

**COMBATING CYBER MONEY LAUNDERING: SELECTED
JURISDICTIONAL ISSUES**

**A RESEARCH PAPER SUBMITTED TO THE FACULTY OF LAW OF THE
UNIVERSITY OF THE WESTERN CAPE IN PARTIAL FULFILMENT OF THE
REQUIREMENTS FOR THE DEGREE OF MASTER OF LAWS**




**PREPARED UNDER THE SUPERVISION OF
DR R KOEN**

**AT THE FACULTY OF LAW, UNIVERSITY OF THE WESTERN CAPE
OCTOBER 2010**

TABLE OF CONTENTS	PAGE
CHAPTER 1: PRELIMINARY MATTERS	1
1.1 Introduction	1
1.2 Literature Review	4
1.3 Research Questions	6
1.4 Significance of Research	7
1.5 Research Methodology	7
1.6 Key Words	7
CHAPTER 2: THE CONCEPT OF CYBER MONEY LAUNDERING	8
2.1 Basic Concept of Money Laundering on the Internet	8
2.2 Importance of Prevention	9
2.3 Role of the Internet in Placement, Layering and Integration	12
2.4 Methods of Cyber Money Laundering	16
CHAPTER 3: REVIEW OF LAW AND INTERNATIONAL INSTITUTIONS	20
3.1 Legal Instruments Applicable to Cyber Money Laundering	20
3.1.1 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances	20
3.1.2 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime	21
3.1.3 First, Second and Third Money Laundering Directives of the European Union	23

3.1.4 Council of Europe Convention on Cybercrime	25
3.2 International Institutions Dealing with Cyber Money Laundering	28
3.2.1 The Basel Committee on Banking Supervision and Regulation	28
3.2.2 The Financial Action Task Force (FATF)	29
3.2.3 The Wolfsberg Group	31
3.3 Conclusion	34
CHAPTER 4: JURISDICTION OVER CYBER MONEY LAUNDERING	35
4.1 Introduction	35
4.2 Local and Transnational Cybercrime	35
4.2.1 Location of Acts	38
4.2.1.1 Effects Doctrine	38
4.2.1.2 Ubiquity Theory	39
4.2.2 Location of Victims	40
4.2.3 Nationality of Perpetrator	41
4.3 Investigation and Prosecution of Cyber Money Laundering	41
4.3.1 Investigation	42
4.3.2 Prosecution	44
4.3.3 Substantive Criminal Law	45
4.3.4 Criminal Procedural Law	46
4.3.5 Mutual Legal Assistance	47
4.3.6 Encryption	50



4.4 Confiscation and Forfeiture	51
4.4.1 The Criminalisation of Money Laundering	54
4.4.2 Due Diligence Measures	55
4.4.3 Supervisory Measures	56
4.4.4 Reporting of Suspicious Transactions	57
4.5 Conflicting Jurisdictions	57
4.5.1 Custody of the Perpetrator	60
4.5.2 Damage	61
4.5.3 Nationality of the Perpetrator	62
4.5.4 Strength of the Case	62
4.5.5 Fairness	63
4.6 Conclusion	63
 UNIVERSITY <i>of the</i> WESTERN CAPE	
CHAPTER 5: ALTERNATIVE MEASURES TO COMBAT CYBER MONEY LAUNDERING	65
5.1 Review of Existing Approaches and Ideas	65
5.1.1 The Know Your Customer Regime	65
5.1.2 Customer Due Diligence	66
5.2 A New Approach	68
5.2.1 Undercover Investigations	70
5.2.2 Remote Searches	71

CHAPTER 6: CONCLUSION

73

LIST OF REFERENCES

77



Acknowledgements

Firstly, I would like to thank DAAD, for funding this masters programme and the University of the Western Cape for generously accommodating us.

I would like to extend my thanks to my family and friends who supported me during this research project.

Lastly I would like to extend my appreciation towards my supervisor, Dr R Koen, for his valuable guidance and patience.



DECLARATION

I declare that the research paper '*COMBATING CYBER MONEY LAUNDERING: SELECTED JURISDICTIONAL ISSUES*' is my own work, that it has not been submitted for any degree or examination in any other university, and that all the sources I have used or quoted have been indicated and acknowledged by complete references.

Student..... Date.....

Signed.....

Supervisor..... Date.....

Signed.....



LIST OF ABBREVIATIONS

CDD	Customer Due Diligence
EBF	European Banking Federation
EFT	Electronic Funds Transfer
E-money	Electronic money
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
IP	Internet Protocol
ISP	Internet Service Provider
KYC	Know Your Customer
SAR	Suspicious Activity Report
UNODC	United Nations Office on Drugs and Crime
SWIFT	Society for Worldwide Interbank Financial Telecommunication



CHAPTER 1

PRELIMINARY MATTERS

1.1 Introduction

Money launderers have long taken advantage of the cover offered by operating in multiple jurisdictions.¹ All but the most incompetent criminals know that prosecution and investigation of crimes are more complicated when multiple jurisdictions are involved.² From the perspective of money launderers, the internet offers high degrees of anonymity while allowing for almost instantaneous financial transactions. As a result, money launderers have turned increasingly to the internet as an efficient means of concealing the origin of dirty money. Ideally, a cyber money launderer would use at least one jurisdiction with bank secrecy laws while using loopholes in other legal systems and international co-operation to facilitate his criminal activities. The growing trends towards globalisation and increased international trade make life even easier for cyber money launderers. Financial services have long been global and electronic, allowing transfers of money around the globe from literally anywhere.

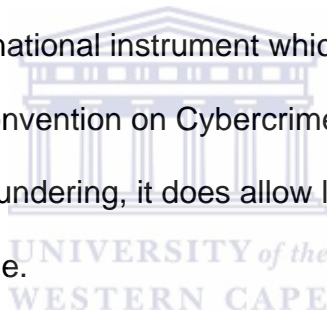
Cyber money laundering is a relatively new concept. Not much research has been done on the topic as compared to other aspects of anti-money laundering law. More specifically, there is no real authority on the issue of jurisdiction over cyber money laundering. Cyber money laundering is essentially money laundering conducted over the internet. It is, therefore, simply a new technique of committing the traditional crime of money laundering. As a result, the internet is a mere tool used by money launderers to launder dirty money in cyberspace.

¹ Evans (1995: 1).

² Evans (1995: 1).

However, cyber money laundering would qualify in some instances as a cybercrime. The fight against cyber money laundering thus requires an examination of both cybercrime and of the existing principles of anti-money laundering initiatives.

Given the scale of money laundering, it is not surprising that there are numerous bodies which are involved in the battle against it. Although most of these bodies initially did not envisage the technical difficulties associated with cyber money laundering, it is safe to assume that their work nevertheless will be useful in combating it. The Convention on Cybercrime of 2001 is indispensable in the fight against cyber money laundering. It was drafted by the Council of Europe but it was intended to be an international instrument which would combat cybercrime effectively.³ Although the Convention on Cybercrime does not deal directly with the issue of cyber money laundering, it does allow law enforcement agencies to pursue it indirectly as a crime.



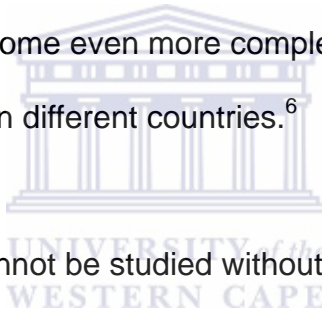
The Financial Action Task Force (FATF) is an inter-governmental body established for the sole purpose of creating anti-laundering strategies based on international co-operation. The FATF was established as early as 1989 and has proved to be invaluable in the fight against money laundering. As combating money laundering is its sole purpose, the FATF has managed to keep abreast of the latest developments in money laundering. Relevant to cyber money laundering is the fact that banks and other financial institutions are advised not to keep anonymous accounts and to verify the existence of their customers.⁴ In addition to this, banks and financial institutions are advised to take reasonable

³ Lovet (2009: 68).

⁴ Jaarsveld (2004: 698).

measures to establish the true identity of their customers.⁵

Jurisdiction over money laundering is determined largely by the internal legislation of a state, in the light of international law and the recommendations of international institutions. Cybercrimes have been studied without specific focus on the issue of cyber money laundering. This holds true especially in respect of jurisdiction over cyber money laundering. The principles governing a sovereign state's right to prohibit certain conduct are well established with regard to conduct in the real, physical world. The same applies to a state's powers to punish those who commit such prohibited conduct. However, cybercrimes tend to complicate these basic principles as they often stretch across the territories of several states. This can become even more complex when criminals route their attacks through computers in different countries.⁶



Cyber money laundering cannot be studied without reference to jurisdiction over cybercrimes. As the internet allows cyber money launderers to take full advantage of multiple jurisdictions, the prosecution of cyber money laundering could give rise to positive jurisdictional conflicts. In other words, more than one state may wish to prosecute the same act of cyber money laundering. The issue of conflicting jurisdictions is a serious one which has yet to be resolved in international law.

It is submitted that the international nature of cyber money laundering can give rise to numerous problems involving confiscation and forfeiture of the proceeds of crime, especially where these proceeds are located in the intangible world of

⁵ Jaarsveld (2004: 698).

⁶ See Brenner (2006: 189).

the internet. The recommendations of the FATF merely set out minimum standards with which member states must comply. These require countries to adopt legislative measures relating to confiscation but do not delve into technicalities which may arise during the physical confiscation process. It merely is required that countries do not interfere with the rights of *bona fide* third parties.

Following the digital trail of cyber money laundering offences always will be a great challenge. This necessitates high degrees of communication between countries and rapid responses in order to preserve digital evidence.

Unfortunately, the framework of treaties and other arrangements which may form the basis for mutual legal assistance is far from ideal.⁷ Mutual legal assistance also may involve high costs and this burden is placed mostly on the party providing such assistance.⁸



1.2 Literature Review

Since cyber money laundering is a relatively new concept, there is no real authority on the issue of jurisdiction over cyber money laundering. Where authors have considered jurisdiction the focus has been on jurisdiction over cyber crimes in general.⁹ Authors tend to build on the content of international conventions, not delving into the complexities of jurisdictional issues relating to the crime of cyber money laundering.

⁷ Grabosky (2007: 217).

⁸ Grabosky (2007: 217).

⁹ See, for example, Brenner & Koops.

Bachus has concluded that cyber money laundering does simplify and accelerate the process of money laundering.¹⁰ However, her research in this field has focused primarily on the financing of terrorism through money laundering, in response to the events which occurred in America on 11 September 2001.

Brenner is probably the most authoritative writer on the issue of jurisdiction over cyber crimes, a topic which is of paramount relevance to the question of jurisdiction of cyber money laundering. With regard to the issue of conflicting jurisdictions, Brenner is of the opinion that in such cases the claims of each state should be prioritised.¹¹ However, the question of how states would go about prioritising conflicting claims over cyber money laundering remains unresolved.¹²

According to Clark, since international law has not yet resolved the issue of prioritising claims, the solution traditionally has been negotiation between states.¹³ For Brenner the response to this is a list of factors which should be taken into consideration when determining jurisdiction over cyber money laundering. He submits that territory remains the main factor for determining whether a sovereign state has jurisdiction over a crime. Often treaties and statutes declare that a state has jurisdiction when the crime has been committed in the territory of a sovereign state.¹⁴ According to Brenner, modern jurisdictional provisions expand these laws to include nationality and conduct which has an effect, or is intended to have an effect, in a sovereign state.¹⁵

¹⁰ Bachus (2004: 835).

¹¹ Brenner (2006: 197).

¹² Brenner (2006: 207).

¹³ Clark (2004: 180).

¹⁴ Brenner (2006: 196).

¹⁵ Brenner (2006: 193).

