear cybercrime offences, and which shall have a structure that is analogous to existing ones, such as the International Criminal Court (ICC), the International Criminal Tribunal for the Former Yugoslavia (ICTY) and the International Court of Justice (ICJ) (Schjolberg (2011: 6). If this recommendation ever sees the light of day, it would help further as a viable regulatory possibility for cyberlaundering. But the starting point remains to have cyberlaundering conceptualized legally as a cybercrime.
for all serious offences.\textsuperscript{750} Whilst the notion of ‘serious offences’ applies equally to cyberlaundering, it is worth noting that the emergence of cyberlaundering also came together with other forms of cyber-related offences that complement it. Offences such as cyberfraud, internet piracy, copyright infringement, hacking and phishing, amongst a host of several others, are increasingly becoming very profitable illegal enterprises and means through which illegal proceeds are derived.\textsuperscript{751} Unbeknown to many, however, technologically-savvy criminals are also potential cyberlaunderers who use the same technology (i.e. cyberspace) to ‘wash’ the illicit funds. In the end, through the mastery of their operations, the funds appear to be clean, without apparent links to their criminal origins. Therefore, closer attention should be paid to fighting cybercrimes in general, for they are propagating the exponential growth of cyberlaundering. The inextricable link between the notion of cyberlaundering and cyber-criminality further supports this submission. This is why this study emphasizes the need to fortify the current AML and anti-cybercrime (ACC) legal regimes, which are currently geared towards fighting money laundering and cybercrime. For example, certain regulatory measures such as the policing of the internet and the creation of awareness towards internet criminality through education are

\textsuperscript{750} See discussion in Chapter 4, paragraph 4.2.3.2.1. Cf Article 2 of the \textit{United Nations Convention against Transnational Organized Crime} (i.e. the Palermo Convention, adopted by the General Council of the United Nations on 15 November 2000 and came into force on 29 September 2003) and Financial Action Task Force (2003: 3).

\textsuperscript{751} One part of the commercial spectrum that is most stung by these crimes are private companies and organisations. A recent study shows that the cost of these offences for companies results in an annual loss of up to $36.5 million per company. ArcSight (2011: 3).
crucial as they also help to stem the growth of cyberlaundering, although indirectly.\textsuperscript{752}

In this way, by tackling these predicate crimes, a major stronghold of cyberlaundering is being rooted out. But, of course, the capacity to do this is dependent on certain extraneous considerations, particularly whether efficient policies exist to ensure that they are suppressed adequately.\textsuperscript{753}

5.5.1.1.3 Awareness towards lax jurisdictions

As another general approach towards preventing cyberlaundering, more attention should be given to certain jurisdictions that have been known to have lax AML and ACC laws. In the past, the Financial Action Task Force (FATF) blacklisted countries that did not have adequate AML systems. These countries were called Non-Cooperative Country or Territories (NCCTs).\textsuperscript{754}

\textsuperscript{752} Policing the internet is a crucial strategy for fighting cybercrime. Several countries are doing this. For example, in the United States, there is the Federal Bureau of Investigation (FBI) and the Financial Crimes Enforcement Network (FinCEN) to name a few (Cf discussion in Chapter 4, paragraph 4.3.2.4). On the international plane, there is the International Police Organization (Interpol). Interestingly, several non-state actors and non-governmental organisations have also ceased the reins in the campaign against cybercrime. For example, in the US, one of such is known as CyberAngels Internet Safety Program, which is an educational training site on cyber safety. (Cf for more details see its website at <http://www.cyberangels.org/> [accessed on 4 April 2012]). In the United Kingdom, there is the Internet Watch Foundation (IWF), which aims to regulate criminal internet content. (Cf for more details see its website at <http://www.iwf.org.uk/> [accessed on 4 April 2012]). There is also Internet Hotline Providers (INHOPE), which caters for the entire continent of Europe, and which serves to deter online child abuse. See its website at <http://www.inhope.org/gns/home.aspx> [accessed on 4 April 2012]. For a discussion on several other strategies against cybercrime, see Furnell (2002: 269) and McQuade (2006: 457). For the varied strategies employed against money laundering see Reuvid (1995A: 175), Reuvid (1995B: 191) and Jones (1995: 195). Cf Zeldin and Florio (2007: 413).

\textsuperscript{753} This issue is strongly linked to the challenges of enforcing the regulation of cyberlaundering expressed earlier. This is because most countries are incapable of fighting cybercrime. See paragraph 5.3.3 above.

\textsuperscript{754} Some countries that were often on the NCCTs reports were, 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
Although, the FATF has stopped doing this,\textsuperscript{755} it has replaced the blacklisting system with a more stylized initiative, which includes having regional and sub-regional FATF-Styled Regional Bodies that monitor the progress of the AML systems in countries within a particular region.\textsuperscript{756} Most former NCCTs are still subjected to close monitoring. Interestingly, these former NCCTs also lack the ability to fight cyber-criminality, making the policing of internet operations seem like a farce. Where jurisdictions are ill-equipped to fight cybercrime in the same jurisdiction where AML laws are neither very strong nor weak, the combination presents an attractive template, and constitutes a perfect breeding ground for cyberlaundering operations.

Even in countries with effective AML regimes, because the internet has made the world today a global village, jurisdictional boundaries are blurred and the legitimacy of the AML systems in those countries is consequently affected. Even from countries with strong AML legal regimes, such as the United States and the United Kingdom, for example, it is possible for criminals to run websites that are operated in the former NCCTs. This makes local control within the relevant jurisdiction, virtually impossible. Thus, former NCCTs,

\textsuperscript{755} In October 2006, the FATF announced that there were no countries on its NCCTs list. See Financial Action Task Force (an undated internet website) ‘Non-Cooperative Country and Territory’ available at <http://www.fatf-gafi.org/document/4/0,2340,en_32250379_32236992_33916420_1_1_1_1,00.html> [accessed on 4 April 2011]. Cf Financial Action Task Force (2007A: 3).

\textsuperscript{756} Some of the FATF-Styled Bodies include the Asia/Pacific Group on Money Laundering (APG), Caribbean Financial Action Task Force (CFATF), Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), the Financial Action Task Force on Money Laundering in South America (GAFISUD) and the Middle East and North Africa Financial Action Task Force (MENAFATF), as well as the Eastern and Southern African Anti-Money Laundering Group (ESSAMLG).
although now delisted, are still viable avenues for the operations of trans-border criminal activities, especially where the internet is involved. Therefore, because criminals will continue to exploit avenues where they believe the likelihood of getting caught is slim, it is important to keep focus on such jurisdictions and develop an adequate law enforcement infrastructure to continually fight money laundering and cyber criminality. This is a crucial starting point in preventing cyberlaundering.

Together with the need to fit cyberlaundering into the legal frame of money laundering and cybercrime, and coupled with the need to fight predicate offences, the need for awareness of lax jurisdictions is also an important aspect of the general preventive measures against cyberlaundering. An approach that is more focused on certain problems of cyberlaundering is discussed below.

5.5.2 Target approach to cyberlaundering regulation

The reason why cyberlaundering is so problematic is because it capitalizes on existing loopholes in the AML legal regime, thus widening the scope for criminal enterprises as a result of technological innovations. As such, it is prudent to grapple with those aspects of cyberlaundering that are being exploited for criminal operations. This is necessary to concretize the prevention pillar of the ACL legal regime, which is the purpose of this section. Given the imminence of the problem, one needs to deal with the very thorny issues that make cyberlaundering a seemingly elusive and
unfathomable problem. Therefore, other than the general approach discussed above, a target approach to cyberlaundering is adopted. This consists in promulgating regulatory measures for certain identifiable aspects of cyberlaundering such as: online banking which requires new CDD measures; the issue of anonymity which can be solved with the right cryptography and biometry; aspects of electronic payment systems; and online gaming, which, for purposes of this study, encompasses virtual worlds and online gambling.

5.5.2.1 Adopting new CDD measures

The present AML legal regime is largely one-sided, applying mainly to financial institutions and other third parties or intermediaries such as correspondent banks, legal persons and other non-financial institutions. However, these entities are all of a ‘terrestrial’ nature and do not cater for the ‘cosmic’ nature of cyberlaundering. The other plausible recourse, in the form of ACC laws, does little to help the situation, as there are currently no AML measures transposed or merged with the notion of cyber criminality – all of which, again, reiterates the purpose of this study. What follows is an elaboration of the areas where the CDD measures are needed against cyberlaundering. These include adopting new Know Your Customer (KYC) principles and creating new wire transfer models as a plausible remedy to the

---

757 See discussion in Chapter 4, paragraph 4.2.2.1.
current cyberlaundering techniques of online banking\textsuperscript{758} and online auctioneering.\textsuperscript{759}

\subsection*{5.5.2.1.1 Modifying the KYC principle}

With regard to CDD measures for banks, and for the typical bank-customer relationship, the KYC principle is one that is ingrained in the prevention pillar of the current AML legal regime. It represents a vetting process conducted by banks which, essentially, requires banks to be fully aware of the profile of prospective clients or customers prior to transacting with them, and for subsequent future transactions.\textsuperscript{760} The FATF’s Recommendation 20 requires financial institutions to have a basic knowledge of their transacting customers.\textsuperscript{761} In recent times, this principle has been further expanded by the Wolfsberg Group.\textsuperscript{762} With its often advocated risk-based approach, which requires financial institutions to identify the criteria to measure potential money laundering risks with every case scenario, and judged on its own merit,\textsuperscript{763} the Wolfsberg Group adds its bit to fortifying the KYC principle. Thus, the KYC principle is the precondition laid down for a financial institution wishing to transact with prospective customers. Although a

\textsuperscript{758} Cf discussion in Chapter 3, paragraph 3.5.1.
\textsuperscript{759} Cf discussion in Chapter 3, paragraph 3.5.2.
\textsuperscript{760} See discussion in Chapter 4, paragraph 4.2.3.1.1.
\textsuperscript{762} Cf discussion on the Wolfsberg Group of Banks in Chapter 4, paragraph 4.2.2.1.1. See also footnote 401 above.
\textsuperscript{763} 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. Cf discussion in Chapter 4, paragraph 4.3.1.5.
continuous application of this measure to subsequent customer transactions might seem unnecessarily monotonous and mundane, the KYC principle should be applied throughout the duration of the bank-customer relationship.\textsuperscript{764}

The debacle here is simply that the applicability of the KYC principle, as stipulated by the current AML legal regime, does not extend to online banking\textsuperscript{765} and several other online transactions.\textsuperscript{766} The very essence of the problem is the possibility of multiple parties having access to a single online bank account, provided that the log-in information is at hand. Hence, as a result, the actual identity of the customer or user of the online banking services cannot be ascertained. This gets compounded further by reason of the fact that most online banks without terrestrial offices welcome all manner of applications from prospective customers who wish to open an account online, without resorting to the vetting process usually conducted by terrestrial financial institutions. As such, 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.

\textsuperscript{765} Cf discussion in Chapter 3, paragraph 3.5.1.
\textsuperscript{766} Online transactions are non-face-to-face transactions that fall within the broader ambit of higher risk scenarios, which, by virtue of Recommendation 5 of the Forty plus Nine Special Recommendation of the FATF, calls for enhanced customer due diligence (CDD) measures. This has roots in Recommendation 8 of the Forty Recommendations, which provides that financial institutions should have policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions. The latter provision should also be read with the Basel CDD paper (section 2.2.6) which provides that, before financial institutions accept risks, there must be adequate CDD measures to mitigate higher risks. See Financial Action Task Force (2004: 4) and Basel Committee on Banking Supervision (2001A: 4).
The Electronic Banking Group of the Basel Committee on Banking Supervision (BCBS) proposed a solution to this quandary in its 2001 report on risk management principles.\textsuperscript{767} The report assesses the applicability of the KYC principle and certain other due diligence requirements to non-face-to-face customers. The BCBS proposes 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. This is expressed below:

\begin{quote}
Financial institutions are advised to mitigate higher risks by ensuring the certification of documents presented; requisition of additional documents to complement those which 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.\textsuperscript{768}
\end{quote}

Regardless of the stringent nature of this recommendation, it still does not solve the problem.

As a starting point, and as a result of the above, two categories of financial institutions should be identified for the purpose of ensuring that the KYC principle can be applied against cyberlaundering. These include, on the one hand, financial institutions having both terrestrial and cyberspace presence,

\textsuperscript{767} Baseline Committee on Banking Supervision (2001A: 90).
and, on the other hand, financial institutions present in cyberspace but without a terrestrial presence.

(a.) Financial institutions with a terrestrial presence

At the time of the BCBS’s report, the first category of financial institutions was predominant. Online banks without a terrestrial presence were, at the time, almost inconceivable. Hence, its recommendation would perfectly suit those online banks that have a terrestrial presence, and it would be logical to require potential customers wishing to open an online account at a bank to be physically present, at least at the initial phase. This would enable the bank to vet the customer, which means having a face-to-face interview with every customer. After this process, customers could begin to conduct banking transactions online. By so doing, the bank can conduct the necessary verifications and thus act in line with the required KYC principle.

(b.) Financial institutions without a terrestrial presence

For the second category of financial institutions which operate purely in cyberspace, without any terrestrial presence, a more circumspective approach should be adopted. Given that the KYC principle is premised on the notion of contact (i.e. which often requires meeting with prospective customers for purposes of verification) and oversight (i.e. the continuous supervision of the customer and subsequent transactions performed), online banks should be brought under the KYC principle. As such, because of the grave potential for
cyberlaundering that these banks create by operating elusively in cyberspace, they should be required to have terrestrial office(s) where their prospective customers should also be required to report, as a mandatory first step to operating an online bank account. Only in this way can the KYC principle be satisfied.

This study recommends that the distinction between financial institutions with a terrestrial presence and those without one should be completely erased. This will ensure that the internet and its increasing capabilities do not keep growing out of the bounds of existing legal frameworks meant to curtail the growth of crime. Therefore, online banks without a terrestrial presence should be outlawed. Weighed on a scale, having the notion of convenience that these banks create as a mitigating argument on the one hand, and having the rationale for regulation on the other hand, the abolition of these banks is further justified in the absence of proof that these banks and their activities cannot be regulated effectively if their existence is kept in cyberspace alone, without a terrestrial presence.

The same rationale should be transposed to online auctioneering as well. As discussed previously, the loophole in this case is in the bidding process, in which one bidder outbids other bidders excessively, making the bid impossible for other bidders to match, until the object of sale is finally sold to him or her.\(^7\)\(^6\) Where the funds in question are illicit in nature, it would have

\(^7\)\(^6\) In this example it is assumed that the cyberlaunderer exploits a perfectly legitimate online auction site. Alternatively, the cyberlaunderer could set up his/her own auction site and even bid with
been ‘washed’ successfully. Therefore, just as with online banks, online auction sites should conduct CDD measures for all prospective bidders in order to ascertain their identities, and they should have a record of each one, in order to help potential investigators to ‘follow the money’.

5.5.2.1.2 Adopting new wire transfer models

Wire transfers are synonymous and essential for the workings of online banking which, as discussed already,\(^770\) is one very prominent avenue that aids cyberlaundering. The subject requires some investigation with a view to ensuring that the gaping lacunae presented are filled.

Wire transfers refer to the electronic transfer of funds, meaning the equivalent value of funds, at the request of a customer from one bank account to a beneficiary account, which is usually another bank.\(^771\) Of several electronic messaging systems that exist today for the trans-border transfer of money, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system is the most prominent. It is used amongst most banks today for both local and international transfer of funds.\(^772\) Unlike the local wire transfers,

---

\(^{770}\) See elaborate discussion in Chapter 3, paragraph 3.5.1.


\(^{772}\) Widely used the world over, the SWIFT electronic messaging service has earned a good reputation amongst banks. It is stated in its website that “SWIFT has its headquarters in Belgium and has offices in the world’s major financial centres and developing markets. SWIFT provides additional products and associated services through Arkelis N.V., a wholly owned subsidiary of SWIFT, the assets of which were acquired from SunGard in 2010. SWIFT does not hold funds nor does it manage accounts on behalf of customers. It also does not store financial information on an on-going basis… [It secures the] exchange of proprietary data while ensuring its confidentiality and integrity.” See SWIFT ‘Company Information’ available at <http://www.swift.com/about_swift>
international wire transfers pose a problem because they have loopholes that are prone to cyberlaundering operations. The US’ Drug Enforcement Administration (DEA) has successfully identified the vulnerability of the SWIFT system which criminals have since exploited, as stated in the quote below:

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 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].

A summary of the text above is simply that criminals have been able to use wire transfers to launder money through intermediary or correspondent banks because there has not been a requirement for their identities to be revealed to such intermediary banks in the process. This is because the current system used by SWIFT allows for their identities to be concealed. The result is that the intermediary banks are completely oblivious to the identities of the person sending the funds and the receiver.

773 Drug Enforcement Administration: National Drug Intelligence Program (2010: 79). Bracketted words are the author’s.
In line with the recommendation of the DEA and a prior recommendation by the BCBS, a new type of messaging system needs to be introduced in order to ensure that intermediary banks are not sidelined or slighted in the overall duty to conduct the requisite CDD measures. Pursuant to the need, in November 2010, the DEA’s National Drug Intelligence Program introduced a new type of SWIFT messaging system known as the MT 202 COV, which seeks to address the issue by enabling intermediary banks to retain both originator and beneficiary information on virtually all wire transfers that are processed between the originator and the beneficiary banks. As such, whether the relevant intermediary bank is local or international, the information is captured regardless of the link it might have with the originator bank. Hence, where the MT 202 COV is implemented, intermediary banks are put on the same pedestal as other financial institutions, and much would be required from them as regards their roles, as they also take up the mantle of ensuring that adequate CDD measures are adhered to. In this way, they would no longer be operating blindly, and criminals would not exploit their functions.

Apart from the US, where the MT 202 COV has been issued as a compulsory guideline for financial institutions which now have a compliance obligation, this system does not yet exists in other countries. As a result,

---

777 Soon after the BCBS made its May 2009 recommendation for the transparency in conducting cross-border funds transfer, the Board of the Federal Reserve System of the US issued a circular with
the vulnerability of wire transfers with SWIFT through intermediary banks for cyberlaundering operations still remains in other countries today. Therefore, it would be useful to adopt the MT 202 COV or its equivalent in other countries as well. Given the very broad and far-reaching nature of international wire transfers, it is unhelpful if laws are not harmonized, especially, when it comes to combating cyberlaundering.

5.5.2.2 Protected biometry and cryptography

The problem of anonymity, which is an inextricable feature of the internet, is one which has fertilized the growth of cyberlaundering. This is because the cyberlaunderers consider themselves so unidentifiable, that they resort to the platform of the internet, which provides the necessary veil. 778 This section discusses certain ways in which the concern of anonymity can be tempered. Primarily, with proper biometric and cryptographic infrastructures in place, this is possible. Both issues are explored further.

5.5.2.2.1 Employing biometric methods for identification

Biometry is any observable or measurable parameter of a person. 779 It entails the identification of humans by those features, traits or characteristics unique


778 For a detailed discussion on the issue of anonymity and its causal relationship to cyberlaundering, see Chapter 3, paragraph 3.2.2.3.

to them, such as one’s fingerprint, iris, footprint, retinal pattern; face, hand and foot geometry, DNA and dental records, amongst several others.\textsuperscript{780} Scientifically, amongst its many varied uses, biometric information is used for identification purposes, as it can be used to readily identify individuals. Its relevance for identification purposes comes out prominently with respect to online transactions, as it runs parallel to the problem of anonymity, which underlies the problem of cyberlaundering. Not knowing the individual behind the computer is a recurring theme of the problem, which correlates with the very need to ensure that proper identification measures are in place. The ability to identify a person who transacts online could very well transcend levels of human ability, because what the eye is able to see as physical proof often equates to irrefutable proof, as opposed to what technology can produce. This is due mainly to the fact that technology is but a human creation at the end of the day, which is not invulnerable to human fallibilities such as error, alterations, defacements and variations. Having this in mind, in devising ways to ensure the identity if an individual, the most plausible solutions should always be concocted.

For all online transactions, better biometric systems need to be put in place as safeguards, especially for those transactions that are of a financial nature. When online transactions are performed, the \textit{status quo} at present requires persons to provide only a name and password with which to ascertain that the

\textsuperscript{780} In its extended form, biometrics also entails behavioural characteristics such as a person’s voice, gait, mannerisms, signature dynamics, one’s key stroke dynamics or other act or expression. Cf Caloyannides (2004: 291).
person attempting to gain access to the account is the individual who owns the account. This often comes with fields on a web page which individuals are required to populate with the requisite name and password. This system can be described as a single-standard approach, as it operates without the use of any biometric feature. This study proposes the need to develop a more complex system of identification that would establish a more comprehensive biometric infrastructure for online transactions.\textsuperscript{781} This always necessitates the need for parties to an online transaction to provide two kinds of information: on the one hand, specific information that is only known to him or her, and, on the other hand, a biometric feature that relates to his or her person.\textsuperscript{782} Adopting such a dual-standard verification system is likely to guarantee the identity of persons who perform online transactions. This, to a certain extent, ameliorates the concern of anonymity.

5.5.2.2.2 Ensuring better encryption methods

A message or information which is communicated over the internet is not ‘transported’ around cyberspace in its bare form. It takes the form of encryptions. Within the wider field of cryptography,\textsuperscript{783} encryption is the process through which information is transformed, using a cipher or

\textsuperscript{782} 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 regard to online transactions. Clearly, this aspect is one which merits some technological advancement. This should, however, not be beyond grasp, given the dynamic state of technology.

\textsuperscript{783} Cryptography is the study of techniques necessary to secure communication in the presence of third parties. Cf Beckett (1988: 22) and Paar and Pelzl (2010: 7).
algorithm to make it unreadable to all but the one who possesses special knowledge of it.\textsuperscript{784} Encryption has always been a means by which secret messages are communicated. As it concerns the issue of cyberlaundering, it runs parallel to it, given that it fosters the notion of anonymity, which is what makes cyberlaundering to thrive. Given the technological mould within which encryption is embedded, criminals freely exchange communications over the cyberspace, which goes unchecked. The confidence with which this is done feeds off the privacy argument which can be raised in defence against persons seeking to pry into private communications.\textsuperscript{785} For example, a cyberlaunderer is able to send an encrypted code to a smurf within his/her criminal enterprise via any platform of electronic communication, such as an email containing the details of certain prepaid cards that hold the value of illicit funds. When considered closely, the encryption process in this case, the encrypted code that is sent involves mainly two public keys: one to ‘lock’ or encrypt the plain text, and the other to ‘unlock’ or decrypt the plain text.\textsuperscript{786} The first key is often held by the sender, and the second by the receiver.

In certain instances, a system is available that can intercept the communication. This often appears as a default third party structure generally known as a key recovery, or key escrow system, which is set in place to

\textsuperscript{785} Premised upon the fact that the right to privacy, which includes privacy of communication, is a fundamental human right in any democratic state, it remains a viable argument that can be raised legitimately and illegitimately. In modern times, it has become a veil under which criminals are hiding from law enforcement authorities. See Chapter 6, paragraph 6.2.3 for an extensive discussion of the privacy argument and its merits.
intercept public keys and decrypt the relevant information that transpires.\footnote{787} The key recovery system has the potential of causing data interception. But it is not without problems in practice. For example, in the United States (US), the National Security Agency came up with what is known as ‘Clipper Chip’ - a key recovery system in the form of an 80-bit encryption infrastructure meant to ensure that the US government is able to track encryptions and decrypt data.\footnote{788} As a result, once a suspicious transaction is sensed, the government can decrypt messages in order to find a trail. However, due to the public outcry, mainly privacy concerns,\footnote{789} the Clipper Chip was never fully adopted.\footnote{790}

This study argues that the key recovery system is one which is inextricably interwoven with the fight against cyberlaundering. While the abrasive and unscrupulous monitoring of personal communication is not advocated, it is believed that, on the basis of reasonable suspicion, the key recovery system serves as the necessary caveat to the often unsupervised system of encryption, which is now employed by cyberlaunderers. By ensuring that a mechanism is in place that can easily tap into criminal communications, not only would

\footnote{788} Turner (2011: 161).
\footnote{789} Cf footnote 57 above. For a full elemental discussion of the privacy issue, see Chapter 6, paragraph 6.2.2.
\footnote{790} At present, the US uses a key recovery system protocol known as the Transport Layer Security (TLS) which does not grant any leeway for third party access. Cf footnote 56 above and Turner (2011: 161).
prosecutors have admissible evidence in court, but also the loophole of anonymity is effectively blocked, and cyberlaundering operations are deterred to a great extent. Although the key recovery system represents an essential deterrent system, where it is absent, law enforcement authorities could always resort to obtaining a court order in order to decrypt an encrypted message when there is *prima facie* proof of suspicious transactions occurring.