1.3 Research Questions

Since cyber money laundering entails the use of modern technology, the physical aspects related to the internet and its usage will be researched in the light of the problem of jurisdiction over cyber money laundering. Certain technical and legal aspects involved with internet transactions will be researched. For example, does the location of internet servers have a role in determining jurisdiction over the crime of cyber money laundering and will this have an impact on who has jurisdiction to prosecute the crime of cyber money laundering?

Cyber money laundering renders geographical borders between states more or less irrelevant. Digital money can be transferred literally from one end of the world to the other in an instant. With this it becomes evident that the jurisdictions of several states may be applicable in a single case of cyber money laundering. Although the digital money used in cyber money laundering originated from a specific geographical region (or several), it is clear that it has the potential to affect the interests of a large number of states. How will this affect the rights of states in claiming jurisdiction over the crime of cyber money laundering? More specifically, how would those responsible for combating cyber money laundering approach the problem of states which have conflicting interests in the prosecution of cyber money laundering and the confiscation and forfeiture of its proceeds?

1.4 Significance of the Research

Money laundering is bad for business, development, the economy and the rule of law.¹⁶ As cyber money laundering is a relatively new and advanced form of criminal activity, research into the problematic areas which arise during the investigation, prosecution and determination of jurisdiction over the crime of cyber money laundering is necessary.

By identifying techniques which are used to achieve cyber money laundering and the institutions which are most vulnerable, the research can serve a preventive function and assist in the overall battle against cyber money laundering.

1.5 Research Methodology

This research will be conducted using a desktop approach. Both primary and secondary sources will be used to conduct the research. Accordingly, a range of international treaties, statutes, books, journals, cases and internet sources will be consulted.

1.6 Key Words

Cyber Money Laundering, Internet, Internet Service Providers (ISPs), Digital Money, Financial Action Task Force (FATF), Financial Intelligence Units (FIUs), Placement, Layering, Integration, Customer Due Diligence.

¹⁶ Alweendo (2005: 3) and Bachus (2004: 838).

CHAPTER 2

THE CONCEPT OF CYBER MONEY LAUNDERING

2.1 Basic Concept of Money Laundering on the Internet

Since cyber money laundering essentially consists of money laundering which is conducted over the internet, a brief examination of the concept of money laundering is necessary. Money laundering always will involve the disguising of money, derived from criminal origins, so that said money may appear legitimate. Incorporated into this narrow definition of money laundering is the fact that all money launderers have three objectives in common. They all wish to conceal the origin and ownership of the illegally obtained money, maintain control over it and change its form.¹⁷ These steps are essential in the crime of money laundering, since it is only by these means that a money launderer can launder money successfully.



The concept of cyber money laundering also cannot be explained without reference to the broader concept of cyber crime. Although cyber crime is a relatively new legal phenomenon, it is simply a new method of committing crimes which have been in existence for ages.¹⁸ Unlike the traditional concept of crime, cyber crimes are not physically grounded.¹⁹ However, the term 'cyber crime' itself causes great difficulty for some authors. Thus, 'cyber crimes', 'computer crimes' or even 'IT crimes' could be synonyms or they could refer to different concepts.²⁰

¹⁷ Jaarsveld (2004: 687).

¹⁸ McCusker (2007: 258).

¹⁹ Brenner (2006: 190).

²⁰ McCusker (2007: 258).

It is exactly for this reason that the term 'cyber crime' has been understood to encompass any form of unlawful conduct on the internet.²¹ Since the crime of cyber money laundering would fall easily into this category, it is safe to conclude that cyber money laundering is a subset of cybercrime.

In the past, money laundering was a physical process and required the launderer to transport physically cash which was obtained from illegal sources.²² Due to advancements in technology and the establishment of the internet, this is no longer required. Since they provide better access to information and financial services, the features of the internet make it a perfect tool for the facilitation of money laundering.²³ Such features include the speed and ease of transactions, the relative or total anonymity of the parties and the capacity to traverse multiple jurisdictions in mere seconds.²⁴ Globalisation not only facilitated the international laundering of money, but also allowed for international co-operation and the establishment of transnational bodies to combat money laundering.²⁵

2.2 Importance of Prevention

It has been argued that the efforts against money laundering by anti-money laundering authorities should be terminated.²⁶ Advocates of this idea contend that the stringent policies that these agencies impose on financial institutions undermine the economic well-being of certain countries.²⁷ They argue that the anti-money laundering obligations placed on financial institutions lead to an

²¹ McCusker (2007: 258).

²² Bortner (1996: 1).

²³ Jaarsveld (2004: 691) and Kellerman (2004: 1).

²⁴ Jaarsveld (2004: 692) and Kellerman (2004: 3).

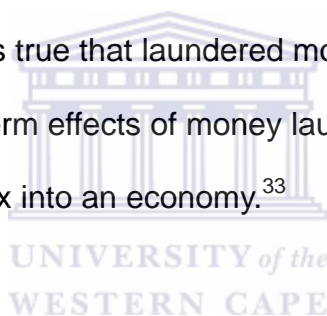
²⁵ Pieth (2002: 8) and Shehu (2000: 2).

²⁶ Stessens (2000: 165) and Rahn (2002: 149).

²⁷ Rahn (2002: 153).

increased administrative burden on these institutions.²⁸ This holds true especially for smaller countries which base their financial sectors on financial secrecy.²⁹

However, this view cannot be sustained. Money laundering has negative implications for national income and output, fiscal policies, exchange rates and the terms of international trade.³⁰ It has been shown that money laundering causes national market-orientated exchange rates to depreciate.³¹ This, in turn, leads to an increase in the price of imports and a decrease in the price of exports. Simply put, the country will find itself in a weaker economic position than it was without money laundering. It has been shown also that criminally-obtained money is used to finance international terrorism and this fact strains international relationships.³² Although it is true that laundered money eventually returns to the country of origin, the long-term effects of money laundering outweigh the short-term benefits of a cash influx into an economy.³³



There are four major consequences of money laundering.³⁴ Firstly, money laundering allows criminals to profit from their criminal activities and creates funding for future criminal activities.³⁵ Removing the financial incentive for criminals to commit such crimes is a key element in the overall fight against crime. In addition, investigating instances of money laundering sometimes may be the only way of retrieving or returning stolen money to victims.³⁶

²⁸ Stessens (2000: 165).

²⁹ Jaarsveld (2004: 688).

³⁰ Bartlett (2002: 1).

³¹ Bartlett (2002: 1) and Jaarsveld (2004: 688).

³² Jaarsveld (2004: 688).

³³ Bachus (2004: 838).

³⁴ Alweendo (2005: 3), Bachus (2004: 838) and Jaarsveld (2004: 688).

³⁵ Bachus (2004: 838) and Jaarsveld (2004: 688).

³⁶ Bachus (2004: 838).

Secondly, money laundering is considered to be bad for business.³⁷ Most financial institutions and businesses rely on their good reputations in order to build future business relationships. In all economies, businesses require a free and competitive market in order to survive. The effects of money laundering undermine such a free and competitive market structure.³⁸

Thirdly, it has been argued that money laundering is bad for the economic growth of developing countries.³⁹ Such countries tend to rely on secrecy to develop a strong financial sector.⁴⁰ However, this secrecy hinders the detection and prosecution of money laundering activities within such countries.⁴¹ This, in turn, leads to social instability and ultimately impedes lawful commercial development.⁴² While illegal funds injected into a developing country may seem to be a fast way for that country to build wealth, in the long run it imposes heavy burdens on the world economy by harming effective economic activity.⁴³ Businesses will be reluctant to invest in countries which are subject to such unstable dealings.⁴⁴

Lastly, money laundering is bad for global and national economies.⁴⁵ Since the globalisation of the world's economy, the wealth of each country affects the well-being of all other countries.⁴⁶

³⁷ Alweendo (2005: 3) and Bachus (2004: 838).

³⁸ Bachus (2004: 839).

³⁹ Bachus (2004: 839) and Jaarsveld (2004: 688).

⁴⁰ Jaarsveld (2004: 688).

⁴¹ Bachus (2004: 840).

⁴² Bachus (2004: 840) and Jaarsveld (2004: 688).

⁴³ Jaarsveld (2004: 688).

⁴⁴ Bachus (2004: 840).

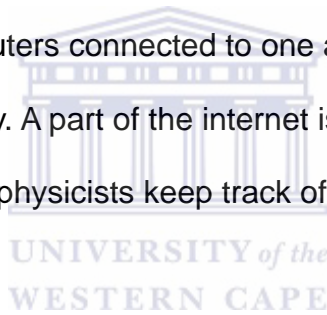
⁴⁵ Bachus (2004: 840).

⁴⁶ Bachus (2004: 840).

Every year enormous amounts of money are spent in the fight against money laundering, which money could have been spent better had money laundering not existed.⁴⁷ Money laundering also promotes distrust in the financial sector, which has a negative impact on the economic growth of a country.⁴⁸

2.3 Role of the Internet in Placement, Layering and Integration

The internet has been described as 'a virtual geography created by computers and networks, and includes invisible and intangible paths constructed through the space continuum'.⁴⁹ The most basic explanation of the internet is that it is comprised of a global network of computers that all speak the same language. A network is a group of computers connected to one another, enabling them to share information accurately. A part of the internet is the World Wide Web, which was created initially to help physicists keep track of data of colleagues in similar fields of expertise.⁵⁰



In the light of modern financial transactions, banks use electronic funds transfers (EFTs) through telecommunication links via bank computers.⁵¹ Banks are connected to one another through a computer messaging system that is operated by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).⁵² As EFTs are of vital importance to a money launderer, it is crucial to distinguish between the concept of digital cash and EFTs.⁵³

⁴⁷ Bachus (2004: 840).

⁴⁸ Jaarsveld (2004: 688).

⁴⁹ Jaarsveld (2004: 694).

⁵⁰ Jaarsveld (2004: 691).

⁵¹ Panurach (1996: 46).

⁵² SWIFT homepage.

⁵³ Jaarsveld (2004: 692).

A typical example of digital cash is stored value cards, such as credit cards or automatic teller machine cards.⁵⁴ Electronic money or digital cash exists outside of ordinary banks, has no physical presence and, as such, can be manipulated through any computer anywhere in the world.⁵⁵ Account holders can gain access to their accounts indirectly from any computer which has internet access, and in such event financial institutions have no way of verifying the true identity of their customers.

EFTs or wire transfers are electronic transactions carried out by an originator through a financial institution with the aim of making money available to a beneficiary.⁵⁶ EFTs are brought about by instructions from the originator.⁵⁷

Sometimes the beneficiary and the originator may be the same person, if such person has numerous accounts and simply transfers money from one account to another.



Regardless of the form it takes, money laundering always involves three stages.⁵⁸ The first stage of money laundering is referred to as the placement stage.⁵⁹ This would involve the placement of money obtained from illegal origins into cyberspace (more commonly known as the internet).⁶⁰ The main advantage of the internet here is the use of Electronic money (E-money), which is digital money that can be exchanged freely over the internet without the use of an intermediary.⁶¹

⁵⁴ Fera (1996: 2).

⁵⁵ Jaarsveld (2004: 693).

⁵⁶ Jaarsveld (2004: 692).

⁵⁷ Jaarsveld (2004: 692).

⁵⁸ Bachus (2004: 842) and Philippsohn (2001: 3).

⁵⁹ Philippsohn (2001: 3).

⁶⁰ Jaarsveld (2004: 695).

⁶¹ Philippsohn (2001: 3).

Intermediaries are sometimes subject to certain reporting requirements pertaining to transactions of a suspicious nature. Thus, the FATF requires, among others, financial institutions to report transactions which they suspect or have reasonable grounds to suspect involve funds that are the proceeds of criminal activities.⁶² When the proceeds of crime are in the form of E-money, they could be used to buy goods or foreign exchange over the internet, to be resold at a later stage. This transaction simultaneously will enjoy a very high degree of anonymity.⁶³ E-money thus could be used to place dirty money without having to conduct face-to-face transactions.