5.5.2.3 Regulating electronic payment systems

As discussed previously, electronic payment systems (e-payment systems) are the instruments with which cyberlaundering is bolstered. In the past, the trend with the traditional notion of money laundering was for people to leave money overseas, or in some unlikely terrestrial location. But with the rise in e-payment systems, people are beginning to ‘leave’ money online, without such money being ‘connected to a financial institution, which can change hands rapidly between digital identities of the same or different person’. This fact points to the issue of anonymity, which rears its head again through e-payment systems. E-payments systems circumvent the KYC principle, given that the digital identities of e-payment system users are, in many cases, unidentifiable.

The possible ways of regulating e-payment systems will now be discussed. The discussion will also look into the establishing of electronic money

---

791 See Chapter 6, paragraph 6.2.3 for further discussion on the issue of evidence gathering as it relates to the prosecution of cyberlaundering.

792 See detailed discussion in Chapter 3, paragraph 3.3.

793 Dementis (2010: 10).
institutions, stricter controls for smart cards and the possibility of fusing the money-trail with the bit-trail.

5.5.2.3.1 Establishing electronic money institutions

In its 2009 Directive 2009/110/EC, the European Union (EU) recommends that member states should establish a new model of monetary institution that caters solely for the growing emergence of e-money, known as ‘electronic money institutions’ (otherwise called e-money institutions). By definition, an e-money institution is one that is authorised under the Directive to issue e-money. The rationale behind this recommendation comes in light of the reality that the e-money service providers, including their issuers and agents, do not exactly fit the definition of ‘financial institutions’ as generally understood, other than those financial institutions already having e-money services which they provide. The scope of e-money service providers as envisaged under the directive is quite broad. It encompasses all models of e-

---

796 The EU defines e-money as an “electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions […], and which is accepted by a natural or legal person or legal person other than the electronic money issuer.” See Article 2(2), Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC. Cf discussion in Chapter 3, paragraph 3.3.1.
797 As regards the term ‘financial institutions’, which, as outlined by the FATF, means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer (inclusive of private banking). For an elaborate definition of ‘financial institutions’ see discussion in Chapter 4, under paragraph 4.2.2.1. See Financial Action Task Force (2012A: 115). Cf Financial Action Task Force (2003: 16).
payment systems\textsuperscript{798} as long as the services provided involve e-money as defined in the directive.\textsuperscript{799} Thus, by reason of the delineation and categorization, the rationale is that AML measures can be applied effectively to these e-money institutions, as a legal framework is established and proper supervision can be ensured. As such, persons (i.e. both natural and legal) who do not fulfil the prerequisites laid out in the Directive cannot willy-nilly become an e-money service provider. Compared to the services provided by financial institutions, e-money institutions are limited in the services they provide,\textsuperscript{800} which helps further in identifying deviances in the activities engaged in and as well as regulating such activities. Notably, amongst several salient measures set out in the Directive, the e-money institutions are not allowed to outsource their functions to agents or third parties.\textsuperscript{801} This ensures that the line between regulated and unregulated entities is not blurred by the activities of agents who could be unscrupulous in their operations. Also, the provisions pertaining to e-money institutions are

\textsuperscript{798} This includes the merchant-issuer model, the bank-issuer model, the non-bank issuer model and the peer-to-peer model. For further discussion see Chapter 3, paragraph 3.3.2.

\textsuperscript{799} See footnote 66 above.

\textsuperscript{800} The activities of e-money institutions are set out in Article 6 of the Directive. A summary of these activities refers:

(a.) Provision of payment services;
(b.) The granting of credit related to payment services;
(c.) The provision of operational services and closely related ancillary services for the issuing of e-money or the provision of payment services;
(d.) The operation of payment systems, and
(e.) The rendering of business activities other than e-money, with regard to the Community and national law.

\textsuperscript{801} Article 3(5) of the Directive. The possibility, however, exists where the requirements under Article 17 of the Directive are met.
not applicable to those institutions that are subsidiaries of a holding company located outside of the respective state’s territory.\textsuperscript{802}

As against cyberlaundering, however, this might be difficult to regulate or enforce in practice, given the transnational nature of the problem. This creates the possibility that cyberlaunderers who run enterprises that fit the definition of e-money institutions may be able to continue rendering such services abroad under different aliases or using trusted smurfs. In the end, the veil is not pierced and the transnational shield for cyberlaunderers remains strong. More importantly, for our purposes, the Directive does not exactly set a limit on the value stored on the relevant electronic payment instrument. This is left for member states to determine.\textsuperscript{803} There is, however, solace in the fact that a monetary limit should be determined, as opposed to where several e-money service providers do not set a limit deliberately in order to entice customers. But the fear that countries might set unreasonable high value thresholds still exists. Having an almost ‘capless’ e-payment instrument has the potential of fostering cyberlaundering.\textsuperscript{804} This is why a minimum and maximum threshold should be set as well to give even more effect to the purposes of the Directive.

Overall, while the notion of e-money institutions as stated in the Directive serves as the much needed basis upon which the exponential exploitation of e-payment systems for cyberlaundering operations can be curtailed, the

\begin{flushleft}
\textsuperscript{802} Article 8(1) of the Directive.
\textsuperscript{803} Article 9(1) of the Directive.
\textsuperscript{804} See discussion in Chapter 3, paragraph 3.3.3.2.
\end{flushleft}
loophole is only filled from one side. This is because the Directive has only a regional scope. Outside of Europe, the notion of e-money intuitions remains an alien concept for many other countries, both in concept and practice.805 This study thus proposes that the legal framework for e-money institutions, as contained in the Directive, should be adopted into international and national laws. Defining the parameters is a corollary to regulation, and establishing e-payment institutions to operate separately from the traditional notion of financial institutions goes a great length in curtailing and containing the illegitimate uses of e-payment systems.

5.5.2.3.2 Stricter controls for smart cards

Further to the prior discussion, a closer look into smart cards is necessary. With the steady rise of prepaid or smart cards as a means of payment,806 and given the fact that this has become a viable method through which cyberlaundering takes place,807 it only follows that the loopholes in this system that sustain illegitimate activities should be eliminated. To rehash a

---

805 Even within Europe, the Directive itself is relatively new. The obligation upon member states to enact its stipulated measures came into effect on 1 April 2011, and as with the enactment of new laws, enforcement challenges that exist within every sovereign institution remain a bane to the effectiveness of the Directive. In the United States (US), a new kind of money services business is being considered known as ‘provider of prepaid access,’ which does not take the form of e-money institutions as set out in the EU, but only seeks to close some gaps in the regulation of e-payment systems. Notably, as opposed to the EU directive, the new system adopted by the US excludes certain low value prepaid programs. Cf Financial Action Task Force (2010D: 52) and Federal Register ‘Proposed Collection; Comment Request; Renewal with Changes to a Currently Approved Collection; the Registration of Money Service Businesses (MSB); FinCen Report 107, To Incorporate Changes to The MSB Definitions and Add Provisions for Prepaid Access’ (an internet web page dated 10 June 2010) available at <https://www.federalregister.gov/articles/2011/10/06/2011-25607/proposed-collection-comment-request-renewal-with-changes-to-a-currently-approved-collection-the> [accessed on 20 April 2011].

806 See discussion in Chapter 3, paragraph 3.3.3.

807 See discussion in Chapter 3, paragraph 3.3.3.2.
few salient points: smart cards are problematic because transactions are often not followed or monitored, and, as opposed to the traditional notion of a financial institution, there is no central reporting system to conduct the needed oversight. The problem is further compounded by reason of the fact that merchants who offer smart card services are usually unscrupulous and do not engage in the necessary vetting process for new or potential customers.

This is another side-effect of not having e-money institutions under which such merchants would fall, subjecting them to adopting the requisite AML systems.

The problem with smart cards also crops up when one considers the applicability of the AML’s rationale on simplified CDD measures. The FATF’s Recommendation 10 provides that financial institutions should undertake CDD measures. There is, however, a caveat to this rule that permits some flexibility in its application: (1) For certain financial activities that are proven low risk, which includes a financial activity that is carried out by a person on an occasional basis, the CDD measures may be not be applied, and (2) Reduced or simplified CDD measures may be carried out for low risk cases.

Therefore, where a particular financial activity is considered low risk or performed occasionally, no CDD measures apply, whilst, to the contrary,

---

808 See discussion in Chapter 3, paragraph 3.3.3.2.
809 See discussion in Chapter 3, paragraph 3.3.3.2.
where an activity is not low risk or not performed occasionally, the standard CDD measures apply. Accordingly, simplified CDD measures are applicable where the financial activity in question is deemed or judged as low risk. The problem with this rationale surfaces through the medium of electronic payment systems, where transactions involving smart cards are deemed low risk in many jurisdictions. As a result, the majority of these transactions fly under the radar, and are not subject to the application of standard CDD measures. Also, if not completely exempted, at the discretion of the relevant authority conducting a risk assessment, reduced CDD measures may be applied to transactions involving smart cards. When it comes to smart cards, such classification that determines the applicability or inapplicability of CDD measures are not quite as effective due to the fact that smart cards have the potential to perform structured transactions, and transactions can be structured under a particular designated threshold with numerous smart cards, thereby boycotting the applicability of set CDD standards. This is a significant loophole, which, again, points to why the present AML system for this system needs to be adapted to suit imminent needs.

Other than the regulatory possibilities through adapting the existing AML legal system, prepaid service providers who issue smart cards should be subject to the same CDD and KYC measures by which financial institutions

---

812 For example, in Australia, transactions with smart cards involving amounts falling below 1000 Australian Dollars are completely exempt from the application of AML laws [Section 6(2) of the Anti-Money Laundering and Counter-Terrorism Financing Act of 2006]. The EU takes a much wider approach, as it regards transactions with smart cards as financial activities, regardless of any value limit on the smart card. As a result, these transactions fall within the purview of AML laws. However, for designated cases of low risk, simplified CDD measures are applied (Article 11 of Directive 2009/110/EC).
must abide. Just as is evident in Article 2 of the German Banking Act of 1998 (\textit{Gesetz über das Kreditwesen Kreditwesengesetz} - \textit{KWG}), which extends CDD measures to prepaid service providers, this measure should be adopted across the board.\footnote{Cf discussion in Chapter 4, paragraph 4.3.3.2.}

Also, the smart card should be addressed as a sole entity, given its unique characteristics and features. Attention should be paid to the existing regulatory systems and how a solution should be carved to solve the dilemma. Mentioned briefly is how the DEA has influenced the State of Nevada to adopt the SB-82 law, which now enables law enforcement authorities to investigate suspicious smart card transactions and freeze the stored value in these cards when a criminal is caught with them.\footnote{See discussion in Chapter 4, paragraph 4.3.3.5.3.} This system is key to regulating smart cards, and signals why government authorities should take up the reins of regulation, where parties and individual proprietors are not willing, because of corporate interests. Whilst this study strongly recommends the much-needed adoption of the SB-82 law for the regulation of smart cards, it is not oblivious to the herculean nature of its practical enforcement on a broad scale.\footnote{This ties in with the discussion on enforcement challenges faced in the regulation of cyber-laundering. See previous discussion in paragraph 5.3.3 above. See discussion in Chapter 3, paragraph 3.3.3.2.} This is why it might be difficult to regulate smart cards by limiting their functions and capacities, by, for instance, ensuring that there is a cap on the amount that can be loaded onto these smart cards.
cards, contrary to what exists currently.  

Although one could argue that by limiting the functions and capacities of smart cards the very essence of their innovation is gradually eroded, weighed against the dangers they harbour, especially in their perpetuation of cyberlaundering operations, the latter argument would not hold water. Thus, this study recommends strongly that the value of smart cards should be restricted to a particular amount, by restricting its turnover limits and by limiting the number of smart cards per customer.  

Though this might seem quite probable in lieu of regulation, such measures can still be circumvented in a world of smurfs, where smurfs having smart cards registered in their own name can be operate for the benefit of the main party who facilitates the crime. Moreover, this is likely to cause an uproar amongst merchants of smart card services, as this might conflict with their corporate interests.

5.5.2.3.3 Fusing the money-trail with the bit-trail

The philosophical and sociological aspects of money centres around the notion of exchange, which gradually developed as a corollary to human needs and wants, becoming what society now accepts as legal tender. The latter concept - legal tender - is, by definition, one that is a medium of payment allowed by law or recognized by a legal system to be valid for meeting a

---

816 For example, for the purpose of enticing customers, a smart card company known as the Freedom Eagle Card does not place a limit on the amount of value to be loaded onto the smart card.

817 Cf Ping (2004: 50) and Straub (2002: 534).

818 See footnote 76.
financial obligation.\textsuperscript{819} This concept forms what is known as the money-trail, which exists today in the form of paper currency, such as US Dollars, the British Pound Sterling, the European Euro, and so on. However, with the advent of modernization, which has spawned technology, and which in turn has revolutionized and defied old norms and conventions, money now exists in the form of the bit-trail. The bit-trail is essentially what has been the thrust of this study, which is the e-payment system, or, more specifically, e-money. Whether or not the bit-trail follows as a legal tender, just as the money-trail, is contentious, depending on the relevant region, state or society and the intentions of the parties involved.\textsuperscript{820} The bit-trail, because of its technological ambit, is a contrast to the money-trail, not developing along its lines and its form, and given its widely varying nature, both mediums of payment continue to grow apart. This also explains why the financial regulatory authorities of different governments cannot apply their financial laws, which include AML laws, directly to the obtuse bit-trail.

This reality prompts the rationale that this study posits, which is that the money-trail should be fused with the bit-trail as a long-term solution for the problem of regulating e-payment systems. This would force the bit-trail under


\textsuperscript{820} Following the logic of trade by barter, in terms of which parties to a trade agreement can elect any object as choice payment for the relevant goods, the same logic holds with e-money. Accordingly, as long as both parties have a unified intention on the object of payment, the issue of legality plays a minor role. However, for the purposes of control and regulation, the legality and, or, illegality of the object of payment becomes important. We have seen above, through the EU Directive 2009/110/EC, that the issue of e-money now falls within the purview of regulation, and the argument holds that e-money now fits the frame of a legal tender, at least as far as the EU is concerned.
the broad financial regulatory umbrella that currently exists for the money-trail. Just how feasible this can be, is what is left to determine.

Historically, this idea seems to have existed, but was never brought into practice. In the year 2001, the European Central Bank engaged in discussions with certain technological firms in order to embed the Radio Frequency Identification (RFID) microchips in the high-denomination euro notes, at the time of the latter’s conception.\(^{821}\) Although at the time, the technology was available to bring this to fruition, the project did not materialize. Had it materialized, the anonymity feature of the money-trail would have been stripped away, and every bank note having the RFID chip would have carried its own record. Also, by virtue of the RFID chip embedded in currency notes, there is a possibility that the chip number can be used as payment online. By having such mixed forms of electronic and physical money, and where the money can be used as legal tender in cyber space, governments would have been able to permeate the ghostly nature of e-payment systems by merging the traditional money-trail with the growing elusive bit-trail. Essentially, another way of interpreting this solution is that e-money should be brought under the present AML legal regime.

\textbf{5.5.2.4 Regulating online gaming}

The internet today is littered with all sort of activities to preoccupy one’s time. As a kryptonite to many a game addict, there is always the ‘fun

element’ inherent in these activities, which is never lacking, although, amongst these millions, there are some who mischievously exploit such activities for their nefarious operations. The activities in question here include virtual worlds and online gambling, which are the main areas for online gaming; and a fraction of the millions of people in question are cyber launderers. Being one of the very problematic aspects of cyber laundering, for which a concrete ACL legal regime is sought, regulatory measures for virtual worlds and online banking are explored in depth below.

5.5.2.4.1 Measures against the avenue of virtual worlds

As discussed previously, a virtual world is an online gaming platform belonging to the family of Massively Multiplayer Online Role Playing Games (MMORPGs), and it allows players to simulate practically all aspects of reality on a virtual platform, enhancing interactions through their avatars. Of the many dangers that this heralds, the current AML legal infrastructure does not extend to virtual worlds. For example, virtual worlds create the possibility of tax evasion, especially with the possibility that in-world money exchange services, such as the Second Life’s Xstreet allows for virtual

---

822 For prior elaborate discussions on virtual worlds, see Chapter 3, paragraph 3.5.5.
823 For prior elaborate discussions on online banking, see Chapter 3, paragraph 3.5.3.
824 See Chapter 3, paragraph 3.5.5.
825 Cornelius and Hermann (2011: v), and Klimmt (2011: 3). Cf Chapter 3, paragraph 3.5.5.
826 This principle is constituted in the fact that players, called ‘ Residents’ in the virtual world, are not charged value added tax (VAT) when transacting with fellow residents, but are only charged this when conducting transactions with third parties. This rationale can be found in Article 1 of the Council Directive of the European Union 2002/38/EC, which was adopted by the European Union Council on 7 May 2002 and came into force on 1 July 2003. Cf discussion in Chapter 3, paragraph 3.5.5.
currencies to be changed to real-world money.\footnote{827}{See discussion in Chapter 3, paragraph 3.5.5.} Also, anonymity is a principal feature of virtual worlds, due to the very indistinct nature of human representation on such platforms through the use of avatars.\footnote{828}{See discussion in Chapter 3, paragraph 3.5.5.} In addition, virtual worlds perpetuate the possibility of smurfing or structuring transactions; put in the other words, virtual worlds help with the layering of illicit funds.\footnote{829}{See discussion in Chapter 3, paragraph 3.5.5.}

In light of the discussion in the preceding chapter, where it is established that there is currently no legal framework in existence to contain the dilemma of the cyberlaundering,\footnote{830}{See discussion in Chapter 4, paragraph 4.3.3.} as is the purpose of this study, virtual worlds are currently beyond the reach of existing AML legal frameworks. In effect, this leaves several pertinent questions unanswered, key of which is how these virtual worlds can be regulated to prevent the possibility of their use for cyberlaundering.

Given the above, and for want of laws that should address the problem directly, this study posits that internal control of virtual worlds should be strengthened, with adequate oversight from outside authorities with a designated mandate. As a potentially viable solution, some of these internal measures deserve some elaboration.

The first point of call where internal control is needed are the financial institutions in virtual worlds that are wholly unregulated, which is a grave oversight, considering the massive combined value of virtual economies that
are currently north of US $18 billion\textsuperscript{831} (in real-money, of course). ‘Virtual banks’ should be made subject to the same regulations and control to which terrestrial banks are currently subjected, although this is quite challenging in reality to expect virtual banks to adhere to record-keeping and reporting requirements.\textsuperscript{832} Nevertheless, a reasonable attempt would undeniably be the first step in addressing the vulnerability and blocking the awfully gaping loophole. Few financial authorities are awakening to this reality, and having begun to feel the pinch, AML compliance is now required for certain virtual banks. For example, recently, the company behind Entropia Universe, MindArk, obtained permission from the Swedish Financial Authority to conduct legitimate banking activities in its virtual world.\textsuperscript{833} In effect, proper scrutiny is ensured in line with the existing AML system. This also implies that the Swedish Financial Authority would conduct supervisory oversight over the activities of virtual banks in Entropia Universe, as the designated third party with the requisite authority. Companies behind other virtual worlds, such as SL, are yet to obtain such a license. If this initiative is made uniform across all jurisdictions, and the requisite authorities are able to ensure compliance, the threats posed by virtual banks would be lessened considerably.

\textsuperscript{832} This links back to the discussion on the intangibility of the internet, which aids cyberlaundering. See paragraph 4.2 supra.
\textsuperscript{833} Mindark (2009: 4). One factor that facilitates this is the strict and increasingly rigid nature of the Swedish financial system, to which companies, such as MindArk - a Swedish company – are subjected. In other jurisdictions, there is no such obligation where several other companies which develop virtual worlds are located.
Apart from the possibility of legal regulation from outside authorities, one needs to also consider the possibility of internal legal regulation. One legal issue here is whether the internal rules and regulations of a virtual world carry any legal weight, or whether they can be decisive in deterring cyberlaundering. As with competitive sports, the rules of the game define the particular sport or game. These rules must be obeyed as they apply to all players of the game, and they also distinguish the particular sport from other sports. The rules exist to protect the interests of all players, both actively and passively. It follows that the obligation to adhere to these rules, which can be said to be soft law, is only incumbent on the players of the game, and does not apply to unrelated third parties. Violating the rules attracts sanctions. For the purposes of the ACL campaign, this can be seen in a positive light. Where the companies behind these virtual worlds are able to incorporate certain AML measures into the rules of the game, such as compulsory reporting or identity disclosure, players are forced to comply when conducting activities and performing transactions in the virtual economy. This could as well mean that dubious activities in virtual worlds can be deterred extensively.

More importantly, for effective regulation, the control measures proposed should involve both operators of virtual worlds and law enforcement authorities, and both parties must work together. For instance, operators of

virtual worlds should also be compelled to file suspicious transaction reports (STRs) to the necessary Financial Intelligence Units (FIUs). However, given the problem of corporate interests, as discussed earlier, and also given the likelihood that these rules could be circumvented by clever residents, the solution proposed is not without challenges.

5.5.2.4.2 Measures against the avenue of online gambling

Unlike virtual worlds, the fact that unscrupulous online casinos are warehouses for cyberlaunderers is no secret. This is because of the clandestine nature of online casinos. Cyberlaundering is achieved through online gambling, by either using an online gambling service which might appear legitimate, or by setting up an online gambling website for the purpose of having the dirty funds cleaned. Given that online casinos are invariably informal financial institutions that fit the traditional frame of financial institutions, save for the wagering cloak under which they operate, one wonders why they are not subject to the same scrutiny as traditional financial institutions. Following the adaptive approach to regulation, online casinos should be brought under the current AML legal regime. This can be done by adapting existing local and international AML laws. These laws should

---

837 Cf Financial Action Task Force (2010D: 8), the Egmont Group (2004E: 2), Jamali (2009: 48) and Muller (2007: 87). The FIU is the brain child of The Egmont Group, which is an informal body of government receiving agencies that share a common goal of providing a forum to enhance mutual cooperation and to share useful information in detecting and combating money laundering. See detailed discussion on the FIU and the Egmont Group in Chapter 4, paragraphs 4.2.2.1.1 and 4.2.2.2.3.

838 See paragraph 5.3.1 above.

839 See discussion in Chapter 3, paragraph 3.5.3.

840 See discussion in Chapter 3, paragraph 3.5.3. Cf Bumeter (2001:2) and Schopper (2002: 310).
ensure that online casinos are not only compelled to adhere to entrenched AML standards, such as reporting an record-keeping, but that the laws themselves should be wholly dedicated to the operations of casinos. What should be prevented is a situation where the laws serve only a perfunctory role. One way of achieving this is by ensuring uniformity of practice. This requires ensuring that the wagering activities of online casinos are not subject to variables which can be manoeuvred easily at will, as is the case today, but that they have a uniform practice of set guidelines, both for the actual gaming activities and the management of the casino. To this end, all online casinos should belong to a central associative body compulsorily. This body should ensure that casinos are run in line with a well-entrenched manifesto, with rules and guidelines that includes the requisite AML measures. This associative body could be national or international.\footnote{Having an international body or association of online casinos would seem more feasible given the transnational nature of the online casino business, even though national branches could be established as well. Such an association can be created by an international agreement, such as by a treaty or convention. However, given the discussion in paragraph 5.3.4 above on the problems associated with the roots of cyberlaundering (i.e. money laundering and cybercrime), part of which explains how there is yet to be a truly international legal infrastructure against cybercrime, the implementation of the solution proposed becomes a challenge in practice.} Also, as it should be endowed with some measure of autonomy and influence, it must serve the interests of online casinos as a whole. This body could be vested with supervisory power that would help to ensure adequate oversight of online casinos. This would deter criminals from creating online casinos at sheer whim for the purposes of ‘washing’ ill-derived funds.\footnote{See Chapter 3, paragraph 3.5.3, for how the easy creation of online casinos fosters its vulnerability to cyberlaundering operations.}

---

841 Having an international body or association of online casinos would seem more feasible given the transnational nature of the online casino business, even though national branches could be established as well. Such an association can be created by an international agreement, such as by a treaty or convention. However, given the discussion in paragraph 5.3.4 above on the problems associated with the roots of cyberlaundering (i.e. money laundering and cybercrime), part of which explains how there is yet to be a truly international legal infrastructure against cybercrime, the implementation of the solution proposed becomes a challenge in practice.

842 See Chapter 3, paragraph 3.5.3, for how the easy creation of online casinos fosters its vulnerability to cyberlaundering operations.
The implementation of such a measure would have to take account of the challenges identified earlier, such as the possibility that this will encroach on well-guarded corporate interests.\textsuperscript{843} Some of these interests include protecting the very profitable business of online gambling,\textsuperscript{844} and maintaining the clientele. In addition, online casinos registered in off shore in countries with very weak AML laws.\textsuperscript{845} As such, this might nip the potential for effective regulation.\textsuperscript{846}

5.6 COMPLIANCE PILLAR FOR THE ACL LEGAL REGIME

The compliance pillar advocated in this study proceeds from the standpoint that there are established laws to be complied with. Although it is one thing to have such laws in place, that alone is not enough.\textsuperscript{847} To ensure compliance, one could learn from the FATF, which places a high premium on having competent and well-resourced authorities, including effective supervisory bodies.\textsuperscript{848} It therefore follows that the notion of compliance is a duty

\textsuperscript{843} See discussion in paragraph 5.3.1 above.
\textsuperscript{844} The online gambling business bourgeons currently as a multi-billion dollar industry, with a net-worth equivalent to the gross domestic products (GDPs) of most developing countries. See Chapter 3, paragraph 3.5.3 for more details.
\textsuperscript{845} Cf discussions in paragraph 5.3.3 and paragraph 5.5.1.1.2. For example, Antigua, Surinam and the Netherland Antilles, as well as some African countries are known territories where most online casinos sites are registered.
\textsuperscript{846} The nature of the problem depends largely on the respective jurisdiction and the effectiveness of the AML laws in place there. For example, due to imminent dangers, the US has gone as far as banning online gambling (albeit only in certain respects) 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. With some pressure from the FBI, in 2007, Linden Labs took an unprecedented step by banning online gambling in Second Life [Jamali (2009: 42)]. Banning online gambling completely might well be the last available solution, should the situation spiral out of control.
\textsuperscript{847} Cf discussion in Chapter 4, paragraph 4.2.2.
incumbent upon persons having a duty to comply on the one hand, and, on the other hand, persons who are meant to ensure compliance.\textsuperscript{849} The discussion now turns to compliance with regard to cyberlaundering. It focuses on the two compliance-bound groups.

\textbf{5.6.1 Duty to comply}

As indicated previously, within the AML legal framework, the duty to comply rests upon financial institutions,\textsuperscript{850} their clients and beneficial owners;\textsuperscript{851} mutual funds and pooled investment vehicles such as hedge funds, private equity funds, unit investment trusts, corporations, trusts and partnerships;\textsuperscript{852} and other designated non-financial businesses such as lawyers, notaries, accountants, dealers in precious metals and stones, and real estate agents.\textsuperscript{853} For the campaign against cyberlaundering, the duty to comply not only includes these parties named above, but also, such duty should be placed on the following individuals and entities:

a) Internet service providers and their proprietors;

b) Facilitators of e-payment systems, including prepaid card companies, electronic currency businesses (i.e. online barter traders)\textsuperscript{854} and their

\textsuperscript{849} Cf discussion in Chapter 4, paragraph 4.2.2.
\textsuperscript{850} Cf Chapter 4, paragraph 4.2.2.1, for the adoption and meaning of the term ‘financial institutions’, which takes on the meaning outlined by the FATF. Cf Financial Action Task Force (2003: 16) and Financial Action Task Force (2012A: 115).
\textsuperscript{851} Cf Chapter 4, paragraphs 4.2.2 and 4.2.3.1.1.
\textsuperscript{852} Cf Chapter 4, paragraphs 4.2.2 and 4.2.3.1.3.
\textsuperscript{853} Cf Chapter 4, paragraphs 4.2.2 and 4.2.3.1.1.
\textsuperscript{854} Cf discussion in Chapter 3, paragraph 3.5.3.
proprietors (i.e. e-money institutions); their agents, merchants of prepaid funds, other e-money service providers, and, more generally,
c) All individuals who are benefactors of the internet service provided, and who are customers or users of the electronic payment service provided.

The aforementioned parties in all three categories are only one part of the compliance equation. Where compliance can be guaranteed from this group, then one part of the compliance issue is solved. This can be done by requiring the creation of an oversight mechanism, which would ensure that this is guaranteed. However, this can only be guaranteed by persons upon whom the duty to ensure compliance is incumbent.

5.6.2 Duty to ensure compliance

The guardians of the present AML legal regime who bear the onus of ensuring compliance with set laws and regulations are also indispensable to the ACL legal regime, as they should play the same role. Essentially, these persons include governments and their relevant authorities and agencies, such as investigative and prosecutorial authorities, Financial Intelligence Units (FIUs) and other regulatory agencies. However, the peculiarity of cyberlaundering crops up here once again, as the avenues exploited for cyberlaundering operations do not necessarily fall within the regulatory scope within which these authorities normally have oversight. This is due to the fact that the cyberlaundering avenues that are being exploited are private-owned
enterprises whose operations are not constrained by the work of public regulatory authorities.

Hence, the duty to ensure compliance should be extended to these parties as well (i.e. internet service providers, as well as facilitators of electronic payment systems and their proprietors). Consequently, this duty should apply to operators of online banks, online auction sites, online barter traders, virtual worlds and online gambling websites. Adequate internal oversight mechanisms should be put in place by these private entities, in order to ensure that their websites and products are used for legal purposes only. This can be done by having effective administrative infrastructures that allow for supervisors and managers to be more aware, vigilant and discrete in their respective businesses. This militates against potential cyberlaundering risks. This measure also requires the parties having a duty to ensure compliance to carry out stringent vetting process, and to conduct customer due diligence (CDD) measures which, essentially, necessitates customer verification.\footnote{The necessary CDD measures and other preventive measures are discussed under the prevention pillar in paragraph 5.4.2 below, given as the goal of this section is to only identify the key actors of the compliance pillar and not the functions itself.} 

A third party authority should also be on hand to ensure that the persons upon whom a duty lies to ensure compliance are also complying with such a duty. Persons or entities with a duty to ensure compliance should also be supervised to ensure that their duty to ensure compliance is observed. This
strategy can be called ‘supervising the supervisor.’ It is one role for which the FATF and the regional FATF-Styled Regional Bodies can be credited.\footnote{Cf discussion in paragraph 5.1.1.3 above. This initiative could also work outside of the supranational sphere where the FATF and the FATF-Styled Regional Bodies play a major role, by ensuring compliance from countries. The initiative should be transposed as well into the national sphere. Governments, or government-created entities, should be established to ensure the requisite supervision. Thus, national jurisdictions should be tasked with this initiative by ensuring that the requisite infrastructures are in place to ensure compliance. For example, in 1998, under the Clinton administration in the US, the Internet Corporation for Assigned Names and Numbers (ICANN) was created. The corporation is tasked with the management of Internet Domain Names and Internet Protocols (IP) addresses, as well as the fostering of operational stability of the internet. Being a broad range of stake holders that include government representatives, business organizations, independent consultants and academics, ICANN is concerned mainly with the regulation of formal or structural aspects of the internet, without giving consideration to website contents or activities. ICANN plays a significant role in identifying websites that are operating without the requisite license. Granted that these websites are vehicles for cyberlaundering operations, a government infrastructure such as ICANN would help in the regulation of cyberlaundering. For more information on ICANN, see ICANN (the Internet Corporation for Assigned names and Numbers) ‘About Us’ an undated internet webpage available at <http://www.icann.org/en/about> [accessed on 2 May 2012]. Yar (2010: 16). Cf Mueller (1999: 497).}

The compliance pillar is thus the foundation that guarantees and fortifies the other two pillars of the ACL legal regime.

5.7 SUMMARY

This chapter sets out the concrete regulatory measures for cyberlaundering. But it takes account of the potential problems along the way that pose a threat. An adaptive approach is employed for the regulation of cyberlaundering. According to this approach, two of the existing pillars holding the current AML legal regime (i.e. prevention and compliance pillars) are amended to cater for the cyberlaundering dilemma. In keeping with this approach, two broad methods are recognized for the regulation of the problem: a general approach which identifies broad measures that could help in regulating cyberlaundering, and a target approach, which addresses directly

\footnote{Cf discussion in paragraph 5.1.1.3 above. This initiative could also work outside of the supranational sphere where the FATF and the FATF-Styled Regional Bodies play a major role, by ensuring compliance from countries. The initiative should be transposed as well into the national sphere. Governments, or government-created entities, should be established to ensure the requisite supervision. Thus, national jurisdictions should be tasked with this initiative by ensuring that the requisite infrastructures are in place to ensure compliance. For example, in 1998, under the Clinton administration in the US, the Internet Corporation for Assigned Names and Numbers (ICANN) was created. The corporation is tasked with the management of Internet Domain Names and Internet Protocols (IP) addresses, as well as the fostering of operational stability of the internet. Being a broad range of stake holders that include government representatives, business organizations, independent consultants and academics, ICANN is concerned mainly with the regulation of formal or structural aspects of the internet, without giving consideration to website contents or activities. ICANN plays a significant role in identifying websites that are operating without the requisite license. Granted that these websites are vehicles for cyberlaundering operations, a government infrastructure such as ICANN would help in the regulation of cyberlaundering. For more information on ICANN, see ICANN (the Internet Corporation for Assigned names and Numbers) ‘About Us’ an undated internet webpage available at <http://www.icann.org/en/about> [accessed on 2 May 2012]. Yar (2010: 16). Cf Mueller (1999: 497).}
the problematic areas of cyberlaundering. The prevention and compliance pillars of the ACL legal regime should be built in line with the AML legal regime. By adapting the rules and standards of the current AML legal regime to cater for cyberlaundering, and in some instances creating new ones, invariably, the ACL legal regime is formed. Hence, the ACL legal regime is a variant of the current AML legal regime. The main rationale that underscores the proposed regulatory framework against the menace of cyberlaundering is that a new legal framework needs to be created and existing standards need to be adapted. In the long run, the regulatory measures outlined in this study do not only add significantly to the ACL legal regime but to the broader fields of money laundering and cybercrime as well.

However, the ACL legal regime cannot rest on the two pillars of prevention and compliance alone. Accordingly, the discussion is not complete, because the enforcement pillar, which embodies certain prosecutorial issues related to cyberlaundering, such as the investigative and jurisdictional issues of cyberlaundering, has not been discussed. This crucial issue is dealt with in the next chapter.
CHAPTER 6

PROSECUTING CYBERLAUNDERING

6.1 INTRODUCTION

This chapter deals with the enforcement pillar of the anti-cyberlaundering (ACL) legal regime. Much like the preceding chapters of this study that attempt to pave an untreaded path in the law and unravel a novel issue currently unexplored, this chapter takes the ACL campaign a step further by exploring legal ramifications pertaining to the prosecution of cyberlaundering. It completes the discussion on the pillars of the ACL legal regime, and complements the prevention and compliance pillars discussed in the preceding chapter.

The chapter begins by identifying certain important issues and challenges that come with the prosecution of cyberlaundering. Under the enforcement pillar, this chapter discusses investigative and jurisdictional issues, borrowing from similar principles falling under the current anti-money laundering (AML) legal regime. In establishing the enforcement pillar, this chapter also follows the adaptive approach to regulating cyberlaundering, as posited in the preceding chapter. Given that the current AML legal regime does not cater for this, the adaptive approach employed here also requires a probe into how current anti-cybercrime (ACC) laws can be adopted, as the prosecution of cyberlaundering cases does not only require the mind of money laundering

---

857 See discussion in Chapter 5, paragraph 5.1, and Chapter 4, paragraphs 4.2.1 and 4.2.4.
858 See discussion in Chapter 5, paragraph 5.4.
investigators, but also cyber forensic experts who have tactical intelligence on hi-tech criminality, such as cyberlaundering demands. This chapter further discusses recent case studies that provide evidence of the urgent need for a proper ACL prosecutorial policy. Certain technical issues or formalities involved in establishing the ACL legal regime complete the discussion on the enforcement pillar.

6.2 PATH TO PROSECUTING CYBERLAUnderING: ISSUES AND CHALLENGES

The issue of prosecution is one of the many distinguishing factors that set cyberlaundering apart from the conventional notion of money laundering. This is because cyberlaundering has a significant technological ambit to it. Its uniqueness can, therefore, not warrant a typical apple to apple comparison in the area of prosecution, when compared to the traditional concept of money laundering. Prosecutors using traditional lenses are sure to find nothing. As regards its investigation, one needs to rely mostly on the investigative tactics applicable to cybercrime for two main reasons: First, in most cases, cyberlaundering investigators handle electronic evidence which, for detection, requires a cyber forensic mind. Secondly, as is a characteristic of cyberlaundering, the playing field is mainly the internet. This is why it is important to identify the issues and challenges on the path to the effective prosecution of cyberlaundering. Some key obstacles to the effective prosecution of cyberlaundering include certain practical and logistic
considerations, the problem of obtaining the cooperation of witnesses, the privacy argument; the nature of electronic evidence, and its admissibility in court. These issues are discussed further below.

6.2.1 Practical and logistic challenges

Cybercrime is trans-border in nature. This is because the internet, which is the playing field, is transnational in nature.\textsuperscript{859} This rationale is equally valid for cyberlaundering. When conducting investigations across national borders, certain practical problems are sure to crop up that would cause delays and expenses. For example, given the time difference between jurisdictions, investigators might be forced to arrange teleconferences with people in different countries at inconvenient times.\textsuperscript{860} This would not be an issue if the crime were local in nature.

Also, there is the language barrier. Information obtained from other countries might be in a different language, and translation services might be required. This is a stumbling block to speedy and efficient prosecution, especially where the relevant law enforcement agency lacks the resources. This situation is further compounded when witnesses, who speak foreign languages, are transported across jurisdictions for purposes of prosecution. This not only retards the prosecution, but it also increases the costs of the criminal process.

On a more poignant note, there is the issue of political will which, where lacking, might amount to a failed hope for the prosecution of

\textsuperscript{859} See discussion in Chapter 3, paragraph 3.2.2.4.
cyberlaundering. The issues of political will and lack of means are recurring themes when it comes to broad discussion of the ACL legal regime, and are also problems that are common to all pillars of the current AML legal regime. 861

6.2.2 The right to privacy

Fundamental human rights have always been long-standing tenets of a democratic state. One of these is the right to privacy. However, given the exigencies of safeguarding security in the public interest, the question that arises in this context is this: To what extent should the privacy claim prevail when pitted against the right of law enforcement agencies to pry into electronic communications for the purpose of safeguarding the public interest value of security? If the scales are tipped in favour of privacy, then the right to privacy could very well be an obstacle to effective prosecution of cyberlaundering, especially during the investigative phase. In finding a right balance, some key issues need to be brought to light. These are discussed further below.

6.2.2.1 Personal information and new electronic devices

One’s personal information is often a good starting point for law enforcers conducting cyberlaundering investigations. However, one’s presence on the internet is known only to the extent that the information is fed into the

861 For a detailed discussion of these factors, see Chapter 5, paragraph 5.3.3.
internet. In this day and age, with the exponential development of technology, and the increasing use of electronic devices and social media platforms that often require a particular measure of personal information, one’s privacy is curtailed to some extent. With increased growth of the so-called data-banks and their inter-connections, as well as the memory capacity of electronic archives, more personal data can be stored for much longer periods of time. Even more, personal data can be gathered without the personal knowledge or consent of internet users, due to the fact that small pieces of software, known as cookies, can be downloaded onto the relevant computer the moment certain web pages are visited. This explains why investigators in the prosecution of cybercrime are keen to seize the computer used. The capacities of new electronic devices and the internet render internet users vulnerable to the risks associated with their use, chief of which is the potential violation of personal privacy. However, what might seem as a disadvantage in the use of computer systems, is an advantage for law enforcement agencies, due to the fact that the amount of information recorded onto a computer system would be of great help to law enforcers and investigators who are able to identify victims, thus linking the crime to the criminal. Viewed from this perspective, the danger of violating one’s privacy is not necessarily a barrier to prosecuting cyberlaundering.

---

A databank is synonymous with a database, and it implies an electronic repository of information classified into different subjects, in order to facilitate the use and quick retrieval of deposited information when required.


See the discussion in paragraph 6.4.4 below.
6.2.2.2 The legal protection of personal data versus investigative needs

Every country has its own privacy laws to protect personal data. All categories of personal data are protected, including electronic traffic data,\(^{865}\) data on location,\(^{866}\) video-surveillance and biometric analysis,\(^{867}\) and genetic data.\(^{868}\) These laws are meant to regulate the extent to which one’s privacy is protected by indicating permissible and impermissible situations regarding access to electronic records and communications. For example, in South Africa, the Electronic Communications and Transactions (ECT) Act\(^{869}\) stipulates instances when electronic communications may be intercepted.\(^{870}\) Similarly, the Regulation of the Interception of Communication and the Provision of Related-Information Act\(^{871}\) (RICA) lists analogous provisions. In the United States (US), the Right to Financial Privacy Act\(^{872}\) (RFPA) and the Electronic Communications Privacy Act\(^{873}\) (ECPA), together, regulate most aspects of personal data protection. The RFPA focuses more on the requisite prior authorization that law enforcers need to have before obtaining an

---

\(^{865}\) Electronic traffic data refers to data on telephonic and electronic traffic, such as information via telephonic terminals (i.e. calls on fixed landlines and mobile networks), as well as fax, short message service (sms), multimedia message service (mms), and electronic mails (emails).

\(^{866}\) As the name suggests, data on location refers to data relating to the location or geographic site of the electronic communication device used.

\(^{867}\) This refers to personal information that can be accessed from video-surveillance installations, which are ideally meant for the protection of persons and property. These tallies with biometric analysis which enables law enforcers to assess the geometry of the face, irises. The acquired information can then be compared with data previously recorded. Busia (2004: 87).

\(^{868}\) Genetic data refers to information that can be derived from an individual by virtue of the person’s genome or hereditary information. However, the argument holds that genetic data could incur the risk of discrimination and racial profiling. Busia (2004: 88) and Solove (2011: 59).

\(^{869}\) Act 25 of 2002.

\(^{870}\) See sections 51 and 52 of the Act.

\(^{871}\) Act 70 of 2002. See sections 2 to 11.


individual’s financial records from financial institutions. On the other hand, the ECPA prohibits internet service providers from dispensing the details of one’s electronic communications. These laws are found in both common law and civil law jurisdictions. On the other side of the pendulum is the public interest consideration. As an underlying rationale, specialized investigative agencies are the protectors of laws and the guardians of freedom. They are empowered to ensure that the security of the state and its people is guaranteed, and that society is protected from crime. This right is a collective right to which a society, and not just an individual, can lay claim. The protected interest in the crime of cyberlaundering is a combination of certain public interest values, such as the protection of organs of state and their processes and ensuring the stability of its financial sector.

In the acquisition of data, there are certain basic principles that serve as a guide to investigators. These include the fact that law enforcers are only allowed to gather and store information that is pertinent to the relevant investigation. Only such data as is required for the investigation may be gathered, and the means to achieving the objectives of investigation must be proportionate and reasonable. Whatever falls outside of these bounds potentially violates existing privacy laws. Law enforcers must adhere to these principles.

---

874 See sections 3401-3409 of the RFPA.
875 See sections 2510(12) of the ECPA.
876 For example, in Germany, many of these provisions are contained in the Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG) 2001.
rules. The issue becomes more intense when the personal data is represented in an encrypted format. In this regard, there is great controversy around a key escrow, otherwise called the key recovery system that enables keys required to decrypt an encrypted data to be held in escrow\(^{878}\) in order to prevent undue interference from third parties. It becomes controversial when the authorized third party is the state and its law enforcement agencies, as is often the case.\(^{879}\) The argument is that having the ‘keys’ in the hands of unauthorized third parties represents a violation the right to privacy.\(^{880}\) Where law enforcers are able to make out a *prima facie* case, as a basis for investigation, they would decrypt encrypted information effortlessly. More often than not, consent by the relevant parties is not required.

### 6.2.2.3 Balancing the scale between privacy and public interest values

What then could be the reasonable basis for conducting investigations without circumventing enshrined privacy laws? Does the collective right to the security of society outweigh an individual’s right to privacy? How should the scale be balanced? Outside of general rules and principles that serve as guidelines, these questions are based on merits, depending on the circumstances of the particular case. As a starting point, the relevant domestic legislation of the relevant jurisdiction should be consulted for guidance.

---

\(^{878}\) An escrow is an agreement reached between two contracting parties and a neutral third party, which obligates the third party to deliver an item held in his/her trust to either of the parties when a certain condition is fulfilled.


\(^{880}\) Straub (2002: 530).
These laws set the limit to which law enforcers can act in acquiring personal data that can be a potential infringement of an individual’s right to privacy. These limits have the general attributes of reasonableness and proportionality, strict observance of which is incumbent on law enforcers. Thus, every alleged infringing action of a law enforcer should be met with the question of whether such action is warranted or has a legally justifiable basis. Obviously, where such action is warranted, the privacy argument would not hold. Conversely, where there is no legal justification for the actions of a law enforcer, any public interest legal argument that might be raised would inadvertently succumb to an individual’s right to privacy.

6.2.3 Electronic evidence and the question of admissibility

Due to the nature of the crime of cyber laundering, and the fact that it has a heavy presence on the internet, much of the evidence required as proof in court comes as electronic evidence. This has certain legal implications for cyber laundering, especially as regards its prosecution. The discussion below deals with electronic evidence in general terms.

6.2.3.1 Nature and characteristics of electronic evidence

Electronic evidence, or sometimes called digital evidence, refers to any probative information that is presented electronically, by virtue of its
capability to be stored or transmitted digitally, which can be used at trial.\textsuperscript{881} Electronic evidence may include, but is not limited to electronic communications, such as emails, text messages and chat room communications, digital photographs, website content, postings on social media, computer generated data,\textsuperscript{882} and computer-stored data.\textsuperscript{883} Akin to real evidence, electronic evidence is latent in nature, especially if it is computer-based. It is often stored on or transmitted by a computer. However, unlike real evidence, electronic evidence could be fragile, as it can be altered, destroyed, damaged or defaced.\textsuperscript{884} In order for electronic evidence to be accepted at trial, a court has to determine that three main requirements are met - relevance, authenticity, and originality.\textsuperscript{885} As a fundamental principle of law, the party

\textsuperscript{881} Casey (2004: 12). Cf Marcella and Greenfield (2002: 29), and Nelson, Philips, and Stewart (2010: 102). In some jurisdictions, such as South Africa, the term ‘data message’ is used instead of electronic evidence. This is defined in section 4 of South Africa’s Electronic Communications Transactions Act 25 of 2002 as meaning any “data generated, sent, received or stored by electronic means and includes- (a) voice, where the voice is used in an automated transaction; and (b) a stored record.” This definition is consistent with Article 2 of the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce 1996. In South Africa, within the ambit of the law of evidence, the definition of data message is currently being revised. See South African Law Reform Commission ‘The Review of The Law of Evidence - Draft discussion paper on the review of the law of evidence’ Committee Paper 02/2012 Project 126, 29 September 2012.


\textsuperscript{883} Computer-stored data includes central processing units (CPU) of computers, random access memory (RAM) of computers; read only memory (ROM) of computers; tape libraries, optical juke boxes, optical discs, flash memory or universal serial bus (USB) devices, floppy discs, zip disks, or punched cards, among several others. See Wise Geek (an undated website document) ‘What is data storage?’ available at <http://www.wisegeek.com/what-is-data-storage.htm> [accessed on 22 February 2012].


\textsuperscript{885} Mason and Schafer (2010: 710), and Nelson, Philips, and Stewart (2010: 106).
seeking to introduce electronic evidence bears the onus of proving that all three requirements are met.

The question of relevance is one which requires circumspect consideration. This implies that the relevant electronic evidence should be capable of proving or disproving one of the legal elements of a case. Two factors that determine the relevance of electronic evidence are the materiality of the evidence and its probative value. Within the ambit of the law of evidence, relevance is not an inherent characteristic of the related electronic evidence, but it exists as a link between the object and the matter or, so-called, the legal element of the case.

The authenticity of electronic evidence is also required for its acceptance at trial. The associative question in this regard is whether the evidence is legitimate. The authenticity of electronic evidence can be proved by: (a) an indication to the fact that the evidence has been signed digitally by the person who purports to have signed it; (b) that other appropriate security procedures or devices have been applied to the evidence as may be required; and (c) by any other means or method showing its integrity and reliability.

---

886 These factors are often readily ascertainable from the relevant domestic law. For example, in the US, Rule 401 of the Federal Rule of Evidence (Act of 1975, Title 28, United States Code) states the meaning of relevant evidence to include “evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.” This definition embodies the factors of materiality and probative value.

887 For more details, see the Legal Information Institute (an undated internet report) ‘Rule 401, Test for Relevant Evidence’ available at <http://www.law.cornell.edu/rules/fre/rule_401> [accessed on 16 February 2012]. In the highly-regarded US case: United States of America v. Foster 986 F.2d 541 (D.C. Circuit) (1993), the Court stated that the crucial first step in determining relevancy is to “identify the matter properly provable.”

888 Mason and Sheldon (2010: 776). Cf Casey (2004: 19). The principle relating to the authentication of electronic evidence is one that has received much attention over the years, particularly in the US.
The originality requirement is not always as stringent. This is because, in certain instances the court can accept a copy or duplicate of an original where the original is inaccessible, altered or damaged, and where such duplicate is a fair representation of the original.