Secondly, in the layering stage, the money launderer undertakes a series of transactions in order to separate the money from its illegal origins.⁶⁴ This process may include the purchase of goods or merely the transfer of money to different accounts. It is submitted that it is during this stage of the money laundering process that the internet could be of most use to money launderers. Since the internet makes it possible for transactions to be done instantaneously, the money launderer can build up quickly an extensive audit trail with relative ease.⁶⁵

Lastly, during the integration stage, the money must be used by the launderer, ensuring that it appears as his own legitimate wealth.⁶⁶ The launderer could use a fictitious online business which allegedly provides services. In return for these services, the company receives payment from money which has passed through the layering process. At the same time, the money which has travelled through

⁶² FATF Recommendation 13.

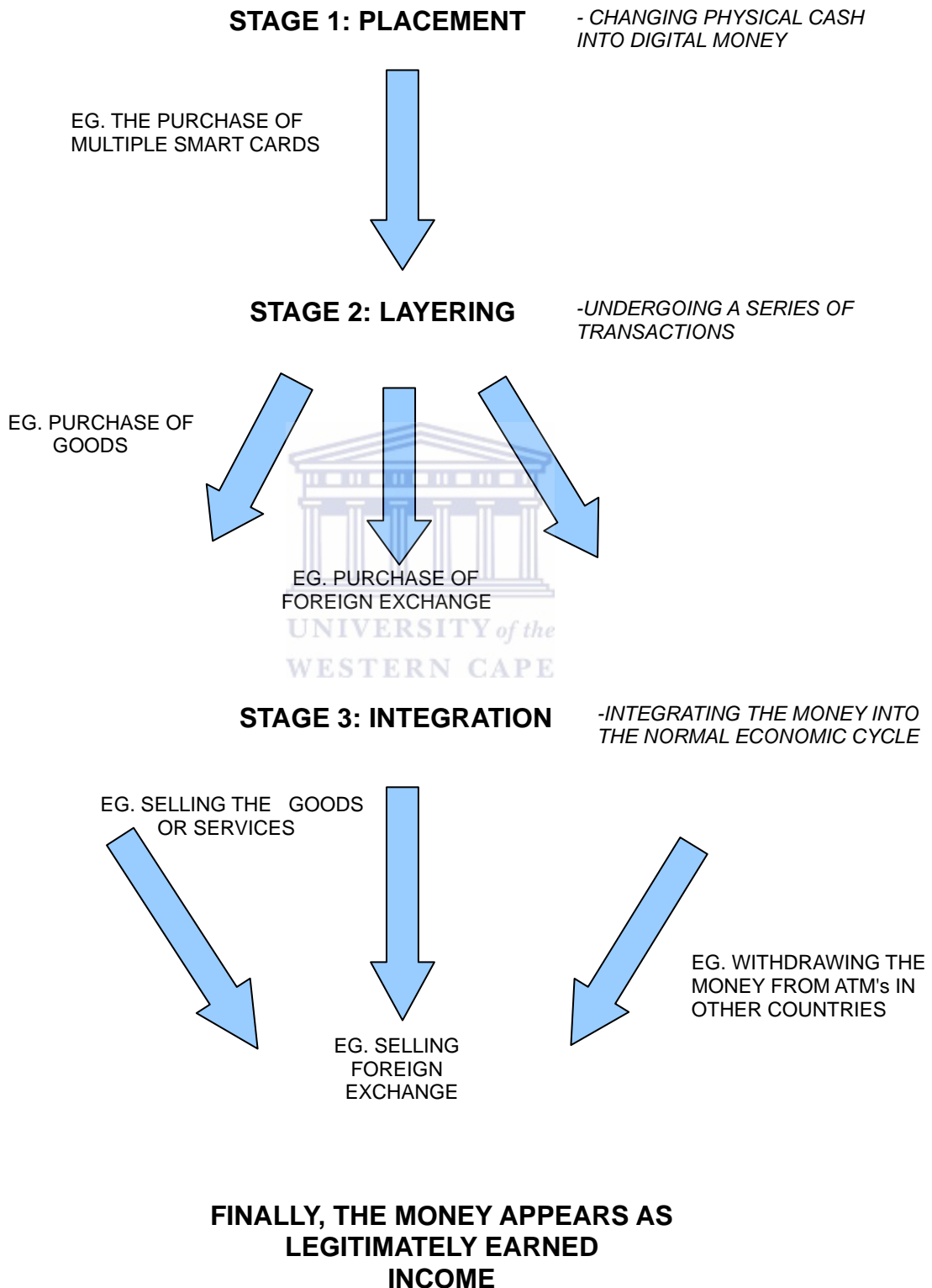
⁶³ Philippssohn (2001: 3).

⁶⁴ Bachus (2004: 844).

⁶⁵ Philippssohn (2001: 3).

⁶⁶ Bachus (2004: 844).

the layering process may be in the name of a fictitious person, even further hindering the prosecution of the crime. Effectively, the wealth of the owner of the company would appear to be legitimate income of the company.⁶⁷ This process is illustrated well by the following diagram, adapted from Phillipsohn:⁶⁸



⁶⁷ Phillipsohn (2001: 4).

⁶⁸ Phillipsohn (2001: 4).

2.4 Methods of Cyber Money Laundering

As may be expected, there are numerous methods through which the crime of cyber money laundering could be committed. They range from the mere misuse of online banks and casinos to more complicated criminal techniques which take advantage of jurisdictional differences among countries. Generally, the methods of the crime are categorised under direct or indirect acts of cyber money laundering.

Cyber money laundering is direct when an individual directly deals with a financial institution while simultaneously hiding his true intentions.⁶⁹ The following is a list of methods through which direct cyber money laundering could be achieved over the internet:

1. Concealment within business structures;
2. Misuse of legitimate businesses;
3. Use of false identities, documents and 'smurfs';
4. Exploitation of international jurisdictional issues; and
5. Use of anonymous asset types.⁷⁰

However, cyber money laundering can be committed indirectly also. This form of cyber money laundering is achieved by avoiding direct dealings with financial institutions.⁷¹ The Hawala system has been a traditional method of facilitating the transfer of funds between Europe and South Asia. In this system, funds are simply moved between those launderers who distribute them at one end of the cycle and those who collect them at the other end.⁷²

⁶⁹ The Egmont Group (1999: 88).

⁷⁰ The Egmont Group (1999: 88).

⁷¹ The Egmont Group (1999: 88).

⁷² Jaarsveld (2004: 693).

In its most basic form, Hawala has been described as ‘money transfer without money movement’.⁷³ However, the Hawala system operates on a strong tradition of reliance and trust between parties, which makes it almost impossible to penetrate.⁷⁴ The participants are also notorious for their lack of record keeping and where records are kept, they are probably encoded.⁷⁵ With the Hawala system, funds are moved between countries in an informal manner.

Upon a customer request, a Hawala operator in one country simply would e-mail his hawaladar associate in another country with the specifics of the transaction. As no names are used in Hawala transactions, correspondence would consist merely of a specified amount with a corresponding password. Once the hawaladar associate receives the password from a recipient, he simply would pay the specified amount out of his own funds in local currency.⁷⁶

By using the Hawala system, a cyber money launderer would avoid possible reporting (of certain transactions) by financial institutions to financial agencies. In fact, it has been shown that these money or value transfer services have been subjected to abuse by cyber money launderers.⁷⁷ These services facilitate anonymous funds transfers and as a result few or no records are kept.⁷⁸ These services are commonly referred to as underground banking systems, of which Hawala is the classic example.⁷⁹

⁷³ Bowers (2009: 379).

⁷⁴ Jaarsveld (2004: 693).

⁷⁵ Jaarsveld (2004: 693).

⁷⁶ Bowers (2009: 379).

⁷⁷ FATF (2003: 2).

⁷⁸ Bowers (2009: 379).

⁷⁹ Jaarsveld (2004: 693).

Indirect cyber money laundering could be achieved using the following methods:

1. E-Cash;
2. Online Auctions;
3. Bankruptcy Frauds;
4. Cyber Terrorism;
5. Online Banking and Fraudulent Credit Cards;
6. E-gold; and
7. Online Casinos.⁸⁰

While online banking has become more attractive to everyday consumers because of the convenience it offers, unfortunately it also has become an attractive avenue for cyber criminals wishing to launder money. Online banks are thus extremely vulnerable institutions in the context of cyber money laundering. The low identification and reporting requirements of some online banks serve only to make them more susceptible to being used in the cyber money laundering process. Online banks also have to deal with a higher number of transactions than ordinary banks.⁸¹ As a result, it becomes much more difficult for online banks to identify suspicious transactions. Cyber money launderers are capable of using multiple individuals and accounts in order to create extensive trails aimed at hindering investigation of their activities. This process is referred to often as 'smurfing'.

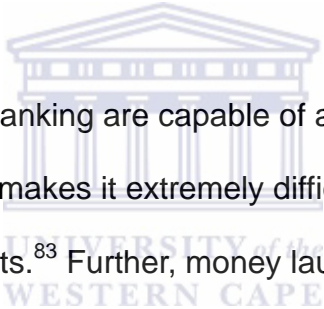
During the layering phase of money laundering, the money undergoes a series of transactions in order to separate it from its illegal origins.⁸² Essentially, the purpose of layering is to ensure that authorities are incapable of identifying the

⁸⁰ Kochan (2006: 112).

⁸¹ Philippsohn (2001: 3).

⁸² Philippsohn (2001: 3).

fact that the money originated from illegal sources. One of the ways of achieving this is through the use of 'smurfs'. These 'smurfs' are individuals used by the cyber money launderer to facilitate the layering phase of the laundering process. In exchange for a small fee, these individuals each will conduct certain transactions over the internet upon the instructions of the cyber money launderer. In this way, the cyber money launderer can complicate further the investigation of his illegal activities. By using 'smurfs', the cyber money launderer also can avoid certain reporting requirements of financial and other institutions. It is obvious that a single large transaction by one individual is much more likely to be reported as suspicious than multiple small transactions by seemingly independent individuals.



Individuals who use online banking are capable of accessing their accounts from anywhere in the world. This makes it extremely difficult for online banks to verify the true identity of their clients.⁸³ Further, money launderers are capable of using highly complicated encryption technology to block out law enforcement agencies.⁸⁴ Without the specific key to unlock such encryption, the information becomes useless to these agencies.

Unfortunately, the means through which cyber criminals can misuse the internet to launder money are almost endless. Where money does not move, as with the Hawala system, there are no suspicious transaction reporting requirements.⁸⁵

⁸³ Jaarsveld (2004: 693).

⁸⁴ Philippsohn (2001: 1).

⁸⁵ Jaarsveld (2004: 694).

CHAPTER 3

REVIEW OF LAW AND INTERNATIONAL INSTITUTIONS

3.1 Legal Instruments Applicable to Cyber Money Laundering

While there are numerous bodies addressing the issue of money laundering, none of them addresses the issue of cyber money laundering directly. The same applies to the initiatives directed at combating cybercrime. As a result, there is a need for law enforcement agencies to utilise the existing initiatives aimed at combating both money laundering and cybercrime in order effectively to combat cyber money laundering.

3.1.1 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances

The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention) of 19 December 1988 was the first of its kind to acknowledge the problem of money laundering.⁸⁶ It became effective in November 1990 and by 1992 fifty-nine states had ratified the Convention.⁸⁷ Although the term ‘money laundering’ is not used explicitly in the Vienna Convention, Article 3 identifies the constituent elements of money laundering, which have formed the basis for all subsequent legislation.⁸⁸ Article 3(1)(b)(ii) states the following:

Each Party shall adopt such measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally: ... The concealment or disguise of the true nature, source ... with respect to, or ownership of property, knowing that such property is derived from an offence or offences established in accordance with subparagraph (a) of this paragraph.

⁸⁶ Jaarsveld (2004: 696).

⁸⁷ Poremská (2009: 389).

⁸⁸ Leong (2007: 150).