6.2.3.2 The admissibility of electronic evidence

The evolution of technology has impacted on the concept of electronic evidence which, in turn, has many ramifications, particularly its admissibility in court. The fragility of and sensitivity around the concept of electronic evidence has the potential of either making or breaking a case against cyberlaundering. Some key issues relating to the inadmissibility of electronic evidence are further brought to light.

Electronic evidence lawfully obtained would be readily admissible in court.\(^{889}\)

In principle, inadmissible evidence is evidence that is not obtained in
accordance with the law. The law in question here refers to the domestic law of the relevant jurisdiction. As with any other kind of evidence for the prosecution’s case, a warrant or a court order is required in order to obtain electronic evidence, otherwise the evidence is inadmissible in court.

Another factor that affects the admissibility of electronic evidence is if the electronic evidence is, by nature, hearsay. Hearsay evidence is a statement that is made by someone other than the declarant, offered in a trial to prove the truth of a matter or the legal elements of the case.\(^\text{890}\) It is a general principle of law that hearsay evidence is not admissible, although exceptions exist in certain cases.\(^\text{891}\) This principle applies equally to electronic evidence.

As mentioned earlier, electronic evidence is generally admissible. If it is of a hearsay nature, automatically, it becomes inadmissible. However, the principal challenge comes when the court has to determine whether electronic evidence is hearsay or not.\(^\text{892}\) It is a fundamental rule that electronic evidence

\(^\text{890}\) Cf Casey (2011C: 57) and Frieden and Murray (2011: 25).

\(^\text{891}\) Such exceptions can be wide-ranging, depending on the jurisdiction concerned. For example, in the US, Rule 801(d)(1)(A)-(C) of the Federal Rules of Evidence Act of 1975 provides that the prior statement of a witness is not hearsay if the person who made the statement is subject to cross-examination at the trial. Amongst several others, some other exceptions include a statement made by a person that conveys his or her sense of the state of an event or condition of something (Rule 803(1) of the Federal Rules of Evidence Act of 1975); a statement made as a result of an excited utterance (Rule 803(2) of the Federal Rules of Evidence Act of 1975); a statement made for medical diagnosis of treatment (Rule 803(4)(a) and (b) of the Federal Rules of Evidence); public records (Rule 803(8) of the Federal Rules of Evidence Act of 1975); family records (Rule 803(13) of the Federal Rules of Evidence Act of 1975) and statements in ancient documents (Rule 803(16) of the Federal Rules of Evidence Act of 1975). In the United Kingdom (UK), there is a distinction between statutory exceptions on the one hand (i.e. statements relating to unavailable witnesses, business documents and previous consistent or inconsistent statements – contained in Sections 116 of the Criminal Justice Act of 2003) and common law exceptions on the other hand (for example, public information, reputation or family tradition and common enterprise – contained in Section 118 of the Criminal Justice Act of 2003).

\(^\text{892}\) The US is an example of how this poses a grave challenge for courts: In the cases of Haag v. United States, 485 F.3d 1, 3 (1st Circuit) (2007); United States of America v. Fujii, 301 F.3d 535, 539 (7th Circuit) (2002); United States of America v. Briscoe, 896 F.2d 1476, 1494 (7th Circuit)
would not amount to hearsay when the evidence results from a machine operation, which merely uses or replicates a human input or programming, and is one that has been generated solely by the technical and mechanical operations of the relevant computer. As such, the electronic evidence must have been independent of all human interferences, manipulations or control. In certain instances where the essential elements of hearsay evidence are not met, electronic evidence becomes admissible. In addition, electronic evidence is one that is hardly decodable by laymen and it often requires an additional action to enhance its interpretation or readability. Consequently, its admissibility raises some questions as well. Also, electronic evidence in its original form might be difficult to bring to court, due to certain practical contingencies. This might cause one to detract from the best evidence rule, which is a fundamental common law rule of evidence. The best evidence rule presupposes that evidence must only be allowed in court if it is the best possible evidence that the case in question allows. Interpreted strictly (1990), the courts held that computer-based electronic evidence is prima facie admissible under section 803(6) of the Federal Rule of Evidence. However, a more grounded rationale soon developed, which is that electronic evidence results from a process and is consequently not averments made by individuals, hence not falling into the category of hearsay evidence. Thus the printed result of a computer-based test (United States of America v. Washington, 498 F.3d 225, 230-31 (4th Circuit) (2007)), a computer based header (United States of America v. Hamilton, 413 F.3d 1138, 1142-43 (10th Circuit) (2005)), and the utterances of a machine (United States of America v. Khorozian, 333 F.3d 498, 506 (3d Circuit) (2003)) do not amount to hearsay evidence. For details see United States Department of Justice (an undated website document) ‘Computer Crime’ available at <http://www.cybercrime.gov/ssmanual/05ssma.html> [accessed on 22 February 2012]. Cf Frieden and Murray (2011: 25).

894 The best evidence rule dates back to the English case of Omychund v Barker (1745) 1 Atk, 21, 49; 26 ER 15, 33, in which Lord Harwicks held that no evidence was admissible unless it was the best that the nature of the case will allow. The reasoning was based on the fact that, in the eighteenth century, an original document was often reproduced or rewritten by hand, and the principle held that if the original was not produced, then there was a high probability that the copy was illegitimate for reasons of fraud or error. See Gilbert (2010: 203).
within the context of electronic evidence, it means that no ‘extra steps’ or alterations of the electronic evidence are permissible. These are questions left for national courts to determine.895

6.2.3.3 Electronic evidence and cyberlaundering

From the discussion so far, certain points come to light as regards the prosecution of cyberlaundering. First, due to its nature, the evidence required to prove a cyberlaundering offence can be quite diverse and broad in its ambit, given that a truly unfathomable web of devices can be created. The nature and form of electronic evidence required would depend on the kind of the cyberlaundering scheme in question, which is the subject of the relevant investigation. For example, with respect to cyberlaundering via online banking,896 certain kinds of evidence other than electronic evidence may be required. This is because a terrestrial bank might be involved, which might have certain physical materials in its possession that might constitute real evidence in court. The same goes for online casinos with a terrestrial presence

895 In the UK, in the case Butera v Director of Public Prosecutions for the State of Victoria, (1987) 164 CLR 180, the court held that the copy of a tape recording is admissible electronic evidence. The court followed the rationale that the content of the tape recording, and not the tape recording itself, is of relevance, and thus it should not matter that a copy is presented as evidence. Also, the court stated that this does not mean that the highly revered best evidence rule is not followed. It further stressed that the law should be developed in line with modernity and should never be left in a state of uncertainty. In the US, Rule 1001(3) of the Federal Rules of Evidence provides that if data is stored in a computer, any print-out or output readable by sight is an original, as long as it is shown to reflect the data accurately. As in the UK, the courts in the US are commonly of the opinion that copies or print-outs of electronic data do not circumvent the best evidence rule. For example, in the case Aguimatang v. California State Lottery (1991) 234 Cal.App.3d 769 [286 Cal.Rptr. 57], the court held that a computer print-out does not violate the best evidence rule as it is considered an original, if it meets the requirements of relevance and authenticity.

896 For an elaborate discussion on cyberlaundering through online banking, see chapter 3, paragraph 3.6.1.
as well.\textsuperscript{897} However, for much of the other cyberlaundering methods such as virtual worlds and online barter trade, particularly as they involve electronic currencies and e-metals, electronic evidence is primarily required. Along with fulfilling the characteristics of electronic evidence and its admissibility test, the electronic evidence in question must have evidentiary weight in order to ensure its reliability in court. Failing this, the case of the prosecutor may fail. This harbours danger due to the fact that cyberlaundering is highly complex and knotty, and the electronic data and devices that are used as tools of operation might be quite fragile. Thus, electronic evidence relating to cyberlaundering should be treated delicately, with a great measure of care and sensitivity. It also does not help that electronic evidence in general is highly susceptible to alterations and damage. Like the typical domino effect, loss of data means absence of admissible evidence in court which, potentially, means a failed prosecution. This is why the detection and preservation of electronic evidence are of paramount importance,\textsuperscript{898} as the following discussion on the investigation of cyberlaundering shows.

\section*{6.3 INVESTIGATING CYBERLAUNDERING}

The issue of investigation rests at the heart of this study, as it represents a significant stronghold of the proposed ACL regime, given that a concrete one is, as yet, non-existent. In this section, an attempt is made to erect this pillar,

\textsuperscript{897} For an elaborate discussion on online casinos as a method of cyberlaundering see chapter 3, paragraph 3.6.3.  
\textsuperscript{898} See paragraphs 6.4.3 and 6.4.4 below.
because the issue of investigation is the necessary scaffold to establish the platform to uphold and sustain the prosecution of cyberlaundering.

Whilst conventional criminal investigative techniques are helpful as a starting point in the investigation of cyberlaundering, these techniques are not entirely sufficient. This is why this study borrows from the existing investigative principles applicable to cybercrime, for the main reason that cyberlaundering operates in the ‘cyber realm.’ However, some of the principles of cybercrime investigation are not entirely different from conventional criminal investigative techniques. As regards cybercrime or digital investigations, no one standard approach is adopted, due to certain technical factors such as the nature of the relevant communications or computing device, the purpose for which the investigation is required, such as criminal, civil, commercial, military, and the facts of the case to be investigated.\textsuperscript{899} For this reason, this section focuses mainly on existing digital criminal investigative principles, as applicable to cyberlaundering.

This section sets out certain fundamental features of digital investigation, which include identifying the role players in the investigative process, the different methods of digital investigation, as well as existing scientific techniques that are applicable to the investigative process. Afterwards, in this section, certain basic elemental factors that are essential to every stage of the cyberlaundering investigation are laid out. These include the detection of cyberlaundering; the seizure and preservation of electronic evidence; the

\textsuperscript{899} Casey and Schatz (2011: 187).
analysis of data, reporting and testimony. In addition, the importance of both local and international cooperation is emphasized as the stronghold that binds the entire investigative process.

### 6.3.1 Applicability of conventional money laundering investigative techniques

Conventional techniques employed for investigating money laundering, as discussed in the previous chapter,⁹⁰⁰ are premised on the notion that actual physical illegal cash lays hidden or concealed somewhere in very clandestine avenues. This applies to cyberlaundering, too. The only difference is the element of absence of physical cash.⁹⁰¹ In the world of cyberlaundering, electronic payment systems (‘e-payment systems’) are the bridges that link the terrestrial world with the cyber world. In the latter, the notion of ‘illicit hard cash’ is replaced with the notion of ‘illicit e-money.’ This is due to the fact that physical cash is replaced with several kinds of intangible financial exchange instruments, such as smart cards and electronic metals (‘e-metals’).⁹⁰² As a result, this makes it difficult for conventional money laundering investigators to ‘follow the money.’ Conventional money laundering techniques would prove futile to cyberlaundering because the latter is made up of an intrinsic technological framework, and the realm

---

⁹⁰⁰ See chapter 4, paragraph 4.2.4.2. Cf Madinger (2012: 301).
⁹⁰¹ Cf discussions on electronic payment systems in chapter 3, paragraph 3.3.
⁹⁰² See discussion in Chapter 3, paragraph 3.3.
within which it operates is the internet. This is why digital investigative techniques represent the bulk of investigative techniques for cyberlaundering.

6.3.2 Fundamentals of digital investigation

The investigation of cyberlaundering demands that trusted investigative methods are used to ensure that relevant digital data are located, collated, analyzed, interpreted, and that evidence that is deduced is reported in a reliable, objective and transparent manner.\textsuperscript{903} Seeing that most of the evidence to prove the existence of cyberlaundering is digital in nature, digital investigative techniques are expedient to the cyberlaundering investigative process. In the discussion below, the essential rudiments of digital investigation are considered broadly. Afterwards, the key actors in the investigative process are identified. The purpose here is to determine generally the relevant role players in a cyberlaundering investigation, as opposed to discussing all the functions that come with each role. Some essential digital investigative methods are also discussed, with a view to fitting the investigative issue of cyberlaundering into the right frame.

6.3.2.1 Role players in the investigative process

The investigative process itself involves certain key role players. These include the cybercrime investigator(s) and law enforcement agencies

\textsuperscript{903} Casey and Schartz (211: 187). Cf Casey (2011B: xxii).
functioning to enforce the law.\textsuperscript{904} Also included is the legal advisor. This is a role often played by the prosecuting attorney, who provides legal advice in the investigative process, by giving guidance and direction as it relates to the law.\textsuperscript{905} Although they are expected to work together, it is important for each of these principal actors to maintain their respective lanes in the investigative process and not to interfere with the work of the other. More importantly, along with the requisite skills that come with their respective functions, each party should have a practical understanding of certain basic legal principles, such as privacy and data interception and seizure, amongst several other legal concerns that come with the digital investigations. This is important in order to avoid jeopardizing the course of the investigation.

6.3.2.2 Concept and methodologies of computer forensics

The present digital investigative methods employed to investigate cybercrimes have roots in basic computer forensics. Computer forensics refer to the process of identifying, preserving, analyzing and presenting evidence of a digital nature in a legally acceptable manner.\textsuperscript{906} The concept can also be understood as the use of scientifically derived and proven methods for the preservation, collection, validation, identification, analysis, interpretation and documentation and presentation of digital evidence for the purpose of

\textsuperscript{904} Reyes, O’Shea, Steele, Hansen, Jean and Ralph (2007: 86).
\textsuperscript{905} Reyes, O’Shea, Steele, Hansen, Jean and Ralph (2007: 86).
facilitating and fostering the reconstruction of events deemed criminal, or helping to anticipate unauthorised actions shown to be disruptive to planned operations.  

Digital investigation, within the broader sphere of criminal investigations, is unique for the fact that it is very methodological as it ascribes steps and sequences in the investigative process, and is, consequently, characterized by delicacy and sensitivity, given the ease with which vital data can be lost or, simply, undetected. Essentially, digital investigation includes the following linear-sequenced steps:

- **Forensic preparation:** This is the essential groundwork that should be done before the start of any investigation, and often involves acquiring materials and resources that would help in the course of the investigation.

- **Forensic survey:** This is the so-called sniffing phase, where one seeks to find a potential source for digital evidence within the designated area (i.e. the relevant crime scene, the internet, a computer, etc).

- **Forensic examination:** This is the stage where the relevant data is extracted or sifted from the acquired evidence.

- **Forensic analysis:** This refers to the very thrust of the investigation, where scientific methodology and critical thinking are applied to the evidence in order to address the principal questions at stake.

---

- **Forensic presentation:** This is where the result of a forensic analysis is presented, which satisfies the purposes of the overall investigation.\(^{908}\)

Practice shows that some of these steps are intertwined and not often separated neatly.\(^{909}\) Aside from the steps above, depending on the given scenario, there are several digital investigative methodologies, or ‘process models’, that are used for particular case scenarios, which embody the essential elements of the aforementioned steps. These include the physical model,\(^{910}\) the staircase model,\(^{911}\) the evidence flow model,\(^{912}\) the subphase model\(^{913}\) and the roles and responsibilities model.\(^{914}\) Practitioners (i.e. digital

---

\(^{908}\) Casey and Schatz (2011: 190). Cf Mason and Sheldon (2010: 706) and Slade (2004: 5). This process is also akin to the investigative techniques for the conventional notion of money laundering. See Chapter 4, paragraph 4.2.4.2. Cf Madinger (2012: 303).

\(^{909}\) Carrier and Spafford (2003: 3) and Slade (2004: 4).

\(^{910}\) The physical model form of digital investigation entails a scenario where the digital investigative process is related, continually associated or linked to the physical crime scene, thus oddly perceives the investigated digital device itself as a crime scene. This model is further sub-grouped into the ‘readiness group, deployment group, physical crime scene investigation, digital crime scene investigation, and presentation.’ Casey and Schatz (2011: 190) and Carrier and Spafford (2003: 1).

\(^{911}\) As the name implies, with the staircase model of digital investigation, the investigative process symbolizes an ascending sequence of stairs, on which cybercrime investigators, forensic experts and the public prosecutor work together to scale each step from bottom to top, in a systematic fashion, in order to have a compelling story at the stage of forensic presentation. Generally, the steps include incidents alerts and accusations, assessment of worth, incident crime scenes protocols, identification or seizure, preservation, recovery, harvesting, reduction, organisation and research; analysis, reporting, persuasion and testimony, with the encompassing feature of case management for each step of the way. Casey and Schatz (2011: 193). Casey and Palmer (2004: 5).

\(^{912}\) The evidence flow model of digital investigation is primarily geared towards describing the flow of information in digital investigation from the moment investigators become aware of the crime, until the investigation concludes. This model is akin to the staircase model, save for a significant deviation, being that it goes beyond the given steps by adding certain features, such as the authorization, notification, proof/defense, and transportation of evidence. Casey and Schatz (2011: 191) and Ó Ciardhúin (2004: 3).

\(^{913}\) The sub-phase model borrows from other models in a multitier fashion, and adds different sub-phases to the respective step or phase of the digital investigation. For example, the main steps used in this model are preparation, incident response, data collection, data analysis, findings presentation and incident closure, and the corresponding sub-phases are mainly to survey, extract, and examine with the aim of reducing the amount of data to analyze; assessing the skill level of suspects; recovering deleted files; find relevant hidden data, determining the chronology of file activity; recovering relevant ASCII data; recovering relevant non-ASCII data; ascertaining non-email activity history; and recovering relevant emails and attachments. Casey and Schatz (2011: 195) and Beebe and Clarke (2005: 149).
investigators and other role players in the investigative process) have used these models on a case-subjective basis, and a single model is not always used in a blanket fashion. The rigidity that comes with each of these approaches certainly has unsettling results, and is thus not without criticism.\textsuperscript{915} A key consequence of the close-knit form of these methods is how they tend to exclude certain basic legal elements that are crucial to a digital crime, and as they fall within the perimeters of cyberlaundering, such concerns cannot be overlooked. Some of the left-overs, or identifiable legal issues at stake here can be seen from the start to the end of investigation, and are thus crucial to every stage of the investigative process, as outlined above. These include the incident alert, the requisite authorization, certain threshold considerations, transportation and preservation of the evidence; verification and case management.\textsuperscript{916} These issues, accompanied by any of the applicable investigative models, establish the legitimacy of the entire investigative process.\textsuperscript{917}

\textsuperscript{914} Otherwise known as the FORZA model, this model is suited for cases that require complex digital investigation. It focuses not only on technical issues that follow digital investigation, but also on certain key legal and managerial issues. It defines eight principal roles (i.e. the case leader, system owner, legal advisor, security/system architect, digital forensic specialists, forensic investigator/system administrator, forensic investigator/forensic analysts and the legal prosecutor) and provides six key questions that each role player must answer in an investigation (i.e. who, what, how, when, where and why). However, in this model, the process within each role is not outlined. Thus, it is imperative to reference other models, explaining why the model operates entirely as a higher level of abstraction. Casey and Schatz (2011: 196) and Ieong (2006: 4).


\textsuperscript{917} For more details see paragraph 6.4.4.3 below.
6.3.2.3 Scientific techniques and digital investigations

Digital investigations should not be characterized by overwhelming sophistication and complexity, but rather by simplicity and flexibility. These are qualities that would enable investigators to adapt easily to any given situation. A scientific approach is not as rigorous as one might think. The approach ensures that investigators have the desired level of meticulousness for cyberlaundering investigations. As opposed to having a blanket cover on the whole investigative process, the scientific approach should be applied to every stage of the cyberlaundering investigation. Thus, coupled with the stages of digital investigation identified above, the following scientific principles should be applied to each given step:

- **Observation:** This refers to the occurrence of one or more events that would trigger the start of investigation, or an incident alert;

- **Hypothesis:** On the basis of the incident that occurs, the investigator forms a theory or prognosis of what he thinks might have occurred, or what might have caused such occurrence;

- **Prediction:** On the basis of the hypothesis, the investigator then predicts and tries to locate the cause of the incident or occurrence, by making a concrete and logical determination;

- **Experimentation/Testing:** What follows is a thorough analysis of the available evidence to find the predicted element, cause, or factor. The hypothesis must be tested for possible alternative explanations. If the

---

original hypothesis is correct, other alternative explanations are excluded automatically (a process otherwise termed falsification); and

- Conclusion: The conclusion is formed after the result. It may support the hypothesis, contradict the hypothesis, or indicate the inadequacy of findings to generate a conclusion.

Because these principles serve as a standard thought process that should be applied to each stage of the investigation, they are also vital to the analysis of how cyberlaundering should be investigated.

6.3.3 Employing digital investigative elements for cyberlaundering: A practical assessment

As a general principle of criminal investigations, the goal of conducting an investigation is to uncover the truth. This applies to cyberlaundering as well. The truth that is sought in this case is proof that the requisite elements of a cyberlaundering offence exist in a given conduct, or from a set of material facts. Hence, the purpose of conducting a cyberlaundering investigation is to show that a computer was used to perform a transaction, or a relationship, involving property or benefit, whether tangible or intangible, which is derived from a criminal activity. Broken down into its constituent elements, the result of the required investigation must prove the existence of a predicate offence, an activity, a computer and illegal funds (i.e. the \textit{actus reus} elements), all of which are bound together by the requisite \textit{mens rea} elements of the crime, such as knowledge of the crime and the corresponding associative
intention. In what follows, a distinct investigative method for cyberlaundering is described by adopting certain key elements of digital investigation such as the steps involved in digital investigations and the scientific sequence of investigation. However, cyberlaundering does not fit entirely into the conventional scheme of digital criminal investigation, given that it differs from other kinds of cybercrime. This is due to one material fact - the ‘victim’ element involved - which, in the case of cyberlaundering, is the state and not individuals, as is the case with most types of cybercrimes. Hence, this tilts the focus of the investigation slightly, causing more attention to be given to the elements of the offence and the perpetrator, and not so much to the victim, whom most cybercrime investigators often try to identify, especially when trying to detect the crime. In order to aid this analysis, a hypothetical scenario of cyberlaundering, using the avenues of virtual worlds is given below.

**Cyberlaundering and investigation: A hypothetical scenario**

Jack Sparrow is a drug dealer living in South Africa. He makes roughly US$2 million annually from his unlawful enterprise. He learns about virtual worlds from a friend, who is a game addict, and informs him of the possibility of using such novel method to wash his funds. Jack Sparrow thereupon joins Second Life (SL) as

---

919 See Chapter 3, paragraphs 3.2.1 and 3.2.3.
920 The state is a victim of a money laundering offence because the interests that are protected by criminalising money laundering are the economy of the state and effectiveness of the judicial process. Cf Unger (2007: 149) and Tanzi (2005: 91). This rationale is the same with cyberlaundering, which shares the same protected interests. Cf discussion in paragraph 6.4.2.1.3 below, and the discussion in Chapter 3, paragraph 3.2.3.3.
921 Cf Chapter 3, paragraph 3.6.6.
a resident. He buys a virtual land on which he later builds a big multi-purpose entertainment company called ‘The Lounge.’ The Lounge offers all sorts of social activities, ranging from night clubs to a diner and a coffee shop. Jack Sparrow arranges things in such a way that visiting The Lounge is by invitation only.

John Doe is an acquaintance of Jack Sparrow, who often served as a middle man in his drug dealing enterprise. Jack Sparrow employs John Doe as a smurf, together with several other individuals living across different continents in the world. For a commission, Jack Sparrow requires the smurfs to become residents on SL in order to clean his funds. Jack Sparrow buys several smart cards which he tops with varying value from his illegal funds, after which he sends them electronically to all the smurfs. Jack Sparrow further invites the smurfs to The Lounge on an exclusive basis. Also, Jack Sparrow charges the smurfs a membership fee, which is equivalent in value to the amount or value on each smart card in their possession. The money is paid to Jack Sparrow in Linden dollar (L$) – the legal tender used as currency in SL. Thereafter, Jack Sparrow converts some of the monies back to real world money through an automatic teller machine (ATM), and further trades with the other smurfs with the remainder, after which, again, he converts the proceeds derived into real-world money.

6.3.3.1 **Threshold considerations**

Before commencing a cyberlaundering investigation, certain factors should be considered. It is expedient for these factors to be applied at every stage of the investigation, as they are recurring themes in the entire investigative exercise. They include the scientific process, case management and the applicability of a statute of limitation.
6.3.3.1.1 Adopting the scientific approach

As shown above, the scientific approach is a thought process which utilizes a deductive analysis technique, in order to arrive at a clear, logical and irrefutable conclusion. By working through every stage - observing the relevant facts, forming a hypothesis, making a prediction based on such hypothesis, experimenting and testing the hypothesis for truth or correctness, and deducing a reasonable conclusion as a result - logic is guaranteed and irrational results can be avoided. More importantly, this approach should be applied at every stage of the investigative process. Given the complexity that characterizes digital investigations, especially in the case of cyberlaundering, having such a thought process would help to unravel seemingly incomprehensible cases and stages of the investigation. This is a recurring theme and a golden thread that runs through the discussion that follows. At every stage of the cyberlaundering investigative process discussed further, this logic is applied to the hypothetical case scenario given above, and a deductive analysis is formed at each stage of the investigative process.