Article 3(1)(a) refers to a series of offences which are all related to various aspects of possession, production and illicit traffic in narcotic drugs and psychotropic substances.⁸⁹ Although confined to drug trafficking, the Vienna Convention obliges states to classify money laundering as a criminal offence and requires parties to facilitate the identification, tracing and forfeiture of narcotics and laundered money.⁹⁰

Article 4 of the Vienna Convention establishes jurisdiction for money laundering offences committed in the territory of a state party by one of its nationals, or offences committed outside its territory but which have an effect within its territory.

While the Vienna Convention contributed extensively to the international fight against narcotics-related money laundering, it remains unclear how effective it would be in combating cyber money laundering.⁹¹ However, at least the Convention contains mandatory provisions relating to jurisdiction, confiscation, extradition and mutual legal assistance, which provisions would undeniably assist countries in the prosecution of narcotics-related cyber money laundering.⁹²

3.1.2 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime

Unlike the Vienna Convention, the Council of Europe Convention on Laundering,

⁸⁹ Article 3(1)(a)(i)-(v) of the Vienna Convention.

⁹⁰ Poremská (2009: 389) and article 5 of the Vienna Convention.

⁹¹ Gilmore (1999: 53).

⁹² Articles 3, 4, 5 & 6 of the Vienna Convention.

Search, Seizure and Confiscation of the Proceeds of Crime is not confined to drug trafficking. Its provisions extend to all crimes.⁹³

The crime of cyber money laundering can be inferred from Article 6 of the Convention which reads:

Each Party shall adopt such legislative and other measures as may be necessary to establish as offences under its domestic law, when committed intentionally:

- (a) the conversion or transfer of property, knowing that such property is proceeds, 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 the predicate offence to evade the legal consequences of his actions;
- (b) 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 proceeds; and, subject to its constitutional principles and the basic concepts of its legal system.

As cyber money laundering inevitably would entail the concealment of the origin of money obtained by illegal means, the provisions of the Council of Europe Convention on Laundering could be used in the fight against cyber money laundering. Even though it can be stated comfortably that the drafters of the Convention could not have taken into account the possibility of cyber money laundering, it remains clear from the provisions of Article 6 that the Convention would be applicable to the crime.

Interestingly, the Council of Europe Convention on Laundering does not require that the predicate offence of money laundering be subject to the criminal jurisdiction of a state party wishing to implement the Convention's provisions.⁹⁴

⁹³ Leong (2007: 146).

⁹⁴ Article 6(2)(a) of the Council of Europe Convention.

3.1.3 First, Second and Third Money Laundering Directives of the European Union

The European Union Directive on the prevention of the use of the financial system for the purpose of money laundering (First Money Laundering Directive) was implemented on 10 June 1991.⁹⁵ It was based on the 40 recommendations of the FATF and required financial institutions to establish certain identification, record-keeping and due diligence measures.⁹⁶

In addition to this, it obliged financial institutions to report on any suspicious transactions.⁹⁷ Interestingly, Article 8 prohibits the disclosure to a customer that an investigation of money laundering is being carried out against him. In the case of cyber money laundering, this would be an essential tool in the prosecution of the crime. As money launderers in general construct elaborate schemes to evade detection by law enforcement agencies, they would go to even greater lengths in order to avoid prosecution if they know they are being investigated. Here, cyber money launderers are in a unique position due to the vulnerabilities involved in digital evidence.⁹⁸

In 2001 an amendment was made to the First Money Laundering Directive and the Second Money Laundering Directive was adopted by the European Parliament and the European Union.⁹⁹ The provisions of the Second Directive

⁹⁵ Directive 91/308/EEC.

⁹⁶ Articles 3, 4, 5 of the first Money Laundering Directive and Leong (2007: 147).

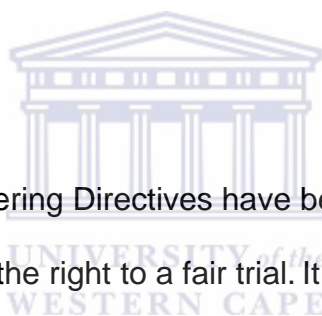
⁹⁷ Article 7 of the First Money Laundering Directive.

⁹⁸ See Chapter 4.

⁹⁹ Directive 2001/97/EC.

have a wider scope and extended the anti-money laundering principles to lawyers, accountants, auditors, notaries, casinos and estate agents.¹⁰⁰ They also provided for the establishment in all member states of Financial Intelligence Units (FIUs) to which suspicious transactions would be reported.¹⁰¹

The Third Money Laundering Directive was adopted in 2005 and is intended to bring the First and Second Money Laundering Directive in line with the FATF revised 40 Recommendations of June 2003. It also extends the provisions of the directives to any financial transaction which may be linked to the financing of terrorism.¹⁰²



However, the Money Laundering Directives have been challenged on the basis that they may interfere with the right to a fair trial. It is argued that the reporting requirements of the Directives could interfere materially with a lawyer's ability to represent a client fully and independently.¹⁰³ In addition, without a report on the effectiveness of the Directives, it is unclear whether they actually are fulfilling their purpose or whether they simply are placing a money-wasting burden on businesses and customers. Unfortunately, the Directives do not contain any specific reference to jurisdiction of money laundering offences.

¹⁰⁰ Article 1 of the Second Money Laundering Directive and Leong (2007: 147).

¹⁰¹ Leong (2007: 147).

¹⁰² Leong (2007: 151).

¹⁰³ Katz (2007: 208).

3.1.4 Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime is indispensable in the fight against cyber money laundering. The Convention was the result of the work of a panel of experts who had to deal with cybercrime, after it was found by the European Committee on Crime Problems that cybercrimes are committed against the:

integrity, availability and confidentiality of computer systems and telecommunication networks or they consist of the use of such networks or their services to commit traditional offences.¹⁰⁴

Although the Convention on Cybercrime does not mention money laundering directly as a cybercrime, it does indirectly allow authorities to pursue it as crime.¹⁰⁵ As cyber money laundering is conducted over the internet, this makes sense.



The Convention on Cybercrime aims at creating an effective legal framework which is based on harmonisation of legal frameworks between member states and the provision of laws and procedures for the effective prosecution of cybercrimes.¹⁰⁶

Article 1 of the Convention defines a computer system as:

any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

Article 2 of the Convention requires states parties to:

adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law ... the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

¹⁰⁴ The European Convention on Cybercrime Explanatory Report No. 9.

¹⁰⁵ Jaarsveld (2004: 696).

¹⁰⁶ Lovet (2009: 68).

The use of the words 'or other dishonest intent' makes it clear that this Convention could be applicable indirectly to the act of cyber money laundering. In addition to this, the Convention deals with illegal access to and interception of computer systems and the misuse of devices in the performance of criminal activities.¹⁰⁷

The procedural methods established by the Convention on Cybercrime are also of significance to cyber money laundering. The Convention requires states parties to adopt legislative and other measures which would enable them to procure information from individuals and service providers within their territory who are suspected of committing a cybercrime.¹⁰⁸ However, this authority is subject to certain limitations to ensure the fair administration of justice.¹⁰⁹

In the fight against cybercrime much emphasis is placed on international co-operation. Accordingly, the Convention on Cybercrime devotes an entire chapter to this.¹¹⁰ More specifically, its provisions cover general principles relating to international co-operation and extradition, as well as general principles of mutual legal assistance and procedures pertaining to mutual legal assistance.¹¹¹ The Convention also deals with mutual legal assistance in specific cases relating to access to stored computer data, the collection of real-time traffic data (such as the internet) and the interception of content data.¹¹²

¹⁰⁷ Articles 3-13 of the Convention on Cybercrime.

¹⁰⁸ Article 18 of the Convention on Cybercrime.

¹⁰⁹ Articles 14 & 15 of the Convention on Cybercrime.

¹¹⁰ Chapter 3 of the Convention on Cybercrime.

¹¹¹ Articles 23-27 of the Convention on Cybercrime.

¹¹² Articles 31, 33 & 34 of the Convention on Cybercrime.

Archick argues that the Convention does take a significant step forward in addressing cybercrime as it forces member states to prosecute computer-related crimes vigorously. By mandating sanctions and making it possible to extradite perpetrators, the Convention enhances deterrence and reduces the number of safe havens for criminals. In addition to this, the provisions relating to the collection of evidence will assist law enforcement agencies in the fight against terrorism.¹¹³

However, Lewis argues that the Convention is critically unbalanced, allowing for sweeping powers of computer search and seizure without corresponding protection of privacy rights. Giving too many powers to investigating authorities could lead to an infringement of the right of free expression on the internet. The costs associated with data-preservation requirements could hinder business and the Convention could force businesses to reshape themselves in favour of law enforcement agencies.¹¹⁴



Archick thinks that the Convention requires more member states in order to be effective. After all, the states which are members of the Convention are not the problem. Cyber criminals would simply route their attacks through countries which are not members of the Convention, for example, North Korea.¹¹⁵ He notes also that the Convention does not allow police authorities direct cross-border access to computer data, which creates an unnecessary time-wasting step.¹¹⁶ Also, he is concerned that the Convention lacks a dual criminality provision, making it possible for one country to request another country to investigate a

¹¹³ Archick (2006: 3).

¹¹⁴ Lewis (2004: 2).

¹¹⁵ Archick (2006: 3).

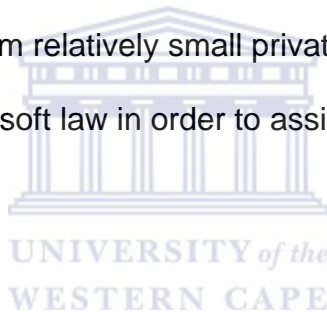
¹¹⁶ Archick (2006: 4).

matter without it being a crime under the latter's domestic law.¹¹⁷

Although the Convention was drafted in 2001, its provisions still seem applicable today. However, given the rapid growth of cybercrime and the excellent profitability it offers to a criminal, the Convention still faces major obstacles. Due to the numerous provisions which have to be incorporated into a state party's domestic legal system, the process of ratification takes a long time.¹¹⁸

3.2 International Institutions Dealing with Cyber Money Laundering

There are various international institutions involved in the fight against money laundering. These range from relatively small private institutions to larger public initiatives aimed at creating soft law in order to assist countries in combating money laundering.



3.2.1 The Basel Committee on Banking Supervision and Regulation

The Basel Committee is an institution which was established in 1974 by the central bank governors of a group of ten nations. It formulates broad supervisory standards and guidelines of best practice in banking supervision, in the hope that other nations will take steps to implement them in their national systems.¹¹⁹ Its primary purpose is to encourage common approaches and standards within banking supervision.¹²⁰ As one author has noted:

the Basel Committee on Banking Supervision is not a classical multilateral organisation. It has no founding treaty, and it does not issue binding regulations. Rather, its main function is to act as an informal forum to find policy solutions and to promulgate standards.¹²¹

¹¹⁷ Archick (2006: 4).

¹¹⁸ Lovet (2009: 69).

¹¹⁹ Leong (2007: 153).

¹²⁰ Leong (2007: 153).

¹²¹ Kerwer (2005: 619).

In December 1988, the Basel Committee adopted the Statement of Principles concerning money laundering. Although the Statement was not enforceable, the participating states decided to follow the principles in accordance with their national legal regulations. The Statement of Principles makes efforts to identify customers and to refuse business with customers who fail to provide adequate identification. In addition, it urges banks to co-operate with law enforcement authorities.¹²² Similar to the Wolfsberg Group, the Basel Committee emphasises the importance of enhanced information sharing.¹²³

3.2.2 The Financial Action Task Force (FATF)

The FATF is an inter-governmental body established for the sole purpose of creating anti-laundering strategies based on international co-operation. It was established as early as 1989 and has proved to be invaluable in the fight against money laundering. As combating money laundering is its sole purpose, the FATF has managed to keep abreast of the latest developments in money laundering.¹²⁴ It has formulated 40 Recommendations and 9 Special Recommendations (on terrorist financing), all aimed at combating money laundering.