6.3.3.1.2 Case management

Case management is another recurring theme in the entire investigative process, as it plays a very vital role. It is crucial to every stage of the investigation, and due to the sensitive and fragile nature of digital investigation, an effective case management ensures that relevant information or data resulting from each step of the process is captured, secured,
documented and woven together, in order to create a comprehensible and compelling picture of events relating to an offense or incident.\textsuperscript{922} Case management also facilitates information sharing, where all role players provide weekly or daily status updates in order to consolidate and archive updated information and the workings of the entire investigative process. Thus, case management functions as a binding chord for the entire investigative process, without which crucial information may be rendered fluid and, consequently, become undiscovered.

6.3.3.1.3 \textit{Statute of limitation}

The prosecution of cyberlaundering should commence on a lawful basis, and one major hindrance to prosecution is where the crime in question has prescribed. This is particularly interesting for the subject of money laundering which involves two distinct offences – the money laundering offence and the predicate offence upon which the former is based. This rationale thus applies to both offences, and a money laundering offence cannot be prosecuted where the requisite predicate offence has prescribed. For money laundering offences, in the \textit{United Nations Convention against Transnational Organized Crime, 2000}\textsuperscript{923} (‘Palermo Convention’), and the \textit{United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances},

\textsuperscript{923} Adopted by the General Assembly of the United Nations on 15 November 2000 and came into force on 29 September 2003.
1988⁹²⁴ (the ‘Vienna Convention’), it is left to the discretion of local jurisdictions to prescribe “a long statute of limitations period within which to commence proceedings for any offence covered under the Convention[s].”⁹²⁵ Thus, in line with this provision, a determination of a statute of limitation is left to the discretion of local jurisdictions. For example, in the US, a five-year criminal statute of limitations applies to all money laundering offences.⁹²⁶ This rationale applies to cyberlaundering as well. Seeing that the entire discussion is premised on a hypothesis, and because a concrete local and international ACL regime is currently lacking, no such time period is prescribed for cyberlaundering. For all intents and purposes, the cyberlaundering offence considered in the following discussion is not deemed to have prescribed.

6.3.3.2 Detection

What should trigger a cyberlaundering investigation? This is the primary question that should kick-start the investigative process for cyberlaundering. Concomitantly, it also indicates an equally important rationale that is glaringly lacking in the process models of digital investigation because the ‘incident alert’ aspect of digital investigation is lacking in these process models.⁹²⁷ As applicable to cyberlaundering, it is important to ascertain an

⁹²⁵ Articles 11(5) and 3(8) of the Palermo and Vienna Conventions, respectively.
⁹²⁶ Sections 1956 and 1957, Title 18 of the United States Code.
⁹²⁷ Casey and Schatz (2011: 200). Cf paragraph 6.3.2.2 above.
incident alert. This is necessary in order to set in motion the investigative process.

As stated earlier, unlike conventional cybercrimes, where there are identifiable victims that could easily report an incident, a crime or the suspected commission of a crime, there are no such victims in the case of cyberlaundering because the state is the victim of the crime. In this regard, one has to resort to the conventional money laundering system through which law enforcers gain knowledge of laundering operations. Thus, the role of Financial Intelligence Units (FIUs) should not be undermined, nor the role of certain individuals who are duty-bound to report suspicious activities. Depending on the system of the relevant local jurisdiction, the FIU could act as a law enforcement body or it could simply channel the information to the relevant criminal justice authority. The obligation to report the suspicion of cyberlaundering activities depends largely on the method of cyberlaundering operation in focus, and such reporting should be made only on the basis of a

---


929 See the anti-money laundering (AML) principles set out in Chapter 4, paragraph 4.2.3.2.3. Recommendations 22 and 23 of the Forty Recommendations of the Financial Action Task Force provide that, other than financial institutions, the duty to report is also incumbent on lawyers, notaries, other independent legal professionals and accountants who engage in the activities of their clients, such as real estate transactions; management of client money and other assets including securities; management of bank, savings and securities accounts; creation, operation or management of legal persons or arrangements; buying and selling of business entities, and the organisation of contributions for the creation, operation or management of companies. See Financial Action Task Force (2012A: 20), Cf Financial Action Task Force (2003: 8). Also, the obligation is incumbent upon non-financial entities, such as dealers in precious metals or stones, as well as trust and company service providers. See Financial Action Task Force (2012A: 20). Cf Financial Action Task Force (2003: 16).
reasonable suspicion. For example, financial institutions are in the best position to report suspicious activities that involve cyberlaundering through the online banking system. Their ability to report, however, is premised on their capacity to identify or detect cyberlaundering operations, as it is clear that cyberlaundering, via online banking, is quite different from the mere performance of structured transactions in terrestrial banks. This shows why capacity building and skills development are vital to this embryonic stage of the ACL regime.

The importance of detection is also important to the area of electronic payment systems (i.e. e-payment systems), which is the main tool used for cyberlaundering operations. The question is how law enforcement authorities can detect suspicious transactions where such transactions have not been reported. Most electronic transactions have 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.”

It is usually a hassle for authorities to monitor every digital signature closely for suspicious transactions. For this reason, oversights are almost sure to occur. Practice shows that some financial institutions and companies are now cognizant of this fact. Certain pre-paid card companies now use the services of some independent detection agencies to monitor the prepaid card

---

930 For a detailed discussion on what amounts to ‘reasonable suspicion,’ see discussion in Chapter 4, paragraph 4.2.3.2.1. The concept of reasonable suspicion is incumbent on the existence of a predicate offence for cyberlaundering, as one of its constituent elements. See discussion in paragraph 6.4.3.2 below.
931 See discussion in Chapter 3, paragraph 3.6.2.
transactions by their customers. One such company is Red Plc, which offers the PRISM Merchant system \(^{933}\) and which boasts the 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. \(^{934}\)

Although the success of this system cannot yet be ascertained, this clearly shows that the issue of detection is gaining currency. It also shows that national security is becoming privatised by the mere fact that the detection of cyberlaundering is delegated or outsourced to private entities. Nevertheless, this should not detract from the fact that the responsibility to report suspicious transactions lies with law enforcement authorities and the persons mentioned when they have reasonable suspicion.

---

\(^{933}\) For more information see Red Plc (an undated website document) ‘PRISM Merchant System’ available at <http://www.redplc.com/about/> [accessed on 16 February 2012].

In the hypothetical scenario given above, the activities of Jack Sparrow and John Doe could only be detected by way of the internal regulatory mechanism put in place by the gaming website, SL. By tracing and monitoring closely the activities of every resident in the virtual world, the company would be in the best position to report such suspicious activities. However, the likelihood of this is slim, given the always overshadowing *raison d’être* of corporate concerns, because such profit-driven enterprises would first like to safeguard their own interests before public policy considerations.\(^{935}\)

Overall, given that the state, as an institution, is made up of individuals who are its composite members, the interests of the state equate to the interest of the public. Thus, in safeguarding this interest, everybody, as opposed to a designated few, should bear the burden of raising an alarm on cyberlaundering activities. Intuitions or suspicions premised on reasonableness that are derived from ongoing monitoring of high-risk areas should be reported timeously. For example, in the hypothetical scenario above, a fellow SL resident with knowledge, or reasonable suspicion, of the illegal activity could take the initiative and report to the relevant FIU of law enforcement agency.

### 6.3.3.3 Survey

At this stage investigators should be ready to recognize and identify potential sources of digital evidence. This is crucial in order to ascertain what kind of

\(^{935}\) This is but one of several challenges to the effective regulation of cyberlaundering. Cf discussion in Chapter 5, paragraph 5.3.1.
evidence to preserve. To carry out this exercise, investigators should be able to identify the \textit{actus reus} elements of the crime of cyberlaundering. At the survey stage, the \textit{actus reus} elements alone can be judged, because the investigators cannot have all relevant information to ascertain the equally requisite \textit{mens rea},\footnote{Ascertaining the presence of \textit{mens rea} comes at the analysis stage. See paragraph 6.3.3.7 below.} although a presumption of such is important as part of the overall reasonable suspicion required. On the basis of such reasonable suspicion, the need to obtain authorization is justified in order to proceed with the investigation.

6.3.3.3.1 \textit{Establishing the actus reus elements of cyberlaundering}

In light of all relevant facts, and based on the report given, investigators should be able to deduce the \textit{actus reus} elements of the crime of cyberlaundering. From the set of hypothetical facts, these are identifiable as follows:

(i.) \textit{Predicate offence}: The predicate offence in question is drug dealing, which is generally criminalized in terms of local and international law. Where the crime is not committed in the place where the cyberlaundering prosecution is sought, the predicate offence has to be criminalized in the country where prosecution is sought, as well as in the country where the crime was committed. This satisfies the dual criminality requirement.\footnote{See Article 6(2)(c) of the Palermo Convention and Article 7(15)(c) of the Vienna Convention. Cf discussion in Chapter 4, paragraph 4.2.3.1.1.} Also, the predicate offence should not have
prescribed, or be barred by the relevant statute of limitations at the time the cyberlaundering operation had occurred. Important to note as well is the fact that Jack Sparrow and John Doe need not have been convicted of such predicate offence.  

(ii.) **Illegal funds**: The next element of cyberlaundering that emerges clearly from the set of facts is the presence of illegal funds – US$2 million in this case, which is derived from the predicate offence. This element is often easily identifiable, because all that has to be proven is the link between the funds and the predicate offence.

(iii.) **An activity**: The activity element could be rather broad in nature. It primarily means what the accused did with the illegal funds or how he tried to conceal the origin of such funds. This element depicts how cyberlaundering deviates from the conventional concept of money laundering because, with the latter, the relevant activity happens in the terrestrial world. For example, the money launderer would purchase a house, a car or a painting. As is seen from the given scenario, the illicit funds are diverted into the ‘cyber world’. In this case, Jack Sparrow layers the illegal proceeds by funnelling them into SL, using his army

---

938 The Palermo and Vienna Conventions do not have express provisions in this regard. It is, however, stated in Articles 3(4) and 3(5) of the Council of Europe Directive 2005/50/EC on the prevention and use of financial systems for the purpose of money laundering and terrorist financing, adopted by the European Parliament and the Council of Europe of the European Union on 26 October 2005, which came into force on 25 November 2005. Cf Basel Institute on Governance: Assets recovery Knowledge Centre (2007) ‘Anti-Money Laundering’ available at <http://www.assetrecovery.org/kc/node/82bce589-7805-11dd-9c9d-d9fcb408dfe3> [accessed on 5 February 2012]. These different elements are crucial to this study, and they would be analyzed in detail in relation to cyberlaundering in the following chapter (Chapter 5).

939 Cf detailed discussion on the concept of ‘an activity’ in Chapter 3 above at paragraph 3.2.4.2.
of smurfs, John Doe included. Given the compounded and extremely complex nature of the activity element, an understanding of which often eludes many, cyber launderers are able to waltz freely, without being detected. The activity is often so well simulated that, ordinarily, every semblance of illegality evades the eye. This is no doubt a challenge posed to investigators. Also, to comprehend properly the relevant activity - or ‘activities’, in which cyber launderers engage, investigators need to be properly acquainted with the nature of such activity. For example, an investigator who is ignorant about the concept of virtual worlds would be simply unable to detect the cyber laundering operations in which Jack Sparrow and John Doe have engaged. Therefore, the activity element is one that requires investigators to be versed in the cyber laundering schemes that exist with not just virtual worlds, but also several other new technologies that are vulnerable to cyber laundering operations.  

(iv.) A computer: This is the key technological element of the crime, and it is intertwined with the activity element. Both should be understood together, because the idea of a computer adds flesh to the notion of activity involved. The computer, which also encompasses the concept of the internet, is the means through which the activity is conducted. In this case, the focus is on SL, which is an internet gaming company

---

940 For a detailed discussion on the key vulnerable avenues for cyber laundering, see Chapter 3 above at paragraph 3.6.
941 See detailed discussion in Chapter 3 above at paragraph 3.2.4.2.
that serves as the platform upon which cyberlaundering operations are conducted.

6.3.3.3.2 Authorization

The need for investigators and law enforcement bodies to acquire a warrant or authorization forms an essential part of the survey phase of investigation. This is crucial in order to proceed with the investigation, because authorization is required for the search and seizure of digital evidence. Prudence dictates that it is best to err on the side of caution by acquiring the requisite authorization at an early stage of the investigation in order to forestall any loophole that will undermine the investigation. Acting on reasonable suspicion, the investigator or law enforcement officer can seek the requisite authorization, which is usually a court order issued by a judge or magistrate within the relevant jurisdiction.\textsuperscript{942} Depending on the facts of the specific case, legal advice should be sought at this stage of the investigation to ensure that the necessary nuances of the law are considered, especially as regards the authorization process. Therefore, in the given hypothetical scenario, it would be prudent for the relevant law enforcement authority to obtain a search warrant soon after reasonably suspecting the commission of the crime, and after having also made sure that the constituent elements of the crime are met.

\textsuperscript{942} For a discussion on how the relevant jurisdiction can be determined, see paragraph 6.5 below.
6.3.3.4 Seizure and confiscation of potential evidence

Once investigators or law enforcement officers have the requisite authorization, the next step is to proceed to with the seizure and confiscation of the potential evidence. Depending on the circumstances of each case, the potential evidence in question would most likely be instruments, tools or assets related to the activity in which the cyberlaunderers have engaged.\footnote{Cf Walden (2010: 607).}

The legal basis that underlies the duty of law enforcement bodies to act exists in the relevant legal instruments. At the international level, examples of such legal instruments are the Vienna and Palermo Conventions;\footnote{See Article 12(1)(a) and (b) of the Palermo Convention. Cf Article 5(1)(a) of the Vienna Convention. Cf. see discussion in Chapter 4, paragraph 4.2.4.4.} as well as the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism,\footnote{Article 3 of the Convention which was adopted by the Council of Europe on 16 May 2005, and which came into force on 1 December 2009.} (the Warsaw Convention) which most countries have ratified.

From the given scenario, several things could be seized as potential evidence, such as the smart cards which have been loaded with the illicit funds, and the electronic financial records, if any, that indicate how Jack Sparrow has structured payments into these cards. With smart cards, however, the issue is tricky. One must remember that the funds on certain smart cards can be accessed by more than one party. Consequently, the fact that a smart card has been seized does not mean that the funds on it have also been seized. This is due to the fact that an accomplice or a person in cahoots with the accused...
could very well have the funds on the card transferred or removed from the smart card.\textsuperscript{946} Thus, additional steps must be taken to ensure that the funds on the card are frozen as well. Given that most smart card companies, after retail, are often ‘detached’ from the smart card as well as the activities and transactions conducted with the smart card, unlike several terrestrial banks and their respective customers’ accounts, the possibility of freezing creates difficulty. First, there must be a legal basis for freezing at the national level because the provisions in existing AML laws such as the Vienna, Palermo and Warsaw Conventions do not provide for this scenario.\textsuperscript{947}

Also, perhaps the most important potential evidence is Jack Sparrow’s account or profile on the internet platform itself (SL) which, like other potential evidence, such as hard drives, emails stored on the web server and mobile devices, to name a few, can be seized. Jack Sparrow’s profile on SL will have sufficient details or history of his activities, which can form a thread to allow law enforcement piece together the underlying scheme. This can, however, be done only with the cooperation of SL as the principal internet service provider. Although the issue of privacy is one that might serve as reasonable defence against the ability of law enforcement to search and seize

\textsuperscript{946} Cf see discussion in Chapter 4, paragraph 4.3.3.6.3.
\textsuperscript{947} Article 12(1)(a) and (b) of the Palermo Convention. Cf Article 5(1)(a) of the Vienna Convention which does not entail this scenario. Nor is there an applicable provision in the Council of Europe Convention on Cybercrime (otherwise known as the Budapest Convention) which was adopted by the Committee of Ministers of the Council of Europe on 08 November 2001 and came into force on 1 July 2004. However, as discussed in Chapter 4, paragraph 4.3.3.6.3, a similar law that should apply is the SB-82 (NV Senate Bill 82-75\textsuperscript{th}, BDR 14-266, which came into effect on 1 July 2009) of the American state of Nevada, which permits law enforcement agencies to investigate suspicious activities involving smart cards and freeze funds for up to 10 days after such seizure.
any possible evidence, the authority of a search warrant should, ideally, trump any of such concerns, whether raised by SL or Jack Sparrow.

6.3.3.5 Preservation

The notion of preservation of digital evidence is equally important, and it is also a vital stage in the digital investigative process. Necessary steps must be taken to ensure that potential evidence is captured in its current state, and more importantly, that the integrity of the potential evidence is preserved. The aim of this stage of the investigation is to ensure that the evidence obtained is accurate, reliable, professionally acceptable, and irrefutable.948 For this purpose, the role of the forensic expert is indispensible. In practice, the preservation process involves the care in transportation of the potential evidence from the crime scene to the forensic laboratory, or between laboratories,949 and the use of duplicate copies of all sources of data.950 This allows investigators to have two categories of exhibits: the first, being the original one, is catalogued and stored in an environmentally controlled location, and in an unmodified state. The second one is the duplicate of the original material, which is created and scrutinized as the investigation progresses.951 For our purposes, such precautionary steps should be applied to the smart cards, the web server of SL which has Jack Sparrow’s account and profile, and possible communication devices, such as his email account and

948 Casey and Schatz (2011: 210).
mobile devices. Potential evidence obtained from any of these, or from any other identifiable source, is essential in order to put together the pieces of the puzzle.

### 6.3.3.6 Examination

The examination stage of digital investigation involves extracting and viewing information from the evidence, and making it available for analysis. This stage of the investigation requires a great deal of meticulousness. It involves resource-intensive and very protracted steps in order to avail useful results in a timely manner. In line with a rationale that underscores the physical process model of digital investigation, at this stage of the investigation, it is important to treat each source of digital investigation as an individual crime scene, and to apply the scientific method. This is a more inclusive and practical approach to forensic examination. It means that each step of the digital investigation (i.e. preparation, survey, examination, analysis and reporting) should be applied to every source of evidence. However, for the examination stage itself, three broad levels of forensic examination are often followed in the examination process, in order to foster collective examination, and to prevent an isolated individual examination of individual data:

---

952 Casey and Schatz (2011: 212).
953 See discussion on the process models in paragraph 6.3.2.2 above. Cf Carrier and Spafford (2003: 3), Casey and Schatz (2011: 212) and Slade (2004: 4).
a) The first includes the survey/triage level of forensic inspection. This consists of a targeted review of all data available to identify which ones contain the most useful evidence and which might require additional processing;

b) The second is the level of preliminary forensic examination and in-depth forensic inspection. This implies the examination of data identified at the survey/triage stage, which might contain the most useful evidence which will help investigators to conduct interviews and developing leads; and

c) The third level is the in-depth forensic examination, which is a more comprehensive examination stage which follows from the preliminary forensic examination stage. This level allows for a more complete understanding of the offence.\textsuperscript{954}

Applying these steps to the given scenario, forensic experts will be able to sift very crucial data from the available data (i.e. smart cards, Jack Sparrow’s account and profile on SL’s web server, etc) that has been seized and preserved. This will help the prosecutor’s case. Several tactics and subprocesses can also be employed during this examination phase, such as recovery,\textsuperscript{955} harvesting,\textsuperscript{956} organisation and search,\textsuperscript{957} and reduction, which

\footnotesize{\textsuperscript{954} Casey, Ferraro and Nguyen (2009: 1354). Cf Casey and Schatz (2011: 212). \textsuperscript{955} Data recovery means where deleted, hidden, lost or damaged data is extracted from available sources, regardless of its relevance to the case at hand. Casey and Schatz (2011: 214). \textsuperscript{956} Data harvesting refers to how the investigator can harvest data for later analysis. However, an important feature of this process is that, unlike the data recovery process, only relevant data is harvested. Thus it requires a more logical application of thought. Casey and Schatz (2011: 215). \textsuperscript{957} Organisation and search involves the grouping of derived data in units in order to accelerate later analysis. As such, relevant data may be grouped, tagged, or clearly separated in order to allow law
often involves reducing the relevant dataset for the analysis stage of the investigation,\textsuperscript{958} as the occasion might warrant.

\textbf{6.3.3.7 Analysis}

Of all other stages, the analysis stage of digital investigation is the most definitive and one which demands intense critical thinking. The scientific method of thought is of particular relevance to this stage. The analysis requires a clear and proper dissection of certain internal attributes of the data. Technically, it requires a probe into certain key component parts of the data such as the specific binary audio and video format of the data items, or the text and narrative, which is the meaning of the data. The salient characteristics derived from these items are then pieced together and set out clearly in order to establish necessary links as well as the origin of the item, which would give a clear determination of the location of the perpetrator.\textsuperscript{959}

This stage is one which tries to make sense of the entire scenario by assembling the necessary data in order to form a clear picture and have a proper understanding of the story. In essence, the analysis stage revolves around certain basic questions such as who, what, where, when, how and why.\textsuperscript{960}
In light of the given hypothetical scenario, the respective questions pertain to the relevant data that has been seized, preserved and examined, such as the smart cards, Jack Sparrow’s account and profile on SL’s web server, and hence the questions: What is the incident? If it is cyberlaundering, who is involved in the alleged cyberlaundering operation? Where did the incident occur? When did the incident occur? How was the operation carried out? And why was the operation carried out? At the survey stage, the first five questions are answered, as such questions involve the *actus reus* elements of the crime, which has been established.\(^{961}\)

At this stage of the investigation the *mens rea* element should be reasonably deduced from the set of facts, as it forms a clear, logical and complete picture. The *mens rea* element of cyberlaundering encapsulates two inseparable requirements: knowledge of the illegality of the funds and an associative intention with the illegal funds, which are applied further to the given hypothetical scenario.

6.3.3.7.1 *Knowledge of the illegality of the funds*

Actual knowledge, and not negligence, of the illegality of the funds is required to establish criminality for cyberlaundering.\(^{962}\) This exercise is also crucial in the investigative process because whatever reasonable deductions are made from available data must constitute proof beyond a reasonable...

---

\(^{961}\) The statute of limitation discussion in paragraph 6.4.3.1 answers the statute of limitations question sufficiently.

\(^{962}\) Cf Chapter 3, paragraph 3.2.4.2.2.
doubt, in order to allow the prosecutor to found a good case in court. Thus, knowledge of the illegal funds is a fundamental element of the crime, being a *conditio sine qua non* for the crime. From the given hypothetical scenario, in order to aid the assessment, certain extraneous factors or indicators could also help to establish the requisite knowledge. For example, where one of the smurfs employed by Jack Sparrow is apprehended, such a person could testify for the prosecution in order to help sustain the knowledge argument. An investigation could be conducted into the finances of Jack Sparrow, which could sufficiently show that he never made a tax declaration on the funds in question, or that he failed to make an accurate declaration, and that there are other possible discrepancies in his finances.

6.3.3.7.2 Associative intention with the illegal funds:
The crux of money laundering inheres in the actual laundering operation, which is a basic rationale also shared with cyberlaundering. The layering phase of cyberlaundering, in which the criminal seeks to disguise the origin of the funds by devising several diabolically clever schemes,\(^{964}\) is a process that lies at the heart of a typical cyberlaundering operation. The intention that serves as the reason behind such operation is the ‘associative intention’ that investigators have to prove. The associative intention runs parallel with the activity element of the requisite *actus reus* discussed earlier,\(^{965}\) as it serves as

\(^{963}\) Cf Madinger (2012: 107).
\(^{964}\) For an elaborate discussion, see Chapter 3, paragraph 3.4.2.
\(^{965}\) See paragraph 6.3.4.3(a)(iii) above.
the ‘reason behind the act’, pointing to why an accused would engage in such an activity in the first place. Hence, the associative intention may also refer to the purpose for which the funds are held, such as to hide the funds from law enforcement bodies, to conceal or disguise their nature, location, source, origin of the illegal funds, as well as to avoid the legal obligation to report the transaction.\textsuperscript{966}

Unlike the other form of \textit{men rea} discussed above, extraneous factors need not be considered to prove the existence of an accused person’s associative intention with the illegal funds. Rather, the associative intention can be proved by simply sorting through available data. This requires more inward looking, and at the analysis stage of the investigation, this is one thread that investigators would have to find. Finding this thread requires investigators to make the necessary links and connections from the acquired, preserved and examined data in order to establish the associative intention element. From the given hypothetical scenario, the smart cards given by Jack Sparrow to his smurfs, if seized, may be used. The fact that there are multiple smart cards containing equal financial value may indicate a structured transaction. In addition, the clandestine nature of ‘The Lounge’, Jack Sparrow’s business enterprise on SL, and the fact that his smurfs are the only exclusive members, is indicative of the fact that an intention exists to evade law enforcement and to disguise the origin of the funds. In sum, investigators can reach the logical conclusion that Jack Sparrow has used SL for the laundering of his illegal funds.