Relevant to cyber money laundering is the fact that banks and other financial institutions are advised not to keep anonymous accounts and to verify the existence of their customers. In addition, banks and financial institutions are advised to take reasonable measures to establish the true identity of their

¹²² Poremská (2009: 389).

¹²³ Leong (2007: 153).

¹²⁴ Jaarsveld (2004: 697).

customers.¹²⁵ While Recommendations 6 and 7 of the 9 Special Recommendations on terrorist financing make no specific reference to cyber money laundering, they are directly applicable to the crime.¹²⁶

Special Recommendation 6 deals with the issue of 'Alternative Remittance' or, as explored in Chapter 2 above, the underground banking systems. Here the FATF requires member states to take measures against any persons (including legal persons) who provide a service for the transmission of money or value.¹²⁷

Regardless of whether such service is provided formally or informally, the service providers should be licensed, registered and subject to all FATF requirements which apply to banks and non-banking institutions.¹²⁸ Lastly, if such service providers carry out this service illegally, countries should ensure that they are subject to administrative, civil or criminal sanctions.¹²⁹ From this it is clear that the FATF realised the possibility of cyber money laundering occurring through, for example, the Hawala system.

Special Recommendation 7 deals with the issue of wire transfers. The previous chapter demonstrated how easily wire transfers (basically, electronic funds transfers) could be used to facilitate cyber money laundering. As a result, the FATF obligates countries to take measures to require financial institutions to include accurate and meaningful originator information on funds transfers. In addition, these financial institutions must be required by their respective countries to conduct enhanced scrutiny of funds transfers which do not contain

¹²⁵ Jaarsveld (2004: 698).

¹²⁶ Jaarsveld (2004: 698).

¹²⁷ FATF Special Recommendation 6.

¹²⁸ FATF Special Recommendation 6.

¹²⁹ FATF Special Recommendation 6.

complete originator information. This information must include the name, address and account number of the originator.¹³⁰ This recommendation was included primarily to preclude criminals from having free access to wire transfers.¹³¹

3.2.3 The Wolfsberg Group

The Wolfsberg Group is an association of global banks which aims to develop financial services industry standards.¹³² Most of the existing initiatives in the fight against money laundering have been led by the public sector. However, the Wolfsberg Principles have been developed by the private sector. In 2000, eleven banks signed a set of principles known as the Wolfsberg Anti-Money Laundering Principles. These principles are a non-binding set of best practice guidelines regarding the maintenance of relationships between private bankers and their clients.¹³³ More specifically, they focus on Know Your Customer (KYC), anti-money laundering and counter-terrorist financing policies.¹³⁴

The Group came together in 2000, in the company of representatives of Transparency International, to work on drafting anti-money laundering guidelines for private banking. These principles were published in October 2000 and were then revised in 2002. In November 2002, the Group published the Wolfsberg Anti-Money Laundering Principles for Correspondent Banking.¹³⁵ Then, in 2004 the Group focused on the development of a due diligence model for financial

¹³⁰ FATF Special Recommendation 7.

¹³¹ Jaarsveld (2004: 698).

¹³² Aiolfi (2006: 4).

¹³³ Hinterseer (2001: 25).

¹³⁴ Aiolfi (2006: 4).

¹³⁵ Aiolfi (2006: 4).

institutions. Through globalisation, financial markets have become more international and integrated in operation.¹³⁶ Because money laundering takes advantage of possible weaknesses in the regulation of financial services, it necessitates a comprehensive and flexible approach.

Attempts to solve this problem have seen much of the regulatory burden being passed on to banks themselves to regulate possible money laundering by their clients.¹³⁷ The Wolfsberg Principles represent the collective initiatives of several prominent participants in financial markets and have the potential to become a set of industry standards for banks.¹³⁸ It is worth noting that of the eleven banks that participated in formulating the Wolfsberg Principles, most have been associated with a money laundering scandal in one way or another.¹³⁹

As with most of the other initiatives aimed at fighting money laundering, the Wolfsberg Principles do not make reference specifically to cyber money laundering. However, it must be remembered that cyber money laundering is a relatively new concept and is (at most) a different technique to achieve the traditional goals of money laundering. As a result, the Wolfsberg Principles remain a viable tool that can be used by private banks to prevent money laundering in general. After all, the primary purpose of the Wolfsberg Principles is to ensure that the services offered by the banks and their international dealings are not abused for criminal purposes. Further, this can be achieved only by accepting clients whose wealth can be reasonably established as

¹³⁶ Hinterseer (2001: 25).

¹³⁷ Hinterseer (2001: 25).

¹³⁸ Aiolfi (2006: 4).

¹³⁹ Hinterseer (2001: 26).

legitimate.¹⁴⁰

The Wolfsberg Principles correspond to a great extent with the Recommendations of the FATF and their KYC and customer due diligence (CDD) initiatives. The Principles cater specifically for private banking and include extensive guidelines for banks to follow in the identification of clients and the requirements of the CDD process.¹⁴¹

In addition, the Principles cover situations that require further due diligence and attention, practices that are associated with identifying suspicious transactions, monitoring programmes, educational measures, and the establishment of an anti-money laundering organisation within each bank.¹⁴²

Primarily the Wolfsberg Principles attempt to convince national and international agencies to adopt a risk-based approach to anti-money laundering law. In the words of Pieth:

Whereas the traditional rule-based approach was rather ineffective, because it asked banks to take specific measures depending on set thresholds or predefined criteria, the risk-based approach is more flexible, it identifies risk variables ... but leaves it up to the institution to set its own priorities for each criterion.¹⁴³

According to this approach, each institution is required to develop its own compliance system which allows for a greater margin of flexibility.¹⁴⁴

The challenges confronted by authorities in financial markets increase with the growth and liberalisation of banks.¹⁴⁵ This problem is exaggerated by the speed

¹⁴⁰ Hinterseer (2001: 26).

¹⁴¹ Pieth (2007: 97).

¹⁴² Pieth (2007: 97).

¹⁴³ Pieth (2007: 97).

¹⁴⁴ Pieth (2007: 97).

¹⁴⁵ Hinterseer (2001: 39).

and large geographic scope of cyber money laundering. The simple fact that banks have increased substantially their international activities in the last decade necessitates the actions taken by international bodies to prevent money laundering. If these actions against money laundering in general are not taken, there would be no platform for regulators to build their initiatives against cyber money laundering. In this regard, the Wolfsberg Principles would be invaluable in the fight against cyber money laundering. At the very least, this would hold true for the banking sector which, arguably, would feature large in cyber money laundering activities.

3.3 Conclusion

The international community has acted on many fronts in its response to money laundering and emphasis has been placed on promoting international co-operation and the establishment of an effective international anti-money laundering regime.¹⁴⁶ However, the various obligations placed on countries to fight money laundering still vary according to their degree of adherence to the relevant anti-money laundering instruments.¹⁴⁷ This creates severe problems for the prosecution of cyber money laundering as the crime is mostly transnational in nature. For this reason, it is crucial for countries to present a unified front in order effectively to combat cyber money laundering.

¹⁴⁶ Moshi (2007: 3).

¹⁴⁷ Moshi (2007: 3).

CHAPTER 4

JURISDICTION OVER CYBER MONEY LAUNDERING

4.1 Introduction

Jurisdiction is defined in the Oxford Dictionary of Law as ‘the power of a court to hear and decide a case or make a certain order or the territorial limits within which the jurisdiction of a court may be exercised’.¹⁴⁸ Broadly speaking, the concept of jurisdiction encompasses three elements. It entails a state’s right to prescribe certain laws to its citizens or in the interest of its citizens, to adjudicate or decide whether such laws have been violated, and to enforce compliance or punish non-compliance with those laws.¹⁴⁹



4.2 Local and Transnational Cybercrime

When determining how existing principles of jurisdiction could be applied to cyber money laundering, one must differentiate between two types of cybercrime: local cybercrime and transnational cybercrime.¹⁵⁰

Local cybercrime occurs entirely within the geographical area of one sovereign state and does not necessarily entail jurisdictional difficulties.¹⁵¹ In the case of local cybercrime, a money launderer would use the internet to facilitate the placement, layering or integration phases of money laundering, but the entire process occurs within the jurisdiction of one state.¹⁵²

¹⁴⁸ Oxford Dictionary of Law (2006: 298).

¹⁴⁹ Brenner (2006: 191).

¹⁵⁰ Brenner (2006: 193).

¹⁵¹ Shams (2004: 93).

¹⁵² Brenner (2006: 193).

Use of the internet means that signals invariably would be transmitted into and out of the sovereign state's jurisdiction. However, this would be merely incidental to the crime and would not affect materially the prosecution thereof.¹⁵³ As a result, regulatory authorities effectively would be able to use existing anti-money laundering legislation to prosecute the crime of cyber money laundering. The mere fact that a cyber money launderer uses the internet in the process of laundering money would not preclude the application of traditional jurisdictional principles.¹⁵⁴

Transnational cybercrime occurs across several states and, as a result, the elements of the crime are scattered among different jurisdictions.¹⁵⁵ This complicates both the investigation and the prosecution of the crime.¹⁵⁶ After all, this is one of the reasons why cyber money launderers find the internet useful during the money laundering process. A state would be able to claim jurisdiction either because a part of the crime was committed within territory of the state or because the effects of the crime were felt within that state. Here the problem is to identify whether the crime actually was committed within the state or whether the effects of the crime were felt there. As technology has advanced, cyber money launderers are able to encrypt their transmissions of data over the internet so that their actions are virtually untraceable. However, a detailed explanation of the intricacies of modern technology and how it can be abused for criminal purposes goes beyond the scope of this paper.

¹⁵³ Brenner (2006: 193).

¹⁵⁴ Brenner (2006: 194).

¹⁵⁵ Shams (2004: 93).

¹⁵⁶ Brenner (2006: 194).

Traditionally, jurisdiction is based on the concept of territory.¹⁵⁷ However, modern statutes and treaties expand on this and include principles of nationality and effect.¹⁵⁸ According to the territoriality principle, states can assert jurisdiction over conduct occurring within their territorial boundaries. While the vast majority of criminals commit their crimes within the territory of one sovereign state, the same cannot be said of cyber money laundering. Apart from the territoriality principle, states can assert jurisdiction also according to the nationality principle. According to this principle, states can assert jurisdiction over their citizens as perpetrators, regardless of where the alleged offence occurred. States may also assert their jurisdiction over perpetrators within their territorial borders under the effects principle if criminal behaviour affects a national interest.¹⁵⁹

As previously emphasised, cyber money laundering increases geographic mobility and the use of telecommunications undermines the traditional models of jurisdiction. It also becomes possible for a perpetrator to commit a crime within another country without physically leaving his own.¹⁶⁰ Jurisdiction is, therefore, no longer determined solely according to the requirement that the perpetrator be physically present within a country at the time the offence was committed.¹⁶¹

Under the modern conception of jurisdiction, a country has jurisdiction to prescribe its laws with regard to any of the following: conduct which, wholly or substantially, takes place within its territory; the status of persons, or interests in things, present within its territory; conduct outside its territory which has or is intended to have a substantial effect within its territory; and the activities of its

¹⁵⁷ Brenner (2006: 191).

¹⁵⁸ Grabosky (2006: 215).

¹⁵⁹ Grabosky (2006: 215).

¹⁶⁰ Brenner (2004: 6).

¹⁶¹ Brenner (2004: 8).

nationals outside (as well as within) its territory.¹⁶²

4.2.1 Location of Acts

Article 22(1) of the Convention on Cybercrime uses the territoriality principle as the primary factor constituting jurisdiction. It reads as follows:

Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

- a in its territory; or
- b on board a ship flying the flag of that Party; or
- c on board an aircraft registered under the laws of that Party; or
- d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

However, using the territoriality principle to justify jurisdiction over a crime is not a simple undertaking when the crime is committed over the internet.¹⁶³ This fact is complicated further by different approaches taken when countries determine jurisdiction over cybercrimes. Thus, courts likely will use various modes to determine whether they have jurisdiction or not. As one source has noted:

One of the issues, therefore, that requires further study is to survey the factors courts will use to determine the location of the act of a cybercrime.¹⁶⁴

4.2.1.1 Effects Doctrine

It is common for states to exercise jurisdiction over conduct which occurred outside their territorial bounds but which has a harmful effect, or is intended to have a harmful effect, within their territory.¹⁶⁵ According to the effects doctrine, states can claim jurisdiction even where the effect of a crime is not a constituent

¹⁶² Brenner (2004: 8).

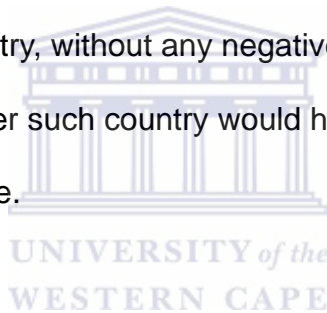
¹⁶³ Brenner (2004: 10).

¹⁶⁴ Brenner (2004: 16).

¹⁶⁵ Brenner (2004: 19).

element of the crime.¹⁶⁶ While the doctrine is accepted widely in the USA, it is criticised severely in Europe.¹⁶⁷

Be that as it may, the doctrine remains a prime ground upon which states can found their jurisdiction over a crime of cyber money laundering. However, countries will experience difficulties in proving whether an act of cyber money laundering had a material effect on them. This will be the case, for example, when an act of cyber money laundering was routed through a country because of low supervision requirements in that particular country. International law requires a sufficiently close connection with an offence before a state may claim jurisdiction over such offence.¹⁶⁸ Where cyber money launderers simply route their attacks through a country, without any negative impact on that particular country, it is doubtful whether such country would have sufficient grounds on which to prosecute the crime.



4.2.1.2 Ubiquity Theory

According to this theory:

an offence is deemed to have taken place on the territory of a state as soon as a constituent or essential element of this offence has taken place on that territory.¹⁶⁹

While this theory is popular in the USA and has been adopted informally into English law, it is more stringent than the effects doctrine as a state can claim jurisdiction only if the effect of the offence constituted an essential element of the crime. However, money laundering has been described as a conduct offence,

¹⁶⁶ Stessens (2000: 221).

¹⁶⁷ Stessens (2000: 221).

¹⁶⁸ Stessens (2000: 221).

¹⁶⁹ Stessens (2000: 218).

and as such, the effects of money laundering cannot be said to be an essential element of the crime.¹⁷⁰ Regardless of this, it is still argued that states will be able to claim jurisdiction under the ubiquity theory due to the broad scope of most money laundering incriminations. Stessens has noted the following in this regard:

Whenever one transaction takes place on the territory of a state, even if the broader money laundering scheme is located abroad, that state will be able to try the money laundering offence. Whereas in some jurisdictions, courts tend to amalgamate all money laundering offences constituting one money laundering scheme (e.g. in Belgium), in other jurisdictions courts will allow separate indictments of every money laundering act (e.g. in United States). In both instances, courts will have jurisdiction, whenever one money laundering act took place on their territory.¹⁷¹

4.2.2 Location of Victims

Jurisdiction can be determined also where the victim of a crime is situated in the territory of a state wishing to exercise jurisdiction over that crime. This has been regarded traditionally as a factor which determines the location of the criminal act. With most cybercrimes, however, the location of the victim can no longer be seen reasonably as a factor determining the location of the crime.¹⁷²

Moreover, some cybercrimes (for example hate-speech and child pornography) have identifiable victims. The same cannot be said of cyber money laundering. As a result, it may be concluded that the location of victims is an inadequate factor for countries to take into consideration when seeking to exercise jurisdiction over cyber money laundering.

¹⁷⁰ Stessens (2000: 218).

¹⁷¹ Stessens (2000: 219).

¹⁷² Brenner (2004: 17).

4.2.3 Nationality of Perpetrator

While territoriality is the major factor determining jurisdiction over most international crimes, jurisdiction can be based also on the nationality of the perpetrator.¹⁷³ Article 22(1)(d) of the Convention on Cybercrime requires states parties to exercise jurisdiction over its nationals:

if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

As the crime of cyber money laundering has no clearly identifiable victims, the nationality of the perpetrator becomes an essential tool in establishing jurisdiction over the crime.

4.3 Investigation and Prosecution of Cyber Money Laundering

As the internet and new technology render geography irrelevant, there could be numerous repercussions for countries wishing to investigate and prosecute the crime of cyber money laundering. As a starting point, jurisdiction may be lacking entirely when all of the countries involved have no authority to assert jurisdiction over the crime of cyber money laundering. Secondly, jurisdiction may exist but be impossible to enforce. This could arise when a country has not outlawed the crime of cyber money laundering and consequently refuses to extradite the perpetrator to a country wishing to prosecute. Lastly, jurisdiction may be claimed by several states simultaneously.¹⁷⁴

¹⁷³ Brenner (2004: 24).

¹⁷⁴ Brenner (2006: 190).

4.3.1 Investigation

Since cyber money laundering is committed, at least in part, over the internet, the use of digital evidence will be essential in the prosecution of the crime.¹⁷⁵

Digital evidence is defined as:

any information of probative value that is either stored or transmitted in a digital form [and is a] representation of information using numbers, such as binary digits, which are not accessible to the human senses.¹⁷⁶

Digital evidence is thus different from evidence which has been replicated from a non-digital format, as it consists primarily of intangible information which originates from digital devices.¹⁷⁷ As a result, high levels of encryption and ease of manipulation are factors which ultimately affect the reliability of digital evidence.¹⁷⁸

In addition, digital evidence has a short life span and often is located in a foreign country, complicating even further the investigation of cyber money laundering.¹⁷⁹ One author has made the following observations about the reliability of digital evidence:

Firstly, altering (inserting, modifying or deleting) digital records is so easy that it may happen accidentally ... Secondly, there is a widespread belief that a competent forensic examination will invariably detect any manipulation of records. This belief is fallacious in the case of digital records ... Thirdly, there is an absence of generally recognised standards of best practice in digital evidence forensic procedures, and a lack of adequate training of forensic examiners ... Lastly, the modern world is becoming more digitally data dependent ... The sheer size of digital data on computers and networks imposes resource challenges to forensic investigators who must organise, scan and sift through these 'electronic haystacks' to determine who is responsible.¹⁸⁰

Cyber money launderers exploit the internet by commencing their laundering process in a different country, concealing evidence in a foreign location and by

¹⁷⁵ Chaikin (2006: 239).

¹⁷⁶ Chaikin (2006: 241).

¹⁷⁷ Chaikin (2006: 239).

¹⁷⁸ Casey (2002: 2) and Chaikin (2006: 239).

¹⁷⁹ Chaikin (2006: 239).

¹⁸⁰ Chaikin (2006: 242).

taking advantage of the weaknesses in international co-operation. The internet consists of countless links, servers, hosts and routers.¹⁸¹ Internet-based digital evidence includes evidence from Internet Service Providers (ISPs) which are scattered all over the world.¹⁸²

ISPs supply their customers with access to the internet, e-mail and web site hosting.¹⁸³ Each computer has a unique Internet Protocol (IP) address. The IP address of a computer is a number which simply describes the location of the computer in the internet.¹⁸⁴ ISPs use log files to store information regarding the identification of a person who was using a specific IP address while accessing the internet via the ISP.¹⁸⁵ These log files could then be used by law enforcement agencies to identify individuals suspected of cyber money laundering.

However, ISPs do not keep these files indefinitely because of the costs involved in mass digital storage.¹⁸⁶ Investigating a case of cyber money laundering would involve tracing digital evidence backwards from the completion of the crime to the implementation of the crime.¹⁸⁷ Given the transnational scope of cyber money laundering, this would require the co-operation of foreign law enforcement agencies and multiple ISPs located in several countries in order to trace the internet communications. The immediate response thus should be to obtain preservation orders for all the countries involved in the overarching crime of cyber money laundering. However, preservation orders for cyber money laundering may be problematic due to time constraints. During the layering

¹⁸¹ Chaikin (2006: 244).

¹⁸² Sommer (1998: 73).

¹⁸³ Sommer (1998: 73).

¹⁸⁴ Carrier (2003: 16) and Chaikin (2006: 244).

¹⁸⁵ Chaikin (2006: 244).

¹⁸⁶ Chaikin (2006: 244).

¹⁸⁷ Chaikin (2006: 245).

phase of cyber money laundering, the perpetrator attempts to conceal the criminal origin of the dirty money. As a result, there is a concern that the fragile digital data will disappear unless they are secured immediately by the relevant ISP.¹⁸⁸

4.3.2 Prosecution

Given the ease with which cyber money laundering can be achieved through the use of the internet, it is essential for prosecutors to equip themselves with sufficient knowledge to respond effectively.¹⁸⁹ As technology continues to advance, it will create more opportunities for criminal exploitation. Further, the incorporation of technological improvements differs from country to country.¹⁹⁰ Countries which are slow to receive technological improvements may serve unwittingly as havens for cyber money launderers. There is thus a need to develop a legal and institutional framework which would enable prosecutions of new forms of crime.

The extent of a prosecutor's involvement in a cyber money laundering case will depend on his role within the criminal justice system of his country. In civil law countries, the decision to begin an investigation may rest with the prosecutor, depending on certain factors. For example, in the United States prosecutors are engaged often in the preparation, organisation and execution of criminal investigations, which provide for detailed prosecutorial oversight. In some countries, prosecutors may be involved even in the drafting of legislation and the

¹⁸⁸ Chaikin (2006: 246).

¹⁸⁹ Grabosky (2007: 201).

¹⁹⁰ Grabosky (2007: 202).

determination of a sentence following conviction.¹⁹¹ If prosecutors are involved in a case from an early stage it would ensure that investigations are efficient and that the rights of suspects are protected.

In common law jurisdictions, prosecutors often must decide which cases to take on and which not. In other legal systems, prosecutors may be obligated to prosecute once there is sufficient evidence.¹⁹² However, most prosecutors face resource constraints and, as a result, a case which is not likely to end in any significant punishment may not be taken up. The resource limitation of most prosecutors is an important factor and may be a major obstacle in the prosecution of cyber money laundering. For example, the costs involved in bringing an ISP from France to South Africa are not trivial.

Prosecutors also are responsible primarily for presenting evidence in court. In cases of cyber money laundering, the presentation of the evidence could be essential in the prosecution of the crime. This is because judges and jurors would be relatively unfamiliar with digital technology and its criminal exploitation.¹⁹³ Essentially, the decision of a prosecutor inevitably is affected by socio-economic values and national interests.

4.3.3 Substantive Criminal Law

The generality of a country's traditional criminal law will determine whether such law is flexible enough to embrace traditional crimes when they are committed with digital technology. The fact that property can exist in an intangible form on

¹⁹¹ Grabosky (2007: 206).

¹⁹² Grabosky (2007: 207).

¹⁹³ Bell (1999: 105).

the internet has brought about a broadening of the conventional form of criminal damage.¹⁹⁴ Highly technical economic crimes seldom are committed against any identifiable victims. Still, they undermine the rule of law and contribute to a weakened economy and, in some instances, to terrorist financing. This is especially so in the case of cyber money laundering.