\textsuperscript{966} For more elaboration, see Chapter 3, paragraph 3.2.4.2.2 (b).
funds because the website platform is barely regulated, and Jack Sparrow has exploited that avenue because it is the most unlikely area that law enforcement agencies would consider when trying to track or trace the illegal funds in question.

6.3.3.8 Reporting and testimony

The conclusive phase of every investigative process is reporting and testimony. A report is compiled which includes reference to the protocols followed, methods used to seize, document, gather, preserve, recover, reconstruct, organize and search key evidence. The report should embody an analysis leading to all conclusions and thorough descriptions of the supporting evidence and analysis. For the sake of objectivity, the report could also contain alternative theories that might lead to other plausible conclusions, but which cannot be followed because they contradict each other, and this might help further to prove the validity of the main conclusion set out.

Legally speaking, for the prosecutor’s case to prevail against Jack Sparrow and his army of smurfs, the content of the report must be weighed on legal scales to ascertain whether the conclusion would be compelling in court, and given the fundamental principle that an accused person in a criminal case is presumed innocent until proven guilty, whether the report compiled will constitute proof beyond a reasonable doubt. In further support of the

prosecutor’s case, forensic experts can testify as expert witnesses at court on some technical elements of cyberlaundering, or on any other material element of the case.

6.3.4 Mutual legal assistance for cyberlaundering investigations

The extensive AML law principles of mutual legal assistance, as discussed in the previous chapter, all apply \textit{in tandem} to cyberlaundering.\footnote{See an elaborate discussion of the principles of mutual legal assistance in Chapter 4, paragraph 4.2.4.1.} This is especially the case with regard to the investigation of cyberlaundering. Given the transnational reach of cyber-related crimes such as cyberlaundering, international cooperation helps to prosecute the case successfully. Without such cooperation, cyberlaundering operations will take place with impunity. One point, however, that needs restating is the need for harmonization of laws across jurisdictions. This would help to cover potential loopholes that may arise, given the fact that states have diverging laws for the regulation of cyberlaundering.\footnote{Cf Angers (2004:50) and Pocar (2004: 36) and discussion in paragraph 6.6 below.} Where laws are not harmonized, criminals are able to recognize and exploit potential differences that may exist.

Also, with mutual legal assistance assured, it goes without saying that the possibility of assets recovery\footnote{Cf elaborate discussion on assets recovery in Chapter 4, paragraph 4.2.3.1.4.} is further cemented, and the principles discussed earlier kick in automatically.\footnote{The author is of the view that the principles of assets recovery of the current AML legal regime, as discussed earlier, apply in the same way \textit{mutatis mutandis} to cyberlaundering. As such, the discussion on assets recovery is not repeated in this chapter. See Chapter 4, paragraph 4.2.3.1.4.}
Given that the trans-border nature of cyberlaundering demands cooperation and not friction, one issue that could affect international cooperation is, however, the unavoidable issue of jurisdiction, which is discussed below.

6.4 ESTABLISHING JURISDICTION FOR CYBERLAUNDERING

A key legal issue within the wide spectrum of the ACL legal regime is that of jurisdiction. By definition, jurisdiction implies the right, authority, and power to apply the law. Traditionally, the concept of jurisdiction encompasses three major distinct concepts: jurisdiction to prescribe, jurisdiction to adjudicate and jurisdiction to enforce, which are horizontal forms compared to the vertical forms of jurisdiction.

Jurisdiction to prescribe refers to the right of any sovereign state to make its law applicable to things, persons, their activities, relations or their status, and their interests in things. A state can exercise such right by enacting legislation, or by passing an executive act or order, or by promulgating an administrative rule, or by a determination made by its court.


974 Certain factors determine jurisdiction locally. This is dependent on the structure of the relevant jurisdiction (i.e. federal government system, unilateral system, provincial, etc). Vertically, jurisdiction in the local sphere is categorized into subject-matter jurisdiction, which allows a local court to establish jurisdiction for the crime because of its related subject matter; *in personam* jurisdiction whereby jurisdiction is established with respect to the capacity of the person (often either as a perpetrator or victim); and *in rem* jurisdiction, which pertains to a thing or property. Cf Cater and Weiner (2011: 728); Henkin, Damrosch, Murphy, and Smit (2009: 1048); Oxman (1987: 277) and Brenner and Koops (2004: 29).

Jurisdiction to adjudicate refers to the right and authority that a sovereign entity has to subject individuals to the process of its adjudicative bodies such as courts and administrative tribunals in order to determine whether a sovereign (national) law has been violated. This form of jurisdiction also means the power of a court or a legal body to hear a case, or to administer justice within a particular area of responsibility.

Jurisdiction to enforce refers to the right and authority of a sovereign body to compel compliance with its laws, or to punish non-compliance thereof, whether through judicial means such as the courts, administrative or executive means. The law is enforced via certain law enforcement agencies such as the police, or by using non-judicial actions.

This section focuses on the jurisdiction to prescribe. The ensuing discussion revolves around this form because it is the principal first step, without which the other two forms of jurisdiction are left undetermined. The legal rationale that underlies the concept of jurisdiction is the principle of *forum non conveniens*, which is a doctrine of conflict of laws, according to which a court may refuse jurisdiction over a matter because a more appropriate forum exists for the matter.

How can jurisdiction be founded for cyberlaundering? Where evidence exists that incriminates a person as an alleged cyberlaunderer, it becomes crucial to

---

ascertain where the accused person should be prosecuted. Given the broad
scope of jurisdiction, it is worth noting its different categorizations.
Jurisdiction could be of a national or an international nature. When the crime
of cyberlaundering has a national scope, that is, when all the relevant
elements of the offence can be found within a particular sovereign territory,
the jurisdictional principles of the relevant local jurisdiction would apply
automatically. Jurisdiction only becomes problematic when it involves more
than one country. Again, it is worth reiterating that cyberlaundering, as a
legal concept, is not yet properly conceptualized in both national and
international laws. Invariably, this affects subsequent deliberations on a
court’s jurisdiction to adjudicate the offence, and any authority’s jurisdiction
to enforce court orders. By reason of the fact that the trans-border nature of
the internet has shrunk the size of the world significantly into a single vast
space, seamlessly blurring all jurisdictional borders between countries, as
well as the transnational nature of the money laundering and cybercrime
offences, which informs this study, the study focuses more on the issue of
jurisdiction on the international plane.

As a necessary conduit in the prosecution process, in this section, the very
pertinent issue of jurisdiction is investigated. The purpose is to find a solution
to cyberlaundering. The issue of jurisdiction in cyberlaundering cases is
discussed upon the legal basis that holds the concept of cyberlaundering,
which is its deep roots in two distinct, but broad categories of crime – money
laundering and cybercrime. The principles of jurisdiction in relation to these
two categories are juxtaposed in order to find the right legal basis upon which jurisdiction can be established for cyberlaundering. To this end, an analogy is given below that forms part of an analysis of how jurisdiction can be found for cyberlaundering. The scientific approach of deductive analysis used for the discussion of cyberlaundering investigations is also adopted for this purpose. Afterwards, deducing from these discussions, certain set guidelines for founding jurisdiction for cyberlaundering are suggested.

**Cyberlaundering and jurisdiction: A hypothetical scenario**

Jack Sparrow, together with his friend, John Doe, are German citizens. They sell household furniture for a living in Berlin, Germany, where they are resident. Their shop is called ‘Comfort Zone.’ They recently found a way to sell their furniture to customers outside Berlin, using the internet. As a result, they created the website called ‘www.comfortzonerfurnitures.com,’ where customers can view their stock and make orders. Jack Sparrow and John Doe accept credit cards, smart cards such as PayPal, and online barter trade instruments such as e-gold currencies and bitcoins, as means of payment, after which they deliver the furniture. With time, their business via the internet started to boom, and profits made up 90% of their monthly total gross. They both decided to close their terrestrial shop in order to focus on selling furniture solely online. Jack Sparrow and John Doe at some point started to have criminal instincts, which led them to swindle and defraud many customers, by either rendering defective performance or by not making deliveries at all. In order to evade being traced, they established another website registered in Antigua and closed the one registered in Germany. However, they successfully linked the new website with the old one, retaining the same web address in order not to lose their customers.
Now, fully in the business of swindling customers by virtue of their illicit business, Jack Sparrow and John Doe began making much more profit, with which they used to establish several other fraudulent websites, such as a fake online banking, lottery, file-sharing and online casino websites, which they both co-managed. One Jim Watson in Australia bought furniture on www.comfortzonefurniture.com. He paid by credit card, but never received any furniture. He reported the case to the local police in Melbourne. The police forwarded the case to the prosecuting authorities in Melbourne. After a thorough investigation, the illegality of Jack Sparrow and John Doe’s business came to light, and besides charging them as co-perpetrators with the crime of cyberfraud, the prosecutor also wants to charge them with cyberlaundering on the basis that their conduct meets the elements of the crime. In the meantime, the prosecutor has requested the assistance of the German criminal justice authorities (Strafjustizbehörden) to freeze Jack Sparrow and John Doe’s mansions, luxury cars and bank accounts in Germany.

6.4.1 Applicability of money laundering principles of jurisdiction

As discussed earlier, amongst the other principles of jurisdiction, such as the nationality principle, the objective territoriality principle, the universality principle, and the passive personality principle, the

---

980 See chapter 4, paragraph 4.2.4.2.
981 The nationality principle presupposes that countries would have jurisdiction over their nationals who have committed crimes outside their territories. This principle is supported by Article 4(b)(i) of the Vienna Convention, and Article 15(2)(b) of the Palermo Convention.
982 The objective territoriality principle implies that a country would have jurisdiction because the action had an actual or intended effect on the country’s territory without the necessary occurrence of the action in that territory. An indirect reading of this principle can be gleaned from Article 4(a)(i) of the Vienna Convention, and Articles 15(1)(a), (b)(i) and (ii) of the Palermo Convention.
983 The universality principle of jurisdiction means that any state would be able to claim jurisdiction on the basis that the alleged offence is of such a serious nature that it threatens the international peace, human rights and integrity that they affect all states and all people. This principle is grounded in customary international law. See discussion at paragraph 6.4.3.3 below.

The Legal Regime for Anti-Cyberlaundering / Daniel Leslie
subjective territoriality principle of jurisdiction is most preferred for the crime of money laundering. The subjective territoriality principle holds that a country can exercise jurisdiction over a money laundering offence where the related property or asset, the accused person, or the laundering operations are within its territory. This holds true regardless of where the predicate offence might have occurred. This rationale is further buttressed by the fact that money laundering is not a result offence but a conduct offence, for it is the conduct that incurs criminal liability. Therefore, the offence of money laundering is deemed to have taken place as soon as a constituent element of the crime is present within the relevant jurisdiction.

Cyberlaundering, on the other hand, typically involves the laundering of illegal proceeds through a computer. However, the rationale that underscores the subjective territoriality principle cannot be adopted directly for cyberlaundering. This is due to one significant fact, namely that the subjective territoriality principle is not concerned with the effects of the

984 The passive personality principle of jurisdiction holds that jurisdiction can be established on the basis of the fact that the national of a state’s party is a victim of the alleged offence. This principle is supported by Article 15(2)(a) of the Palermo Convention.


987 Article 6(2) of the Vienna Convention, and Article 6(2) of the Palermo Convention. An important caveat to this principle is the concept of dual criminality which might serve as a bar to founding jurisdiction. Essentially, where a predicate offence is an offence in one country, but not in another, the former country cannot punish the offence or offences based on said offence (i.e. money laundering) as it is tantamount to governing into another sovereign states’ territory and jurisdiction, which defies the principle of international law.

988 Essentially, the crime of money laundering has the potential to create multi-jurisdictional claims, as it is not focused on whether the crime has an effect or result in that territory, but on whether an essential part of the conduct took place there.
crime, which is a feature of the objective territoriality principle. One should bear in mind that cyberlaundering, by its nature, could be truly ubiquitous, making it extremely difficult to have it couched under a single concept of jurisdiction.

Thus, in line with the hypothetical scenario sketched above, the prosecution authorities in Melbourne would be unable to found jurisdiction under the subjective territoriality principle for the following reasons: (i) The accused person is not within its jurisdiction; (ii) The website is not registered within its jurisdiction; and (iii) The frozen assets are not within its jurisdiction. If any of the above factors were present, and if a mutual treaty between both countries existed, a legal argument could be made out for the extradition of Jack Sparrow and John Doe to Melbourne. However, the issue of extradition opens up a whole new scenario entirely.

989 The issue of extradition is unsettling in the international arena, for political reasons. In principle, jurisdiction itself serves as a strong barrier to extradition. Many times, other barriers, such as a lack of dual criminality of the offence, the political nature of the alleged crime, the death penalty, or the threat of torture tend to subdue a request for extradition. For example, due to differences in the French and US human rights laws, it took years, and with strong pressure from the international community, before the President of France, Jacque Chirac, gave in, in 2002, to the extradition request of the US to have Ira Eihon (famously dubbed ‘the Unicorn killer’) extradited. He was an American who killed his wife and locked her up in the closet for 20 years. More recently, in July 2010, the extradition request made by the US to Switzerland, for famed international filmmaker, Roman Polanski, who is charged in the US with sexual assault allegedly committed in the US in 1978, was refused, on what the US considers immaterial grounds. New York Times (2010) ‘Swiss Reject US Request to Extradite Polanski’ available at <http://www.nytimes.com/2010/07/13/movies/13polanski.html?src=mv> [accessed 24 February 2012].

Also, in certain cases where the barriers to extradition are lowered, as evident in the European Arrest Warrant (EAW), to which the principle of dual criminality does not apply, the issue of extradition is still not without political concerns. The EAW issued by the Swedish authorities against Julian Assange on grounds of having committed sexual assault is a good example. The matter is embroidered with political concerns, which slows down the entire process of extradition. For more details see the case of Julian Paul Assange v. Swedish Prosecution Authority [2012] UKSC 22. Also see Rundle, G (2010) ‘Did he or didn’t he?’ available at <http://www.theage.com.au/national/did-he-or-didnt-he-the-murky-politics-of-sex-and-consent-20101211-18tie.html> [accessed on 15 July 2012].
6.4.2 Applicability of cybercrime principles of jurisdiction

The relevant principles of jurisdiction in relation to cybercrime are contained in Article 22 of the Council of Europe Convention on Cybercrime\(^{990}\) (the Budapest Convention). Specifically, Article 22(1)(a) of the Convention states that jurisdiction shall be established for the cybercrime offences listed in the Convention when committed in the territory of the states parties to the Convention. Also, Article 22(1)(d) of the Convention provides that jurisdiction shall be established for the cybercrime offences listed in the Convention if committed by one of the nationals of a state party, if the offence is punishable under the jurisdiction within which the crime was completed, or if it is committed outside any state’s territorial jurisdiction. These articles embed both the territoriality and nationality principles of jurisdiction respectively. Both principles are peculiar to cybercrime, given the ramifications that come with the concept. The implication for cyberlaundering is least favourable. The territoriality and nationality principles are considered in greater detail, along with the universality principle of jurisdiction, which is another possible claim to found jurisdiction, and which is also relevant to this study. These principles are discussed in line

---

\(^{990}\) The Convention was drawn up by the Council of Europe in Strasburg, with participation of the Council of Europe, observer states Japan, Canada and China. The Convention was adopted by the Committee of the Ministers of the Council of Europe at its 109th session on 08 November 2001. On 23 November 2003, it was open for signature in Budapest, and on 1 July 2004, it came into force. As at 9 March 2012, the Convention had been ratified by 32 states parties. In tandem with the Convention is the Council of Europe Convention on Cybercrime: Additional Protocol to the Convention adopted by the Council of Europe on 7 November 2002 and came into force on 1 March 2006. For more information see the Treaties Office of the Council of Europe at [http://conventions.coe.int/](http://conventions.coe.int/) [accessed on 9 February 2012]. Cf discussion in Chapter 4, paragraph 4.3.2.3.
with some practical examples of how several countries have interpreted them, and, for our purposes, how they can be transposed for the purposes of establishing jurisdiction in cyberlaundering matters.

6.4.2.1 The territoriality principle

Perhaps the most interesting observation of the enshrined principle of territoriality, as outlined in Article 22(1)(a) of the Budapest Convention, is that it provides for the territoriality principle, without distinguishing between the subjective and objective principles of jurisdiction. When applied directly to cyberlaundering, this potentially causes different interpretations because of the elements of the offence of money laundering embodied in it. When exactly would cyberlaundering be committed ‘in the territory’ of a country? one might ask. The territoriality principle of jurisdiction with respect to cybercrimes is often an issue left to local courts to decide. For example, in the US, the minimum contact principle is followed, with which to ascertain territorial jurisdiction for cybercrimes, as enunciated in the landmark case of International Shoe Co. v. Washington 326 US 310 (1945). In this case, the Court had to determine the level of connection that must exist between a corporation that is non-resident within a state, and the relevant state, in order for that corporation to be sued within the relevant state. The Court ruled that one can only be subject to judgment in personam if such a person is not present within the relevant territory of the forum, but if it can be rightfully ascertained that he or she has had, at least, certain minimum contacts with the
The Legal Regime for Anti-Cyberlaundering / Daniel Leslie

However, this rationale proves to be substantially vague when fitted into the cyberlaundering frame, as it is difficult to ascertain what constitutes a minimum contact, especially in light of the hypothetical scenario given earlier. Should the required ‘minimum contact’ relate to the criminal or the crime? And what exactly would amount to a ‘minimum contact’? Fundamentally, when one juxtaposes the territoriality principles of jurisdiction with the notion of cyberlaundering, it conjures up certain factors that serve as determinants, which may or may not indicate the applicability of the territoriality principle. These include the location of the acts, the computer, the person, and the effect(s).

6.4.2.1.1 Location of the act

This implies that a state party can claim jurisdiction on the basis of territoriality where the act or omission (i.e. conduct) of the crime in question was committed on its territory. As far as cybercrime is concerned, several states have tried to adopt the very broad principle of territoriality for cybercrimes. An interesting example is Tasmania. Article 257F(2)(a) of the Tasmanian Criminal Code Act of 1924 provides that jurisdiction would be established where a significant part of the conduct relating to, or constituting the doing of the act, takes place in or within the Tasmanian territory. Several

991 See page 326 of the judgment.
states of the US, too, have similar positions. For example, in Arkansas, North Carolina and Connecticut, if the transmission that constitutes the offence either originates or is received in a state, that state can found jurisdiction on the basis of the territoriality principle.\textsuperscript{992} In Europe, on the other hand, most countries establish jurisdiction when the act is committed within their respective territories, without regard to the nature of the type of cybercrime concerned. For example, in the Netherlands, Belgium and Germany, jurisdiction can be established over persons who have committed offences within their respective territories.\textsuperscript{993} The territoriality principle of jurisdiction in relation to the location of the act, as contained in the domestic anti-cybercrime laws of these countries, have an overarching approach. This approach, which appears to be borrowed from Article 22(1)(a) of the Budapest Convention, to which these countries are parties, is blurry and ambiguous. Impliedly, the determination of the location of the act is a question that is left open.

It has been said that cyberlaundering is ubiquitous in nature and, as such, it is not an easy task to ascertain the place where a particular act is committed. Consequently, due to its nature, cyberlaundering has the potential of founding jurisdiction almost everywhere the conduct is carried out, just as is the case with the traditional concept of money laundering. Thus, given the


hypothetical scenario above, it follows that Jack Sparrow and John Doe committed the conduct of cyberlaundering in Germany, as they performed the laundering within the German jurisdiction, even though Jim Watson is not within that territory. The conduct in this sense relates more to the person than to the actual workings of cyberlaundering. As such, like the objective territoriality principle of money laundering discussed earlier, Melbourne would still be unable to found jurisdiction for the cyberlaundering offence committed by Jack Sparrow and John Doe.

6.4.2.1.2 Location of the computer

Another possibility that lies under the territoriality principle of jurisdiction as regards cybercrime, is the location of the computer that is instrumental in the commission of the crime. This would mean that jurisdiction can be founded on the basis of territoriality, if the computer used is within the territory of the country seeking to found jurisdiction, or if some part of the conduct impacts on a computer that is located within the relevant state.\footnote{Brenner and Koops (2004: 16). Cf Koops and Robinson (2011: 179).} Certain countries in Asia, such as Malaysia and Singapore, require not only that the computer, but that also its program and data to be located within its jurisdiction at the relevant time.\footnote{See article 11(3) of the Singapore Computer Misuse Act of 1993, and article 9(2) of the Computer Crimes Act of 1997.} This also applies where satellites are used as instruments for crime. As they orbit around the world, and are not situated in a designated territorial space, it is plausible for the ground station of the satellite to count

---

as the computer for the purposes of founding jurisdiction.\textsuperscript{996} Even considering the fact that satellites are registered in different jurisdictions, and are deemed to have the ‘nationality’ of the country in which they are registered, a potential jurisdictional conflict may arise where the ground station of the satellite is located in a different location from the jurisdiction where it has ‘nationality.’

Generally, the issue of jurisdiction is dependent largely on the nature of certain types of cybercrime. The basis upon which the location of a computer can be used as link to a crime is determined by the nature of the particular cybercrime, which is, in turn, ascertained by the relevant elements constituting the crime. This might pose a challenge, given that computers could have complex structures and workings, because of their networked or interconnected nature. The matter is further complicated when several networked or interconnected computers are located in more than one jurisdiction. The complication grows and reaches a higher level of abstraction for offences committed using websites. For example, some content-related cybercrime offences such as offences related to child pornography and hate speech involve, principally, two distinct facilitators, namely, the web server\textsuperscript{997} and the content provider.\textsuperscript{998} In principle, for content-related


\textsuperscript{997} A web server refers to computer hardware, or computer software, such as a computer application that delivers accessible content through the internet. The web server is often used to host websites, amongst other functions such as enabling gaming activities, storing of data, as well as for conducting several internet enterprises. See Web Developers Note (an undated website document) ‘What is web server - A computer of a program’ available at <http://www.webdevelopersnotes.com/basics/what_is_web_server.php> [accessed on 1 March 2012].
offences, liability for the crime is not associated with the web server alone, but also with the content provider, if they are not one entity. Again, the difficulty arises when the web server and the content provider are not located within the same jurisdiction.

This is very hard to tell for cyberlaundering, depending on the nature of the relevant cyberlaundering operation. For our purposes, the web server and the content provider are located within the same jurisdiction, which is Germany, and it, Germany, could easily claim jurisdiction for the conduct of Jack Sparrow and John Doe. Thus, Melbourne is yet unable to found jurisdiction.

Equally, Antigua could claim jurisdiction because the web server is registered there. For other methods of cyberlaundering, such as online banking and virtual worlds, it is highly possible for the web server to be separate from the content provider, which harbours the danger that they might have different locations. This would be the case, for example, where Jack Sparrow ran a gaming website from Germany (i.e. having the web server based in Berlin), and employed the services of Company X in Angola, a renowned content provider for online gaming websites. Just as with Antigua, where the necessary links are established, Company X could, at the very least, be

---

998 A content provider is an enterprise that develops content for electronic commerce websites. It studies and incorporates a search engine optimized technology to help customers find content, and it tends to attract the attention of website users. The fact that all website owners (i.e. having the web servers) do not always create their own content tells why a content provider’s business is lucrative, given as most of such website owners often lack the skill. See eHow (an undated internet article) ‘What is an Internet Content Provider’ available at <http://www.ehow.com/about_6695350_internet-content-provider_.html> [accessed on 2 March 2012].

999 See discussion in Chapter 3, paragraph 3.6.1.

1000 See discussion in Chapter 3, paragraph 3.6.6.
regarded as an accessory to the crime, if it has the requisite \textit{mens rea}, amongst other elements of the crime.\textsuperscript{1001}

6.4.2.1.3 \textit{Location of the victim}

Whereas the victims of most cybercrimes are easily identifiable, this is not necessarily the case with cyberlaundering. One may therefore ask: Who is the victim of cyberlaundering? Much like money laundering, the same principles apply here. The protected interest of the offence of money laundering is the economy of the relevant state, and, arguably, the global economy, because, viewed conversely, the crime seeks to destabilize the global economy, causing disruption in commerce, while obstructing justice and undermining operations of law enforcement agencies. Therefore, the state is the victim of the cyberlaundering offence.

In light of the hypothetical scenario, it is wrong to presume that Jim Watson is the victim of the cyberlaundering offence(s) committed by Jack Sparrow and John Doe. Jim Watson is the victim of cyberfraud, and not cyberlaundering. Again, the Melbourne authorities would not be able to assert territorial jurisdiction on this basis. On the contrary, Germany and Antigua, as victim states, can found jurisdiction based on this principle.

\footnote{1001 As a further example, this principle also reflects largely with virtual worlds, and the act will be said to have been committed in the territory where the web server and content provider of the virtual world website are located within the territory of the country seeking jurisdiction.}
6.4.2.1.4 Location of the effect

This rationale purports that territorial jurisdiction can be established for any cybercrime if the effect(s) of the crime are felt by the country asserting jurisdiction. The effects of cybercrime can be indeed varied, and this issue links with the previous discussion. The effect of the crime can only be ascertained to the extent to which it impacts on the victim(s). For most kinds of cybercrime where the victims can be identified easily, for example where someone causes a virus attack on computers, clearly, the persons who own the computers are the victims, and are the ones affected by the crime. For example, in the UK, jurisdiction would be founded irrespective of whether the computer, the program or the data are located within the country’s jurisdiction, so long as the effect is felt within its jurisdiction.\(^{1002}\) The word ‘effect’ in this context can mean anything, as it is quite broad. However, one salient feature that should serve as a common denominator or determinant of the ‘effect’ in question is harmfulness – that is, such effect should be harmful.\(^{1003}\) Similarly, for cyberlaundering, the effect of the crime is felt by the state due to the fact that it is its, the State’s, protected interest that is violated. Therefore, in light of our scenario, once again, Germany is the only state that can assert jurisdiction due to the fact that the laundering operations were carried out and completed within its jurisdiction. The argument is that

---

\(^{1002}\) See article 5(2)(b) of the Computer Misuse Act of 1990, Chapter 18. Cf a similar provision exists in article 257F(2)(b) of the Tasmanian Criminal Code Act of 1924.

\(^{1003}\) This principle is supported in the case United States of America v. Nippon Paper Industries Co. Ltd 109 F. 3d 1, 7 (1st Cir. 1997) where the court elucidated the matter in depth, stating that a state can readily proscribe conduct outside its territory, where such conduct has a substantial effect within its territory, so long as the standards of reasonableness are met.
the effect is felt within its jurisdiction because the illegal proceeds have been integrated into its economy, thus posing a danger to it.

6.4.2.2 The nationality principle

Another important principle that is embedded in the Budapest Convention is the nationality principle. Article 22(1)(d) of the Convention requires a member state to the Convention to establish jurisdiction when the offence is committed by one of its nationals, where the offence is committed outside the territory of the state. It is also important to juxtapose this principle against the concept of cyberlaundering in order to determine its applicability and suitability to the concept.

Generally, the nationality principle always comes second in the ranking order, after the territoriality principle, given the fact that in practice the nationality principle is always applied as an exception to the territoriality principle. For example, in some countries in Europe, such as Germany, the Netherlands, Belgium and the UK, there is a general jurisdictional clause that exists, which allows jurisdiction to be founded over a crime that is committed by a national of the respective states, if the act is punishable where it was committed.\(^{1004}\)

Dual criminality, which implies that the conduct must have been criminalized

\(^{1004}\) See sections 7(2)(1) of the Strafgesetzbuch (German Criminal Code of 1998); article 5(1)(2) of the Wetboek van Strafrecht (Dutch Criminal Code of 1994); article 11 of the Wet houdende de voorafgaande title van het Wetboek van Strafverordening (Belgian Criminal Code of 2012) and the sections 4 and 5 of the Computer Misuse Act of 1990, Chapter 18. Cf South African legislation: Section 90 Electronic Communications and Transactions Act No. 22 of 2002.
in both states, is often a requirement.\textsuperscript{1005} The key element here is to ascertain whether the perpetrator is a national of the state asserting jurisdiction, which often requires proof of the perpetrator’s citizenship. However, other than the nationality of the perpetrator, some countries also have laws that found jurisdiction on the basis of the nationality of the victim.\textsuperscript{1006} But insofar as it pertains to cyberlaundering, this is comparable to the discussion on the territoriality principle above concerning the location of the victim. Bearing in mind that the concept of ‘victim’ in this case is the same (i.e. the state), the same rationale is applicable.

Thus, in line with this principle, given that Jack Sparrow and John Doe are Germans, and not Australians, nor Antiguans, Germany alone can claim jurisdiction on this basis for their cyberlaundering operations.

6.4.2.3 The universality principle

An interesting issue at stake is that of universal jurisdiction. This is an international principle of jurisdiction that is enshrined in customary international law, in terms of which any state can claim jurisdiction over a crime where the crime violates the interests of the international

\textsuperscript{1005} This principle is embedded in Article 18(9) of the Palermo Convention and Article 7 (15) (c) and (d) of the Vienna Convention.

\textsuperscript{1006} This is typically the case with Germany and Belgium. See sections 7(2)(1) of the Strafgesetzbuch (German Criminal Code of 1998), and article 11 of the Wet houdende de voorafgaande title van het Wetboek van Strafvoordering (Belgian Criminal Code of 2012). Certain states in the US such as Michigan also have similar provisions. See section 762.2(1)(d) of the Michigan Compiled Laws, Act of 2004.
This principle is premised on the philosophy that certain basic social norms are *erga omnes*, which is to say that there are rights and duties owed to the international community at large. Therefore, a violation of these norms warrants prosecution by the international community. The principle of universal jurisdiction is rather peculiar because it implies that any country can claim jurisdiction regardless of where the crime was committed, and regardless of the nationality of the victim or perpetrator, as well as any other protective interests a country might have. Due to its sweeping scope, it is controversial and must be applied with great deal of sensitivity in the international arena. The principle is adopted for only selected crimes, and depending on the country, only very few types of cybercrimes fall within its ambit. The principle is generally ranked last in the scale of jurisdictional principles, and is often deemed as the last resort amidst the other principles of jurisdiction. Although the Budapest Convention does not cite it as a jurisdictional ground for the cybercrimes listed under the Convention, the principle is significant to the ACL campaign.

Within the broader discourse of the AML legal regime, amongst several other reasons, universal jurisdiction is important because it helps to prevent a case.

---

1008 This principle was propounded further in the case before the International Court of Justice: *Belgium v Spain (Second Phase)* ICJ Rep 1970 3 at paragraph 33.
1009 For example, in the Netherlands, cybercrimes do not fall under the universal jurisdiction clause (article 4 of the *Wetboek van Strafrecht* (Dutch Criminal Code of 1994). Conversely, countries such as Germany and Belgium can claim universal jurisdiction for prosecuting the cybercrime of child pornography - article 184(3) of the *Strafgesetzbuch* (German Criminal Code of 1998) and article 10ter(1) of the *Wet houdende de voorafgaande van het Wetboek van Strafvordering* (Belgian Criminal Code of 2012). Cf commentaries by Brenner and Kooper (2004: 28).
where money launderers take advantage of the inherent discrepancies in different legal systems for their illicit activities, otherwise known as jurisdictional arbitrage. This raises an interesting question: Given the transnational nature of money laundering that impact on the world economy, why is it currently impossible to assert jurisdiction over cyberlaundering on the basis of universal jurisdiction? A succinct answer is simply that a solid ACL regime is currently lacking. Coupled with this dilemma, an awareness of the problem is equally lacking, let alone the fact that in practice many countries choose not to assert universal jurisdictional over certain crimes. Without a strong international consensus on how to combat cyberlaundering, the principle of universal jurisdiction is ineffective. But universal jurisdiction is bound to become a topical matter once cyberlaundering becomes conceptualized internationally.

Interestingly, a federal law of the US envisages the scenario where universal jurisdiction can be claimed over a crime that impacts on the international economy or foreign commerce. Sections 1030(e)(2)(B) of Title 18 of the United States Code provides that the US government can exercise jurisdiction over criminal activity that affects interstate or foreign commerce. As such, given that the protected interest of cyberlaundering is both local and international commerce, as with money laundering, it can be argued that the principle of universal jurisdiction is embedded in the national law of the
However, given that cyberlaundering, as a legal concept, is not yet grounded in the legal system of the US, this raises concerns of legality because jurisdiction cannot be founded for a non-existent crime.

Applying the principle of universal jurisdiction to our hypothetical scenario, Australia, and in particular, the authorities in Melbourne, Germany, Antigua and any other country that can prove the minimum basis of this principle, can claim jurisdiction over the crime of cyberlaundering committed by Jack Sparrow and John Doe, because their illicit activities can be considered as acts that impact negatively on global commerce.

6.4.3 Guidelines for establishing cyberlaundering jurisdiction

When faced with a scenario or case of cyberlaundering, that is, where from the facts of a case, the elements of cyberlaundering are clearly identifiable, there are three steps that merit consideration in order to adjudge the issue of jurisdiction properly. These steps are premised on the standard of reasonableness, which should be the yardstick with which all cases should be measured in accordance with their relevant respective facts. They are necessary to establish jurisdiction for cyberlaundering. These steps are discussed below.

---

1010 Section 1030 (e)(2)(b) of the United States Code also embeds another principle of international jurisdiction known as the principle of protection. This principle allows a state to exercise jurisdiction over alleged crimes committed outside of its borders, where such allegedly committed crimes threaten its security and basic functions. Nichols (1997: 305). Cf Brenner and Koop (2004: 26). The protective principle is not included in the Budapest Convention and is not discussed separately due to the fact that it would be a reiteration of the universality principle with which it is synonymous.
6.4.3.1 Determining the cyberlaundering conduct

The first step in establishing jurisdiction for cyberlaundering is first to determine the cyberlaundering conduct. This is crucial at the outset, as it is important to delineate clearly the relevant conduct in order not to confuse the activity of cyberlaundering with the underlying predicate offence. From our hypothetical scenario, it is important to examine first the relevant conduct of the accused persons. Jack Sparrow and John Doe committed cyber fraud (i.e. the predicate offence), because they intentionally defrauded customers through their website business, and laundered the illicit proceeds through the same means in order to evade law enforcement (i.e. cyberlaundering).

6.4.3.2 Determining the cyberlaundering avenue

The next step is to identify the platform or means used. Cyberlaundering is always perpetuated or propelled through a particular avenue, or through multiple avenues, as the case may be. Given our scenario, the relevant avenue is the website ‘www.comfortzonefurniture.com’ which was operated by Jack Sparrow and John Doe. This website was operated not just to defraud customers, but also, to launder their illicit proceeds. The illicit proceeds were laundered by them funnelling the illicit funds towards the maintenance and development of the website and their other websites. In fact, for cyberlaundering to be performed on a full-blown scale, one would expect
multiple avenues to be used for the ‘washing’ of illicit funds.\textsuperscript{1011} The ‘washing’ of illicit proceeds, in the cyberlaundering sense of the word can be indeed blurry. Illicit funds that are properly ‘washed’ detract law enforcement bodies from tracing and finding such funds, because an essential trail is obscured. As such, it is imperative to ascertain clearly ‘how’ the illicit funds are laundered, because this would indicate ‘where’ the act was committed and would help to establish a proper ground for exercising jurisdiction.

\textbf{6.4.3.3. Determining the applicable jurisdictional principle}

After establishing the avenue(s) used for the relevant cyberlaundering operation, it becomes easy to establish the correct principle of jurisdiction, and to apply it to the existing facts. To do this, one has to delve into existing laws, because any principle of jurisdiction must be founded on legal grounds. It is important, again, to reiterate that cyberlaundering is not yet conceptualized legally, both on the national and international plane, which points to the purposes and importance of this study. For purposes of jurisdiction, the general principles applicable to combating cybercrime are more suited to the concept of cyberlaundering, and such principles should be considered in making such an assessment. In practice, the territoriality principle ranks first in line, the nationality principle second, with other

\textsuperscript{1011} For example, a criminal mastermind who knows his way around the internet could very well combine multiple avenues in order to launder his funds. The avenues of online banking, online gambling, virtual worlds, and online barter trading are but only few examples of such avenues. See discussion in Chapter 3, paragraph 3.6.
possible claims such as the universality principle following after.\textsuperscript{1012} It is quite possible for more than one jurisdictional principle to apply to a cyberlaundering situation. For example, given our scenario, Germany and Antigua can both claim jurisdiction for the prosecution of Jack Sparrow and John Doe on the grounds of territoriality, and specifically, the location of the computer and the victim.\textsuperscript{1013}

However, to avoid the possibility that the accused persons are prosecuted more than once for their offences, in line with the principle double jeopardy, which is a safeguard, a test premised on reasonableness must be conducted to ascertain where the accused persons should be prosecuted. This often involves striking a fine balance between the interests of justice on the one hand, and on the other, some logistic considerations, such as convenience.\textsuperscript{1014}

But the applicable standards are dependent on the criminal procedural laws of the relevant country. An international convention that provides for this scenario would most certainly erase all doubts and uncertainties surrounding conflicting jurisdictional claims. Thus, in line with the fundamental rationales underlying the jurisdiction to prescribe, the jurisdiction to adjudicate and the jurisdiction to enforce,\textsuperscript{1015} once the crime of cyberlaundering is properly proscribed in national and international laws, a much clearer framework would have been set in place that would determine the relevant court of law.

\textsuperscript{1013} See discussion in pages 33 and 36 above.
\textsuperscript{1014} Cf Aas (2007: 130), Bermann (2003: 106,183 and 226) and Siegel and Borchers (2005: 136).
having jurisdiction to hear the matter, and the relevant authority with the jurisdiction to enforce judgment.

In the given the scenario, Germany can found jurisdiction on multiple grounds, such as territoriality and nationality, and thus has a stronger claim. Also, supporting Germany’s possible claim to prosecute are convenience and cost effectiveness, given that the accused individuals are within its territory. It would not, therefore, be logical for them to be extradited to Antigua, because Germany can make the same and more claims that Antigua could make. This is not to say, however, that Australia is entirely without recourse. Where it is able to found jurisdiction to prosecute Jack Sparrow and John Doe on the predicate offence of cyberfraud, on the basis of territoriality (i.e. location of the victim within its territory), coupled with the argument of convenience, it could also found jurisdiction simultaneously for cyberlaundering on the basis of universal jurisdiction.

Overall, as regards matters on international prosecution, it should be borne in mind that aside from having clear-cut principles, things are not always crystal clear, nor do they portray fully the essence of the black-letter law. At times, clearly set principles are blurred by political undertones that serve as a barrier to prosecution.\textsuperscript{1016}

\textsuperscript{1016} Cf discussion in footnote 989 above.
6.5 THE NEED FOR AN ACL PROSECUTORIAL FRAMEWORK: EXAMPLE OF REAL CASES

As the discussion thus far has shown, there is a dire need to establish an ACL prosecutorial framework. This fact is further augmented by the existence of real cases and scenarios. Current laws do not mirror the reality of cyberlaundering, and this makes one wonder whether laws are truly as dynamic as they are made out to be. Several cyberlaundering cases go undetected, uninvestigated, and consequently, unprosecuted because an ACL legal regime does not exist. There are several cases that evidence this fact. Some of these, such as *United States of America v. E-Gold Ltd, Douglas Jackson, Barry K. Downey, and Reid A. Jackson*, and the pending case against the founder of Megaupload Ltd, Kim Dotcom, are now discussed.

6.5.1 *United States of America v. E-Gold Ltd, Douglas Jackson, Barry K. Downey, and Reid A. Jackson*

The case against E-gold Ltd in the United States (US), which resulted in the court case of *United States of America v. E-Gold Ltd, Douglas Jackson, Barry K. Downey, and Reid A. Jackson*, might well be the first glaring depiction of the prosecutorial challenges surrounding cyberlaundering. The facts and significance to the ACL legal framework are elaborated upon further.

---

6.5.1.1 Facts

E-gold Ltd is a value remittance company that is operated by Gold and Silver Reserve Inc, registered in Nevis in Saint Kitts and Nevis. The company allows for the instant transfer of e-gold ownership between its registered users.\textsuperscript{1018} E-gold is represented in the form of a digital gold currency.\textsuperscript{1019} Established in 1996, the company witnessed great success as its total number of e-gold accounts grew from 1 million in November 2003 to 5 million in 2008.\textsuperscript{1020} However, its success was tainted with illegality when accusations of fraud and money laundering began to emerge.\textsuperscript{1021} In May 2006, the US government indicted E-gold Ltd, along with Gold & Silver Reserve Inc, as well as the founders of E-gold, who are Douglas Jackson, Barry K. Downey, and Reid A. Jackson, on six counts of having violated the provisions of the United States Code (U.S.C.) and the District of Colombia Code (D.C. Code). The charges included conspiracy to launder monetary instruments (section 1956, Title 18 U.S.C), conspiracy (section 371, Title 18 U.S.C.), operation of unlicensed money transmitting business (section 1960, Title 18 U.S.C.), money transmitting without a license (section 1002, Title 26 D.C. Code), aiding and abetting and causing an act to be done (section 2, Title 18 U.S.C),

\textsuperscript{1018} See discussion on E-gold Ltd above in Chapter 3, paragraph 3.4.4.
\textsuperscript{1019} Digital gold currency is a form of electronic money based on ounces of gold weighed digitally. For a detailed discussion on electronic payment system, see Chapter 3, paragraph 3.3.3.
\textsuperscript{1020} See the website of Gold and Silver reserve Inc at <http://www.e-gold.com/unsecure/pgpkey.htm> [accessed on 13 February 2012].
\textsuperscript{1021} Prior to this time, several other e-gold currency companies had come to compete with E-gold Ltd such as OS-Gold, Standard Reserve and INTGold, but none recorded the measures of success recorded by E-Gold Ltd. Most of these other companies have been under scrutiny for money laundering and for being a facade of a sheer Ponzi Scheme. Cf Hallam-Baker (2008: 343).
and criminal forfeiture (section 982(a)(1), Title 18 U.S.C.). The indictment further cited E-Gold Ltd as an unlicensed money transmitting agency that “moves illegal funds for wit.” Faced with fines to the tune of $3.7 million, the accused entered guilty pleas to conspiracy to engage in money laundering and conspiracy to operate an unlicensed money transmitting business. In the resulting case, United States of America v. E-Gold Ltd, Douglas Jackson, Barry K. Downey, and Reid A. Jackson, the Court ruled against E-gold Ltd, stating that “a business can clearly engage in money transmitting without limiting its transaction to cash or currency, and would commit a crime if it did so without being licensed.” As result of their guilty pleas, most of the charges against them were dropped, and their sentence was reduced.

### 6.5.1.2 How cyberlaundering comes into play

The prosecutors could not pin the choate crime of money laundering onto the accused persons, as their conduct did not meet the key element of the

---

1022 The indictment can be found at website of the US Department of Justice at <http://www.justice.gov/criminal/ceos/Press%20Releases/DC%20egold%20indictment.pdf> [accessed on 13 February 2012].


1025 See page 413 of the judgement.

1026 Together with the sentence of 300 hours of community service for each of the non-juristic entity defendants, they each paid minimal amounts of fines between $300 and $200.
crime.\textsuperscript{1027} As such, the conduct could not be linked directly to them, because they simply operated the website which was the avenue for laundering money. This is why the prosecutor could only make out a case against them for conspiracy to engage in money laundering and conspiracy to operate an unlicensed money transmitting business. As stated earlier,\textsuperscript{1028} cyberlaundering is an extension of money laundering, and the liability for the crime of cyberlaundering equates to money laundering, as the two are not separate offences.

This case highlights an important fact, which is how prosecutors are unable to establish the offence of money laundering ordinarily when the offence manifests in the form of cyberlaundering. Pitted against the elements of cyberlaundering,\textsuperscript{1029} the conduct of the accused persons amounts to cyberlaundering in light of the following:

(i.) The accused persons operated an unlicensed money transmitting business that violated section 1960, Title 18 U.S.C. This is an offence that sufficiently constitutes a predicate offence for cyberlaundering;

(ii.) As they operated the website, they profited from it. This fact justifies the existence of illegal funds, which is the other essential element of cyberlaundering;

\textsuperscript{1027}As discussed in Chapter 3, paragraph 3.2.4.1, the elements of the crime of money laundering include the disguise and concealment of the proceeds of the relevant criminal activity, along with the violation of government or state activities and its management system by causing instability in its financial sector, and obstructing the normal activities of the justice and the investigation of crime, (i.e. the \textit{actus reus} of the crime). Together with this, the requisite \textit{mens rea} elements must also exist on the part of the accused in the form of knowledge and intention of the conduct described.

\textsuperscript{1028}See Chapter 3, paragraph 3.2.4.

\textsuperscript{1029}See Chapter 3, paragraph 3.2.4.2 where the elements of cyberlaundering are discussed at length.
(iii.) The illegal funds were laundered through a computer. The fact that the funds were represented in different forms, such as for the upkeep of the website, or for the purchase of personal assets online, can be deemed a combination of both placement and layering phases of cyberlaundering. The laundering cycle is completed as well, because the illegal funds have been eventually integrated into the commercial world; and

(iv.) As for the mens rea elements of cyberlaundering, it is clear also that the accused persons had (i) knowledge of the fact that the funds were derived from crime and (ii) an associative intention to conceal the origin or source of the illegal funds. This is due to the fact that the perpetrators knew that E-gold Ltd was unlicensed for its operations, but continued with its activities, deriving revenue from it, thus avoiding to register it.

The challenges that come with cyberlaundering as regards the question of jurisdiction, as discussed earlier, do not apply here because the cyberlaundering operation in this case was local and not trans-border in nature. The crime of having an unlicensed website is applicable only to the US as a sovereign state having the right to prescribe the law. Had the prosecutor attempted to prosecute the accused persons for cyberlaundering, where there are other jurisdictions involved other than the US, jurisdictional concerns would certainly arise because the US alone would not have been the only country with the right to claim jurisdiction over the offence.

As is a fundamental theory of law, the principle of nullum crimen, nulla poena sine praevia lege poenali dictates that there can be no crime and no...
punishment without a prior penal law. This is the principle of legality, which applies to cyberlaundering as well. However, given the fact that no ACL legal framework exists yet, the above-mentioned elements of cyberlaundering require legal justification. This further justifies the need to establish a legal framework for cyberlaundering. This shows how the lack of an ACL legal framework frustrates prosecutors, forcing them to resort to desperate actions. In this case, the prosecutor was forced to toil through a labyrinth of existing laws in order to found liability for several offences. Without hitting the mark, all of these offences point only to the existence of the more behemoth crime of cyberlaundering.

6.5.2 The pending case against Megaupload Ltd

A more recent example is the pending case against Megaupload Ltd, which, unlike E-gold Ltd, has yet to be heard in court. The facts of the case and its relevance to the ACL legal regime are now described.

6.5.2.1 Facts

Megaupload Ltd operated the website called ‘www.Megaupload.com,’ together with its other similar websites, which render several web services such as image hosting, video hosting, music hosting, and the hosting of pornographic content. It also provides file-sharing services. Megaupload Ltd

---


has its headquarters in Hong Kong. It was founded in March 2005 by Kim Dotcom (born Kim Schmitz), a German-Finnish computer programmer and business man. The Megaupload website grew to become the 13th most popular website on the internet, with an annual revenue of about US$175 million and an average of 50 million visitors per day.1032

On 5 January 2012, Kim Dotcom, Fin Batato, Julius Bencko, Sven Echternach, Mathias Ortmann, Andrus Nomm, and Bram van der Kolk, all of whom are stakeholders in Megaupload, were charged with violating the provisions of Title 18 of the U.S.C. The crimes with which they were charged include conspiracy to commit racketeering (section 1962(d), Title 18 U.S.C.), conspiracy to commit copyright infringement (section 371, Title 18 U.S.C.), conspiracy to commit money laundering (section 1956(h), Title 18, U.S.C.), criminal copyright infringement by distributing a copyright work being prepared for commercial distribution on a computer network, and aiding and abetting of criminal copyright infringement, (section 2,2319 Title 18, U.S.C.; section 506, Title 17 U.S.C.), and criminal copyright infringement by electronic means and aiding and abetting of criminal copyright infringement (section 2,2319 Title 18, U.S.C; section 506 Title 17 U.S.C.).1033


January 2012, the United States Department of Justice seized and closed the website, Megaupload.com, for purposes of prosecuting the accused persons. At the same time, about 330 million Hong Kong dollars in assets of Megaupload Ltd were frozen by the Customs and Exercise Department of Hong Kong. The arrest followed a long-running investigation against Megaupload, which had involved police and security intelligence in Hong Kong, the Netherlands, Germany, Canada, the United Kingdom (UK) and the United States (US). The accused persons were arrested on 20 January 2012 in New Zealand and kept in the custody of the New Zealand police. At the time of writing, the case is still pending and the accused persons have been remanded in pre-trial police custody.

6.5.2.2 How cyberlaundering comes into play

This case is another clear example of the need to establish clear-cut ACL laws that would aid the prosecution of cyberlaundering. Although the facts are not the same as those in E-gold Ltd, the same principle applies. Just as with E-gold Ltd, the accused persons are charged only with the predicate offences which they are accused of having committed. This is due to the fact that there are no ACL laws in place which would serve as the legal basis for prosecutors to act. Thus, prosecutors are hindered from building a proper case of cyberlaundering against the accused persons, even though the elements of

---

wsj.com/article/SB100014240529702046165045777171180266957116.html> [accessed on 13 February 2012].

cyberlaundering exist clearly from the facts. Premised on the fundamental principle of money laundering that a conviction on a predicate offence is not a prerequisite for a conviction for money laundering, it is quite easy to pursue a cyberlaundering case against the accused persons, proceeding from this standpoint. As shown below, the elements of cyberlaundering can be identified from the facts.