At the very least, legislation should enable law enforcement agencies to obtain full records of all transactions made by or on behalf of cyber money launderers and enable them to share that information with other investigative agencies.¹⁹⁵

Ideally, legislation should be general enough to encompass new emerging forms of crime, but not so general as to be impossibly vague. As one author has noted:

Legislation that is over-broad or vague may be subject to inappropriate application. It may be seen as an invitation to the abuse of power. The legitimate goal of criminalizing communications in furtherance of terrorist conspiracies does not justify legislation that would also prohibit or discourage legitimate political expression. In order to avoid this problem, care must be taken to formulate laws as precise and specific as possible.¹⁹⁶

The truth is that technology invariably does advance faster than the law. Where existing law is unable readily to encompass new forms of technical and digital crimes, prosecutors would have no choice but to 'force' the facts into a form apparently consistent with the law.¹⁹⁷

4.3.4 Criminal Procedural Law

One of the most dominant powers that a state can wield against its citizens is the power of search and seizure. It is thus essential that this power is used in

¹⁹⁴ Grabosky (2007: 209).

¹⁹⁵ Bell (1999: 105).

¹⁹⁶ Grabosky (2007: 210).

¹⁹⁷ Grabosky (2007: 209).

accordance with the rule of law.¹⁹⁸ Although cyber money laundering occurs through the intricate web of cyberspace, cyber money launderers inevitably have to use digital devices in order to accomplish money laundering. According to the rule of law, digital devices would be protected also under privacy rights in as much as any other private property would be. The majority of countries require enforcement agencies to acquire formal judicial authority prior to searching or seizing property.¹⁹⁹ Only in some countries is this authority vested in prosecutors or police. Regardless of this, authority to search or seize property ideally ought to be very detailed and contain probable cause of the commission of a crime.²⁰⁰

4.3.5 Mutual Legal Assistance

If, for example, a cybercrime is committed against individuals in Country A, Country B and Country C, the cyber criminal would have committed a crime in each of these countries. Provided each country has a penal law that criminalises the relevant conduct, the perpetrator could be prosecuted in any one of these countries.²⁰¹ However, the matter becomes more complicated in relation to the issue of cyber money laundering.

For a crime to be defined as money laundering, it must contain a placement, layering and integration phase. The same applies to cyber money laundering. While these elements may not be difficult to identify for an overarching crime of cyber money laundering, they could cause great difficulties in the prosecution thereof. For instance, if a cyber money launderer placed the dirty money in

¹⁹⁸ Grabosky (2007: 211).

¹⁹⁹ Grabosky (2007: 211).

²⁰⁰ Grabosky (2007: 211).

²⁰¹ Brenner (2006: 197).

Country A, layered the money in Country B and integrated the money in Country C, there may be doubt as to whether the crime would be prosecutable in any country as the elements of the crime are scattered across several jurisdictions.

As the principle of universal jurisdiction does not apply to cyber money laundering, only countries involved in the crime will have jurisdiction to prosecute. From the example given above, it appears that when several countries are involved in a crime of cyber money laundering, they will be unable to prosecute the crime in isolation. Each would require co-operation from the others in the prosecution of the crime. Co-operation is especially necessary for collecting evidence of the offence. Without the co-operation of other countries, the prosecution of cyber money laundering by a single country surely would yield unsatisfactory results.



Following the digital trail of a cyber money laundering offence always will be a great challenge. This necessitates high degrees of correspondence between countries and rapid responses in order to preserve digital evidence.²⁰² There are two basic types of co-operation: informal legal assistance and formal mutual legal assistance.²⁰³ Informal assistance between countries is based on working relationships between police services of the countries in question and previous joint investigations.²⁰⁴

Although more expeditious than formal mutual legal assistance, informal legal assistance can be relied on only in the absence of compulsory powers required by, for example, search warrants. Formal mutual legal assistance is traditionally

²⁰² Bell (1999: 109).

²⁰³ Grabosky (2007: 215).

²⁰⁴ Grabosky (2007: 215).

born of treaty arrangements between countries and is more cumbersome than informal legal assistance. It usually requires the exchange of formal documents and an offence that exceeds a certain threshold of severity.²⁰⁵ Although any country may request formal mutual legal assistance from any other country, it is usually easier with the existence of prior treaty arrangements.²⁰⁶

Unfortunately, the framework of treaties and other arrangements which may form the basis of mutual legal assistance is far from ideal.²⁰⁷ Mutual legal assistance may also involve high costs and this burden is placed on the party providing the assistance.²⁰⁸ However, countries seeking assistance do sometimes cover the corresponding costs.²⁰⁹

Even the United Nations Convention against Transnational Organised Crime provides for certain cost relief and sharing provisions.²¹⁰ This, however, will apply to cybercrimes only when they are committed by an organised criminal group.²¹¹ Another example of the movement toward harmonisation of cyber crime is the Council of Europe Convention on Cyber Crime. To date this is the most significant initiative in cyber crime control and seeks to achieve a degree of consistency in substantive and procedural criminal law in cases of cyber crime committed across national frontiers.²¹²

While perfect uniformity of substantive and procedural criminal law across the world's legal systems will be almost impossible to achieve, a degree of

²⁰⁵ Bell (1999: 109) and Grabosky (2007: 215).

²⁰⁶ Grabosky (2007: 215).

²⁰⁷ Grabosky (2007: 217).

²⁰⁸ Bell (1999: 109).

²⁰⁹ Grabosky (2007: 217).

²¹⁰ Article 18(28) of the United Nations Convention against Transnational Organised Crime.

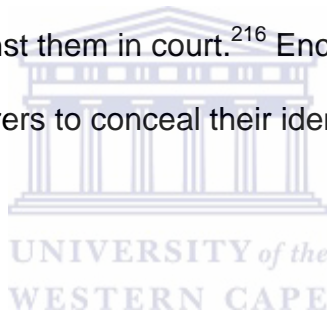
²¹¹ Article 3(1) of the United Nations Convention against Transnational Organised Crime.

²¹² Grabosky (2007: 218).

consistency on core offences is somewhat more achievable.²¹³

4.3.6 Encryption

The problems related to cybercrime are inflated by the widespread availability of encryption technology. This technology enables cyber criminals to conceal the content of electronic communications by mathematically encoding the transaction with a special formula called an encryption key.²¹⁴ The receiving party must have this encryption key to decrypt successfully a coded transaction.²¹⁵ Thus, encryption allows cyber money launderers to conceal information which could lead to exposure of their criminal activities and consequently be used against them in court.²¹⁶ Encryption technology further allows cyber money launderers to conceal their identities or impersonate other users on the internet.



Anti-money laundering authorities thus should be highly educated on the issue of encryption in order to investigate a matter of cyber money laundering.²¹⁷ It is worthy of note that encryption also may cause severe complications during the prosecution phase. The right against self-incrimination is a well-established constitutional right in many countries. Should an accused then be required to provide the encryption key for encrypted information which could incriminate him, it could violate this fundamental constitutional right.

²¹³ Grabosky (2007: 217).

²¹⁴ Straub (2001: 521).

²¹⁵ Straub (2001: 522).

²¹⁶ Grabosky (2007: 212).

²¹⁷ Grabosky (2007: 212).

4.4 Confiscation and Forfeiture

Pieth submits that the primary purpose of anti-money laundering law in the beginning was not so much to criminalise the behaviour of individuals but rather to secure the forfeiture of ill-gotten gains.²¹⁸ The worldwide adoption of laws which enable confiscation of the proceeds of crime reflects the acknowledged importance of depriving a criminal of the profits of crime. These laws acknowledge that the more profitable the crime, the more difficult it becomes for law enforcement agencies to link the criminal to it.²¹⁹

Broadly speaking, there are two ways in which a state can retrieve stolen assets: criminal or civil forfeiture. Criminal forfeiture requires a conviction before assets can be forfeited to the state and is often referred to as conviction-based confiscation.²²⁰ Although more controversial than criminal forfeiture, civil forfeiture allows for confiscation of stolen assets without a conviction.



South Africa and the United States are examples of countries where civil forfeiture is possible.²²¹ In South Africa, the Prevention of Organised Crime Act of 1998 enables the state to confiscate assets belonging to a person not convicted of any crime.²²² The state must show merely that the assets are probably the proceeds of crime, taking into consideration all relevant factors.²²³

²¹⁸ Pieth (2002: 367).

²¹⁹ Smellie (2004: 104).

²²⁰ Smellie (2004: 104).

²²¹ Basel Institute on Governance (2009: 31).

²²² Article 37 of the Prevention of Organised Crime Act 121 of 1998.

²²³ Article 4 of the Prevention of Organised Crime Act 121 of 1998.

Historically, the United States has been in the forefront of proceeds of crime legislation and enforcement action in respect of money laundering.²²⁴ As early as 1960, civil forfeiture was available in cases connected to money laundering under the Racketeer Influenced and Corrupt Organisation Act U.S.C. §1963 (RICO) and the Controlled Substances Act, Continuing Criminal Enterprise Offence U.S.C. §848 (CEE). In addition, the Money Laundering Control Act U.S.C. §1956 provides for both criminal and civil forfeiture. In the United States virtually anything can be forfeited if it is shown that the thing was used in the facilitation of a crime. However, in the case of real property it is required that the role of such property in the facilitation of the crime must be substantial.²²⁵

Interestingly, the United States adopts the doctrine of the fruit of the poisoned tree. This means, for example, that the equity received from the sale of a house which was purchased with laundered money may be forfeited.²²⁶

From this the advantages of civil forfeiture become clear. Civil forfeiture requires proof on a balance of probabilities while criminal forfeiture requires proof beyond a reasonable doubt. Civil forfeiture is achieved through *in rem* proceedings, meaning that the proceedings are targeted at the property itself and not the person. This approach is founded on the proposition that the property (which could consist of money) is guilty of the offence of being used illegally.²²⁷

The following is a list of examples of when it is necessary, or at least better, to do forfeiture civilly:

²²⁴ Smellie (2004: 105).

²²⁵ Evans (1995: 3).

²²⁶ Evans (1995: 3).

²²⁷ Evans (1995: 2).

1. where forfeiture is uncontested, property could essentially be forfeited to the state by default;
2. where the defendant has died, criminal forfeiture would be impossible;
3. where the primary wrongdoer is unknown;
4. where the property belongs to a third party and criminal proceedings cannot be brought against such third party;
5. where the interests of justice do not require a criminal conviction.²²⁸

If all countries are allowed to use civil forfeiture in securing the funds involved in the crime of cyber money laundering, it would be less difficult to recover stolen assets as the burden of proof is lower. By depriving criminals of enjoyment of the fruits of their crime, civil forfeiture would fulfil, to a large extent, the objectives of anti-money laundering initiatives. Also, civil forfeiture does not preclude a subsequent criminal prosecution. Thus, civil forfeiture is an ideal mechanism for recovering assets stolen by means of cyber money laundering.

Ample experience of money laundering has shown just how easy it is to obscure the proceeds of crime. This is exacerbated in the case of cyber money laundering. As a result, financial centres currently place a lot of emphasis on developing a system which would allow for more effective freezing, confiscation, mutual legal assistance and repatriation of stolen assets.²²⁹

But this will be effective only if it encompasses the co-operation of banks, lawyers, FIUs and law enforcement agencies, as well as public and private

²²⁸ Casella (2008: 10).

²²⁹ Basel Institute on Governance (2009: 7).

forensic specialists.²³⁰ Co-operation during a financial investigation is essential in any strategy which is aimed at recovering the proceeds of crime.²³¹

Chapter 2 established the importance of the standards set by the FATF in the fight against money laundering. To this extent, the FATF is considered the main international anti-money laundering standard setter.²³² Relevant to asset tracing, the main international anti-money laundering framework consists of the following elements: the criminalisation of money laundering, due diligence measures placed on financial and certain non-financial businesses and professions, the supervision of these institutions and the requirement to report suspicious transactions to FIUs.²³³ These elements have to be considered individually in order to identify their potential for the tracing and recovery of stolen assets in general.



4.4.1 The Criminalisation of Money Laundering

Individuals who work in financial institutions or deal with others' assets remain the main focus of the criminal offence of money laundering. If these individuals become aware (or should be aware) that the proceeds they are receiving originate from a crime and do not refrain from accepting or transferring the proceeds, they too will be held criminally liable.²³⁴ Although cyber money launderers are capable of laundering money without the assistance of intermediaries, the possibility exists that funds eventually would pass through intermediaries (such as banks or brokers) during the laundering cycle. If these

²³⁰ Basel Institute on Governance (2009: 7).