(i.) The defendants ran websites that violate laws, such as the U.S.C and the Digital Millennium Copyright Act. This is a predicate offence for cyberlaundering;

(ii.) The fact that the accused persons have profited from their conduct makes the funds in question illegal in nature;

(iii.) Also, the fact that the illegal funds have been laundered with a computer satisfies another element of cyberlaundering, given the likelihood that the accused invested the proceeds into developing other subsidiary websites. The nature of the business blurs any distinction between placement, layering and integration of the illegal funds. This is due to the fact that the illegal funds derived from the unlawful conduct fostered the conduct itself. The funds were used for several purposes, such as promoting and operating the Megaupload website, as well as establishing other websites. In the long run, the illegal funds were integrated into the lawful economic cycle, of which the business world forms a part; and

\[1035\text{ Cf Articles 3(4) and 3(5) of the Council of Europe Directive 2005/50/EC.}\]
\[1036\text{ Act 28 of 1998, Title 17, United States Code.}\]
(iv.) The *mens rea* elements of cyberlaundering are also present. The parties had (i.) *knowledge* of the illegality of the funds and (ii.) the *associative intention* to disguise its illegality by proceeding with the illegal conduct.  

This case raises very important and interesting issues of jurisdiction for cyberlaundering, in view of the fact that the accused persons are Germans and Finnish nationals who reside in New Zealand and some in Germany, with their website registered in Hong Kong and other websites in the US.

There are several other similar cases where the prosecutor could build a case of cyberlaundering against the accused, but because of the present deficiencies in the law, this is impossible.  

---

1037 Inference can be drawn from the fact that the defendants had a knowledge of the illegality of their conduct due to the fact that, in a prior civil action case against Megaupload – *Perfect 10, INC v. Megaupload, Kim Schmitz Case No. 11cv0191 - IEG (BLM) (2011)* – the court found that the defendant (Megaupload) had directly infringed on the copyright right of the plaintiff. This should have been a good basis upon which Megaupload should have desisted from the conduct.

1038 For example, on 17 January 2012, with the efforts of the Federal Bureau of Investigation (FBI) in the United States, two Russian citizens, Vladimir Zdorovenin and Kirill Zdorovenin, were extradited from Switzerland to the US. They were charged in the US with committing cybercrime offences such as the theft of victims’ personal identification information, including credit card numbers, by means of computer programs that were surreptitiously lodged in the victims’ computers and that recorded the information as it was entered. The accused persons also allegedly purchased stolen credit card numbers from other individuals, and used the stolen credit card information to make ‘legitimate’ purchases of goods from numerous internet businesses that they operated (i.e. layering). Apparently, the purchases were fraudulent and were meant to deceive banks, credit card service providers, credit card holders, among others, thereby enabling the accused persons to steal the money they funneled to their websites. In essence, via the internet, the accused persons successfully laundered the loot derived from the commission of other cybercrimes. Interestingly, the accused persons were not charged with money laundering, because the elements of the crime are not present. However, the elements of the crime of cyberlaundering are present, and, as such, prosecution of this would have been possible, where laws exist to that effect. For more information see Federal Bureau of Investigation ‘Manhattan US Attorney and FBI Assistant Director in Charge Announce Extradition of Russian Citizen to Face Charges for International Cyber Crimes’ Press Release (17 January 2012) available at <http://www.fbi.gov/newyork/press-releases/2012/manhattan-u.s.-attorney-and-fbi-assistant-director-in-charge-announce-extradition-of-russian-citizen-to-face-charges-for-international-cyber-crimes> [accessed on 11 February 2012].
cases underscores the need to establish a prosecutorial framework for cyberlaundering.

6.6 FORMALITIES INVOLVED IN ESTABLISHING THE ACL LEGAL FRAMEWORK

The ACL legal framework that this study has attempted to establish rests on the prevention, compliance and enforcement pillars, as discussed in this chapter and the previous one. However, it is important to consider certain technical issues, or formalities, that would further fortify and entrench the proposed ACL legal framework.

First, the ACL measures suggested in this study should be incorporated carefully into local legislation in order to ensure that the laws have national legal validity. It is one thing to have laws and measures in place, but another thing to have them implemented. For this reason, this study advocates strongly for the adoption and harmonization of the ACL principles across countries. Given the fact that a chain is only as strong as its weakest link, if the requisite ACL laws are disharmonious across jurisdictions, or where some countries have them and others do not, loopholes in the ACL legal framework are created, which cyberlaunderers will exploit quickly. One such loopholes caused by having disharmonious laws is the fact that it creates the possibility for criminals to settle out of court or, even worse, not to be caught at all. This undesirable scenario should be avoided.
Therefore, in order to allay these fears, it is important to guard against this possibility by taking two fundamental initiatives: (i) There should be an international ACL legal agreement to which countries are obliged to accede; and (ii) The agreement should contain provisions that require states to incorporate the provisions of the covenant into their respective national laws.

In line with these initiatives, the Vienna, Palermo and Warsaw Conventions should be amended to accommodate the ACL laws, or, alternatively, a separate ACL agreement altogether should be established. The fact that law is expected to be dynamic in nature only further supports these initiatives. Also, in line with the proposed regulatory initiative to conceptualize cyberlaundering fully under cybercrime as well as money laundering, the ACL legal framework will also need to be incorporated into anti-cybercrime (ACC) laws.

Although it is preferable to have a supra-regional ACL legal agreement, the aforementioned steps can also be achieved by having an ACL agreement that caters for a specific region. This can be achieved by adapting regional covenants against money laundering and cybercrime, or creating new ones, as the case may be. Given that the Budapest Convention is the only international agreement on cybercrime to which certain countries outside of the European Union, such as the United States, Canada, South Africa and Japan, have

---

1039 See discussion in Chapter 5, paragraph 5.5.1.1.1.
1040 However, of all these signatories to the Convention, the US and Japan alone have ratified and brought it into force. The US ratified the Convention on 29 September 2006 and the enforced it on 1 January 2007. Japan signed the Convention on 23 November 2001, and ratified it on 3 July 2012. Cf discussion in Chapter 4, paragraph 4.3.3.5.
acceded, the Convention should be amended to reflect the ACL provisions as well. In keeping with this position, the ACL legal framework will transcend the theoretical sphere, and shall be reality.

6.7 SUMMARY

In addition to the prevention and compliance pillars of the ACL legal regime discussed in the preceding chapter, this chapter has sought to establish the enforcement pillar for the ACL legal regime. This has been done by exploring pertinent legal issues around the prosecution of cyberlaundering. In view of the fact that the path to prosecuting cyberlaundering is not without challenges, this chapter attempts to overcome these challenges by proposing effective legal measures for the investigation of cyberlaundering and how jurisdiction can be established for it. Sadly, the lack of an effective ACL prosecutorial framework continues to fuel cyberlaundering activities, as examples of real cases have shown. Cyberlaundering remains outside the reach of the current AML and ACC legal regimes. Without giving the proposed ACL measures legal validity through incorporation into national and international laws, the manifestations of cyberlaundering activities will only continue to grow. Realizing that any strong standing edifice today was but a plan drawn out at some point in the past, for the future ACL legal regime, one hopes that this study represents the requisite blueprint.

The next chapter concludes this study with some recommendations.
CHAPTER 7

CONCLUSION AND RECOMMENDATIONS

7.1 GENERAL

This study has concerned itself with the problem of cyberlaundering and how to combat it. Like other technological advancements, a problem of the magnitude of cyberlaundering characterizes these modern times. What is alarming about cyberlaundering is that it continues to elude understanding. This is partly because it is not subject to any regulatory framework. There is also no clear-cut method on how to go about prosecuting cases of cyberlaundering. Despite its increasing prevalence, cyberlaundering has not prompted intervention on the side of the authorities concerned, notwithstanding its damaging effects on the economy, both nationally and internationally. Existing laws, without being adapted, are ill-suited for use against cyberlaundering.

7.2 THE TRIPLE-PILLAR COMBAT STRATEGY

This study has sought to understand what cyberlaundering is, how it works, and how it began. Furthermore, the hard laws and the soft laws pertaining to cyberlaundering were evaluated to see whether they could be harnessed to come to grips with cyberlaundering. This appraisal resulted in the proposal/recommendation that an anti-cyberlaundering (ACL) legal regime be constituted of three main pillars: prevention; compliance; and
enforcement. The prevention pillar encompasses measures to prevent cyberlaundering. The compliance pillar identifies parties who should comply on the one hand, and those who should ensure compliance on the other hand. And the enforcement pillar establishes a prosecutorial framework against cyberlaundering.

But it is not enough to enact laws and to promulgate rules and regulations, for these, too, become obsolete with time, especially given the brisk pace at which technology transfigures itself.

The fact of the matter is that, to keep abreast of the cyberlaunderer, every effort needs to be made by the criminal justice authorities to escalate awareness of cyberlaundering amongst regulatory and oversight bodies. Such an awareness campaign will need to be reinforced with both rigorous research into the area of cyberlaundering and institutional capacity building. Each of these three recommended initiatives is briefly explained below.

### 7.2.1 Increased awareness amongst regulatory authorities

As identified in this study, certain individuals and entities have a key role to play in founding the ACL legal regime. In particular, for the proposed compliance pillar of the ACL legal regime, certain persons bear the responsibility of ensuring the duty to comply, while certain other parties bear the duty to ensure compliance.\(^{1041}\) It is unfortunate, however, that persons upon whom it is incumbent to ensure compliance are unaware of the problem.

---

\(^{1041}\) Cf detailed discussion of this principle in Chapter 5, paragraph 5.6.

---
This pertains mainly to governments and their respective relevant authorities and agencies, such as the investigative and prosecutorial authorities, the Financial Intelligence Units (FIUs) and other regulatory agencies.\textsuperscript{1042} Presently, the problem of cyberlaundering is alien to these regulatory entities.\textsuperscript{1043} This is an enigma and a barricade to its regulation. As a result, the problem of cyberlaundering continues to go undetected and unregulated.

As a necessary first step, the designated regulatory authorities need to be made aware of what cyberlaundering is and what havoc it wreaks.\textsuperscript{1044} Even more, there should be increased awareness at the international level. In pursuance of the proposal that both the current anti-money laundering (AML) and anti-cybercrime (ACC) legal regimes be adapted to accommodate the concept of cyberlaundering,\textsuperscript{1045} the respective key institutions of these two regimes that individually fight money laundering and cybercrime need also be made aware of the problem. For example, Interpol,\textsuperscript{1046} which has championed recent international ACC campaigns, needs to rally and facilitate awareness amongst states members. Interpol’s role is especially important to the enforcement pillar of the anti-cyberlaundering (ACL) legal regime proposed in this study, particularly in relation to the investigation of cyberlaundering.

\textsuperscript{1042} Cf discussion in Chapter 5, paragraph 5.6.2.
\textsuperscript{1043} Further proof of this is evident in the fact that prosecutors are not able to find the trail of cyber laundering in various crimes they investigate, which blatantly bear the cyberlaundering elements. Cf discussion in Chapter 6, paragraph 6.5.
\textsuperscript{1044} Cf discussion on the effects of cyberlaundering in Chapter 1, paragraph 1.2.1.
\textsuperscript{1045} Cf discussion in Chapter 6, paragraph 6.6.
\textsuperscript{1046} For discussion on Interpol in relation to cyberlaundering, see Chapter 4, paragraph 4.3.2.4.6.
As pointed out already, the Financial Action Task Force (FATF) is not entirely oblivious of the predicament.\textsuperscript{1047} Through its numerous policy papers, it has identified some of the many dangers of cyberlaundering, such as new payment systems (e-payment systems, as discussed in this study) and online gambling.\textsuperscript{1048} However, it has not identified cyberlaundering as a legal concept, and has not recognized its full legal ramifications. In line with another solution proposed in this study for the legal conceptualization of cyberlaundering,\textsuperscript{1049} and given the powerful influence that the FATF has in ensuring state compliance with AML laws, this study strongly recommends that the FATF should play a lead role in the legal conceptualization of cyberlaundering and its adaption into the current AML legal regime. This can be accomplished by issuing FATF policy paper(s) on cyberlaundering as a legal concept and its looming legal ramifications, with a strong recommendation to states to incorporate its recommendations in their respective national AML laws.

When the FATF recently revised and emboldened its Forty Recommendations in February 2012, now embodied as the “International Standards on Combating Money Laundering and The Financing of Terrorism and Proliferation,”\textsuperscript{1050} the subject of cyberlaundering was still not given the

\textsuperscript{1047} For discussion on the FATF in relation to the phenomenon of cyberlaundering, see discussion in Chapter 4, paragraph 4.3.2.4.1.4.


\textsuperscript{1049} Cf discussion in Chapter 5, paragraph 5.5.1.1.1.

needed attention. The FATF needs to consider, as a matter of pressing priority, amending its Recommendations so as to prevail on states to implement an ACL legal regime. The FATF’s international standards have since been the template upon which the current AML legal regime rests. As such, in line with the adaptive approach proposed in this study, they form the right starting point from which to begin forging the prevention, compliance and enforcement pillars of the ACL legal regime.

Furthermore, the lead role expected of the FATF is one that should be shared by the Basel Committee on Banking and Supervision (BCBS).\textsuperscript{1051} As with the FATF, the BCBS has also identified one of several dangerous avenues of cyberlaundering, which is online banking.\textsuperscript{1052} Through its widely reputable policy papers, it could place the issue of cyberlaundering in the foreground, playing up the need for countries to enact or implement remedial and preventive measures. This is especially pertinent to the prevention pillar of the ACL legal regime. Similarly, the Egmont Group\textsuperscript{1053} can create awareness on its part by raising consciousness and dispensing information through its FIUs,\textsuperscript{1054} which are situated strategically in countries all over the world.

The Egmont Group, the FATF and the BCBS are key players in the ACL campaign because their work is crucial to the compliance pillar of the ACL

\textsuperscript{1051} For discussion on the BCBS in relation to cyberlaundering, see Chapter 4, paragraph 4.3.2.4.3.
\textsuperscript{1052} Basel Committee on Banking Supervision (2001A: 9). Cf discussion in paragraph 4.3.2.4.3.
\textsuperscript{1053} For discussion on the Egmont Group in relation to cyberlaundering, see Chapter 4, paragraph 4.3.2.4.4.
\textsuperscript{1054} For ways in which the FIUs help with the detection and eventual prevention of cyberlaundering, see discussion in Chapter 6, paragraph 6.3.3.2.
legal regime. This is due to the fact that they make up the other limb of the compliance pillar, as they have a duty to ensure compliance. By conjuring and creating awareness at an international level, these efforts will trickle down to the national level, as in a spiral or domino effect, which would help in instilling the needed awareness amongst states. Awareness will certainly help to kick-start the creation and workings of effective supervisory and monitoring systems.

7.2.2 Continuous research

Research into the mechanics and legal ramifications of cyberlaundering is key to finding how best to combat it. As cyberlaundering evolves from the traditional notion of money laundering, and given the way in which it has adapted or shape-shifted into seemingly unfathomable technological schemes, one would be wrong in thinking that the current cyberlaundering techniques have attained the zenith of their mastery. Not so, for cyberlaundering is a rapidly mutating craft which can only be hobbled by using up-to-date tools. This is why the role of research is an indispensable tool to come to grips with the problem. It is required in order for lawmakers and criminal justice authorities to be on par, if not a step ahead of the machinations and the convoluted schemes of cyberlaunderers. More importantly, the idea is to develop a fund of knowledge and skill that is needed to inform the substantive and procedural measures that are required to deal with cyberlaundering.
7.2.3 Capacity building

Capacity building for the ACL legal regime does not only mean ensuring barricades are currently in place against cyberlaundering, but developing new ones against the growing threat of the problem. The road ahead becomes a daunting one when and where there is no capacity to establish and to enforce an ACL legal regime. Human and institutional capacity should be developed to tackle cyberlaundering comprehensively. Given its novelty and shifting nature, training and developmental initiatives on the issue of cyberlaundering are essential to fighting it. To this end, symposiums, seminars and round-table colloquiums on the issue of cyberlaundering need to be held. Experts need to be brought in from the different cyberlaundering-related disciplines to rub minds on the issue. What springs to mind here are specialists in computer science, information technology, AML law and ACC law. Also, because the concept of cyberlaundering is home to each of these different disciplines, the issue should be debated in the respective forums or conferences of each discipline. This would not only help in creating the much needed awareness of the problem, but also current trends can be tracked, and potential regulatory possibilities to counteract the problem can be conceived.

In addition, this study also recommends that capacity be built in the area of formal education. The academic disciplines of computer science, cybercrime, information technology, and money laundering should augment their syllabuses to include the issue of cyberlaundering. Where the subject of cyberlaundering is inculcated into study modules, invariably, students are
groomed at an early stage, and potential or capacity for the future ACL legal regime is forged.

7.3 EPILOGUE
Famed French writer of the 1920s, Marcel Labordere, wrote 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.” As a result of the economic renaissance that swept the earlier part of the 21st century, the concept of money and its varied sociological implications came under a different light. With giant economies of the world today teetering on the edge of recession that is most reminiscent of the Great Depression, and with some having succumbed already, the sociological phenomenon of money, which shapes human behaviour, is one that needs revisiting, as an understanding of this phenomenon equates to an understanding of a particular form of human behaviour. This, invariably, underscores the essence of money laundering, as a planet within this universe, for human greed and the insatiable depths of the human mind are philosophical and sociological explanations of money laundering. And given the new breed it has spawned, called cyberlaundering, the same explanation also holds for the latter. Cyberlaundering is a confluence of human wit and malignity, and a sheer representation of the kind of evil inherent in the human mind’s stream of

---

As personal and corporate greed continues to drive the current financial sector, the subject of money laundering and its cyberlaundering representation is brought to the fore. Unequivocally, the continued growth of global economic instability being witnessed today is in no small way due to the vast scale of undetected laundering operations carried out covertly through the internet. The economic interest that the current AML legal regime seeks to protect continues to fall prey to those against whom the prosecution is needed. This serves as a stark reminder of the pressing need to revert to the drawing board.

If this study serves an ultimate purpose, it is to prompt action, for the journey has only just begun. Continued laxity carries with it greater costs than what just meets the eye today. One cannot afford to lag behind, or be deterred by the legal challenges that come with cyberlaundering. With the right pillars of the ACL legal regime in place, cyberlaundering, in its monstrosity, would no longer seem insurmountable.

[Word count with footnotes: 109, 362]

1056 In hindsight, this is also reminiscent of the strong words of Mark Antony’s character in William Shakespeare’s Julius Caesar: ‘the evil that men do lives after them; the good is oft interred within their bones.’ Shakespeare (1994: 42).
LIST OF REFERENCES

PRIMARY SOURCES

International instruments


Council of Europe Convention on Cybercrime adopted by the Council of Europe on 8 November 2001 and came into force on 1 July 2004.


Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, adopted by the Council of Europe on 8 November 1990, and entered into force on 1 September 1993.


Council of Europe: Measures Against the Transfer and Safekeeping of Funds of Criminal Origin: Recommendation No R (80) and Explanatory Memorandum, adopted by the Committee of Ministers of the Council of Europe on 27 June 1980.


United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, which was adopted by the General Assembly of the United Nations on 7 December 1987, and entered into force on 11 November 1988.


Official reports


The Legal Regime for Anti-Cyberlaundering / Daniel Leslie


mastercard-releases-prepaid-market-sizing-report.html> [accessed on 30 August 2011].


**Domestic laws**

**Australia**


**Belgium**

Belgian Criminal Code (*Wet houdende de voorafgaande title van het Wetboek van Strafvordering*) 2012.

**Canada**

Proceeds of Crime (Money Laundering) and Terrorist Financing Act (S.C. 2000, c. 17).
Germany


Federal Data Protection Act of 2001 (Bundesdatenschutzgesetz - BDSG).


German Criminal Code of 1998 (Strafgesetzbuch - StGB).

Telecommunications Act of 2004 (Telekommunikationsgesetz - TKG).

India

Information Technology Act No. 21 of 2000.

Indian Penal Code Act No. 45 of 1860.


Malaysia


Netherlands


Nigeria


Singapore

South Africa


Tasmania

Tasmanian Criminal Code Act of 1924.

United Kingdom

Digital Economy Act 2010 (Chapter 24).
Drug Trafficking Offences Act of 1986 (Chapter 32).
Prevention of Terrorism Act of 1997 (Number 807).
Terrorism Act of 2000, Chapter 11.

United States of America

Federal Laws

Banking Act of 1933 (Public Law Number: 73-66).
District of Colombia Code [D.C. Code].
NV Senate Bill 82-75th (BDR 14-266), adopted on 1 July 2009 by the House of Senate, Nevada, United States.
Uniting and Strengthening America by Providing By Providing the Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001(Public law number 107-56).
United States Code [U.S.C].

State laws
SB-82 (NV Senate Bill 82-75\textsuperscript{th}, BDR 14-266) of Nevada, which came into effect on 1 July 2009.

**Court cases**

*International Court of Justice*

*Belgium v Spain (Second Phase)* ICJ Rep 1970 3.

*Nigeria*


**United Kingdom**


**United States of America**


*Haag v. United States,* 485 F.3d 1, 3 (1st Circuit) (2007).


Indictment orders


SECONDARY SOURCES

Books


Books Ltd: London.


**Chapters from books**


Journal articles


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


the Freedom of Expression’ 19(3) Cardozo Journal of International and Comparative Law, 647.


Unpublished works

Jamali, MS (2009) Cyber Laundering

Leslie, DA (2010) Anti-Cyberlaundering Regulation and Control
A Masters thesis submitted to the Faculty of Law, University of the Western Cape, in October 2010, in partial fulfillment of the requirement of Masters of Laws in Transnational Criminal Justice and Crime Prevention.

DBA 1727, III Semester Course Material, Masters for Business Administration Degree, Centre for Distance Education, Anna University, Chennai, India. Available at <http://www.scribd.com/doc/40219342/Ethics-Social-and-Political-issues> [accessed on 2 August 2011].


Internet resources

Internet articles


Bloomberg Business Week (2006) ‘Gold Rush: Online payment systems like e-gold ltd are becoming the currency of choice for cyber crooks’ available at <http://www.businessweek.com/magazine/content/06_02/b3966094.htm> [accessed on 1 September 2011].


NUA (an undated website document) ‘Surveys’ available at <http://www.m.nua.org> [accessed on 3 September 2011]


Scrofina, S (2011) ‘If one were to make a competitor for Bitcoin, what would it be?’ available at <http://www.quora.com> [accessed 5 August 2011].


Virgin Cards (an undated internet article) ‘About us’ available at <http://www.virgin.co.uk/pre-paidcards> [accessed on 15 July 2011].


Websites

Bitcoin
Available at <http://www.bitcoin.org> [accessed on 8 August 2011].

British Broadcasting Corporation (BBC)
Available at <http://news.bbc.co.uk/2/hi/8548190.stm>[accessed 24 July 2011].

CyberAngels
Available at <http://www.cyberangels.org/> [accessed on 4 April 2012].

CyberCash
Available at <http://www.cybercash.com> [accessed on 4 August 2011].

Drug Enforcement Administration

Ecash
Available at <http://www.ecash.com/online/> [accessed on 4 August 2011].

Financial Crimes Enforcement Network
Available at <http://www.fincen.gov/about_fincen/wwd/> [accessed on 9 August 2011].

Financial Sector Assessment Program
Available at <http://www.imf.org/about/projects/worldbank> [accessed on 13 August 2010].

Freedom Eagle Card
Available at <http://www.freedom-card.co.uk/> [accessed on 2 September 2010].

Gold and Silver Reserve Inc
Available at <http://www.e-gold.com/unsecure/pgpkey.htm> [accessed on 13 February 2012].

Internet Hotlines Providers
Available at <http://www.inhope.org/gns/home.aspx> [accessed on 4 April 2012].

International Telecommunications Union
Available at <http://www.itu.int/africainternet2000/Documents/doc7_e.htm> [accessed on 13 June 2011].

Internet Watch Foundation
Available at <http://www.iwf.org.uk/> [accessed on 4 April 2012].

Internet World Stats

Interpol
Available at <http://www.interpol.int/Crime-areas/Financial-crime/Payment-cards> [accessed on 11 February 2011].

NetCash
Available at <http://www.netbank.com/~netcash> [accessed on 4 August 2011].

Treaties Office of the Council of Europe
Available at <http://conventions.coe.int/> [accessed on 9 February 2012].
United States Department of Justice
Available at <http://www.justice.gov/criminal/ceos/Press%20Releases/DC%20egold%20indictment.pdf> [accessed on 13 February 2012].

Wolfsberg Group of Banks
Available at <http://www.wolfsberg-principles.com/index.html> [accessed on 6 November 2011].