²³¹ Basel Institute on Governance (2009: 19).

²³² Basel Institute on Governance (2009: 62).

²³³ Basel Institute on Governance (2009: 62).

²³⁴ Basel Institute on Governance (2009: 63).

individuals then are reminded of their possible criminal liability for money laundering, they are almost certain to co-operate with law enforcement agencies during the course of their investigations.²³⁵ In addition, the FATF recommends that countries should introduce criminal, civil or administrative liability for legal persons.²³⁶

Although focusing on corruption (a possible predicate offence for money laundering), the United Nations Convention against Corruption insists on the same standard when it comes to money laundering.²³⁷ This, in turn, will ensure the co-operation of financial institutions in much the same way as it did with individuals working for such institutions.

4.4.2 Due Diligence Measures

The due diligence measures placed on financial institutions and designated non-financial business and professions will be discussed in Chapter 5. For the purposes of asset recovery, the documents required by institutions to identify their clients, beneficial owners and the intention of the business relationship will constitute yet another source of information for law enforcement agencies investigating a case of money laundering.²³⁸

As seen from Chapter 2, the FATF has recommended that institutions which offer financial services should be made subject also to due diligence provisions.²³⁹ In relation to cyber money laundering, this would mean that law enforcement

²³⁵ Basel Institute on Governance (2009: 63).

²³⁶ FATF Recommendation 2.

²³⁷ Article 26 of UNCAC.

²³⁸ Basel Institute on Governance (2009: 65).

²³⁹ FATF Special Recommendation 6.

agencies would be capable also of using information from 'alternative remittance banking', such as the Hawala system.²⁴⁰

4.4.3 Supervisory Measures

All the institutions in a country which are subject to anti-money laundering legislation are also subject to oversight by a relevant state body. In general, these institutions would attempt first to address the requirements of their supervisors before thinking of the risk of a potential criminal investigation.²⁴¹

Avoiding criminal prosecution for cyber money laundering is an incentive for a financial institution, which could be used to the advantage of an investigator.

This is done by informing the supervisory body of the constraints involved in investigating cases where supervised entities are involved, with the view to allowing the supervisor to remind the supervised entity of its obligations.²⁴² As a last resort, this could be achieved also by identifying financial institutions which do not apply anti-money laundering provisions. Naming and shaming these institutions often has a greater impact than a criminal investigation, as these institutions rely heavily on their reputations within the markets in which they operate.

²⁴⁰ See section 2.4 above.

²⁴¹ Basel Institute on Governance (2009: 68).

²⁴² Basel Institute on Governance (2009: 68).

4.4.4 Reporting of suspicious transactions

The reporting of suspicious transactions by institutions is probably the most interesting tool in an investigator's arsenal for tracing stolen assets, especially with regard to cyber money laundering. When enforcement agencies believe that funds have been stashed away in financial institutions (or other designated institutions) in another jurisdiction, often they would not know which particular institution is involved. If they were then to request mutual legal assistance from a country with a relatively high number of financial institutions, such request would be considered to be a fishing expedition and rebuffed.²⁴³ How can this obstacle be overcome?

Most banks are likely to file a suspicious activity report (SAR) if the information reaches the bank that its client is under investigation for a predicate offence to money laundering. The SAR would be filed with the FIU of the bank concerned.²⁴⁴ The FIU can then make the information available to its counterpart FIU in the country where the predicate offence took place. In turn, the receiving FIU could make the information available to the investigating authority tracing the stolen assets. However, in most instances this information can be made available as intelligence only and not as evidence.²⁴⁵

4.5 Conflicting Jurisdictions

As mentioned previously, cyber money laundering is almost always likely to result in the commission of the crime in multiple countries. If several of these countries then wish to prosecute the cyber money launderer, the result is 'a

²⁴³ Basel Institute on Governance (2009: 65).

²⁴⁴ Bantekas (2003: 325).

²⁴⁵ Basel Institute on Governance (2009: 65).

positive jurisdictional conflict'.²⁴⁶ In other words, more than one country would claim jurisdiction over a perpetrator on the basis of the same conduct.

However, in reality each country would not seek to prosecute the cyber money launderer for precisely the same crime. Instead, countries would prosecute for crimes committed within their territory as part of the larger ongoing crime of cyber money laundering. Each country would then have to prioritise its respective claims in order to exercise jurisdiction over the perpetrator.²⁴⁷

Provided countries ensure that they do not violate the principle of double jeopardy, a perpetrator could be prosecuted sequentially by different countries, all of which have jurisdiction.²⁴⁸

The Convention on Cybercrime offers little guidance on the issue of conflicting jurisdictions. It merely states that 'Parties involved shall ... consult with a view to determining the most appropriate jurisdiction for prosecution'.²⁴⁹ Further, according to the explanatory note, such consultation is not obligatory.²⁵⁰ Even the United Nations Convention against Transnational Organized Crime merely states in, in Article 15(5), that:

If a State Party exercising its jurisdiction under paragraph 1 or 2 of this article has been notified, or has otherwise learned, that one or more other States Parties are conducting an investigation, prosecution or judicial proceeding in respect of the same conduct, the competent authorities of those States Parties shall, as appropriate, consult one another with a view to coordinating their actions.

One author is of the opinion that cases of positive jurisdictional conflicts should be determined by the reasonableness standard.²⁵¹ This standard means that a

²⁴⁶ Brenner (2006: 197).

²⁴⁷ Brenner (2006: 197).

²⁴⁸ Brenner (2004: 43).

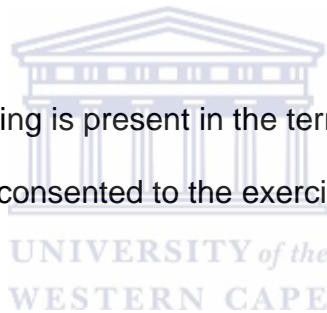
²⁴⁹ Article 22(5) of the Council of Europe Convention on Cybercrime.

²⁵⁰ The Council of Europe Convention on Cybercrime Explanatory Report No. 239.

²⁵¹ Brenner (2004: 41).

country's exercise of jurisdiction to proscribe and adjudicate must not be unreasonable. In determining reasonableness the following list of factors may be useful:

1. the extent to which the activity takes place and has an effect within the territory of the state;
2. nationality, residence or economic activity of the perpetrator;
3. the importance of regulating cybercrimes (more specifically cyber money laundering) to the regulating state;
4. the extent to which another state may have an interest in regulating the activity;
5. the likelihood of conflict with another state also wishing to prosecute the same crime;
6. whether the person or thing is present in the territory of the state; and
7. whether the person has consented to the exercise of jurisdiction.²⁵²



Although these factors are a mere guideline, it remains uncertain which factors should have the more weight in determining positive jurisdictional conflicts. It is clear that a perpetrator's nationality and physical presence will play a big role during this deliberation. With cyber money laundering other factors may be relevant also, such as the location of ISPs and computers from which the crime was committed.²⁵³

Since cyber money laundering renders borders irrelevant, an increase in jurisdictional conflicts is almost inevitable.²⁵⁴ In this regard, the traditional approach of negotiation between countries is no longer a viable option, because

²⁵² Brenner (2004: 29).

²⁵³ Brenner (2004: 42). See section 4.3.1 for a discussion of ISPs.

²⁵⁴ Brenner (2006: 197).

negotiation is time-consuming and unpredictable.²⁵⁵ Sections 4.5.1 – 4.5.5 below consider factors that could be taken into account in the resolution of conflicting jurisdictional claims in relation to cyber money laundering.

4.5.1 Custody of the Perpetrator

A perpetrator's presence within a country is the most logical and most basic rationale for asserting jurisdiction over such perpetrator. However, the issue becomes more complex in the case of cyber money laundering. As mentioned earlier, cyber money laundering renders borders between countries irrelevant. The question then is which of the several competing countries is allowed to bring the perpetrator to justice for the commission of the crime? This does not cause problems for cybercrimes in general, since each country could simply prosecute the perpetrator for an offence specific to its legal regime, if the criminal transaction is factually and legally severable.²⁵⁶ As a result, the fact that one country could prosecute before another would be immaterial.²⁵⁷

However, cyber money laundering problematises the issue since, in most instances, the location of a cyber money launderer is irrelevant. Such offenders are capable of laundering their money from virtually anywhere in the world, using the internet.

²⁵⁵ Brenner (2006: 198).

²⁵⁶ Brenner (2006: 199).

²⁵⁷ Brenner (2006: 199).

4.5.2 Damage

The actual harm caused to a country by an act of cyber money laundering could be a factor in considering a country's claim to prosecute a perpetrator.²⁵⁸

Although this seems like a rational factor to take into consideration, it may be extremely problematic in the case of cyber money laundering. Since cyber money laundering aims at concealing the proceeds of crime, it may be very difficult to determine the actual damage incurred by a country.

Regardless of the difficulties associated with assessing actual damage incurred by countries through cyber money laundering, damage still could be a relevant factor to take into consideration. However, there is a need to develop certain indicators which would assist in this assessment.²⁵⁹ An obvious indication of harm would be the impact on the country from which the dirty money originated. In this sense, funds would move illegally from the normal economic structure of a country to that of another. In essence, the country from which the dirty money has originated would find itself in a weaker economic position. However, since money laundering in general has been linked to terrorist financing, the same argument can be made for the country which receives dirty money.

More specifically, this refers to the country into which the laundered money is integrated. Whether a weak economy is better than an increase in terrorist financing is unclear. Certainly, both could have negative effects on the population of a country.

²⁵⁸ Brenner (2006: 200).

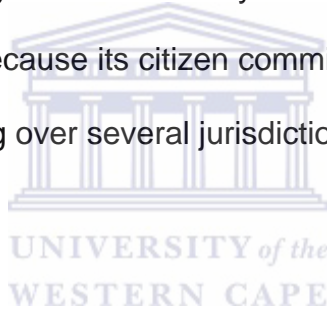
²⁵⁹ Brenner (2006: 200).

4.5.3 Nationality of the Perpetrator

In the traditional concept of crime, the nationality of the perpetrator is always a factor counting in favour of awarding jurisdictional priority.²⁶⁰ However, one author is of the opinion that, in the case of cybercrimes, the nationality of the perpetrator should be a factor that militates against awarding jurisdictional priority.²⁶¹ As another author has noted:

nationality-based criminal jurisdiction reflects the need [for one state] to maintain good relations with other states ... by deterring conduct by its own nationals that reflects poorly on the state abroad.²⁶²

Indirectly, the jurisdiction in which the perpetrator performed the act of cyber money laundering could be said to have 'allowed' the commission of the offence against other countries. Why should a country then be given jurisdiction to prosecute a crime simply because its citizen committed the crime of cyber money laundering stretching over several jurisdictions?



4.5.4 Strength of the Case

As the ultimate goal of the fight against cyber money laundering is bringing the perpetrator to justice, the strength of the case a country can bring should always be an important factor to take into consideration. This can be indicated by the extent to which a country has collected evidence tying a suspect to cyber money laundering, whether the perpetrator could raise any objections to the use of specific evidence, the applicability of the statute of limitations and any other relevant factor in the prosecution of the perpetrator.²⁶³

²⁶⁰ Brenner (2006: 202).

²⁶¹ Brenner (2006: 202).

²⁶² Watson (1993: 17).

²⁶³ Brenner (2006: 204).

4.5.5 Fairness

In a case of cyber money laundering, the fairness and impartiality of a prosecution in a particular country is an important factor to take into consideration when prioritising conflicting jurisdiction cases.²⁶⁴ This should include also considerations of convenience and practicality as to where the prosecution can take place.²⁶⁵

4.6 Conclusion

The truth is that technology has created the means to launder money by use of completely untraceable digital currency. While current money laundering laws apply to cyber money laundering, the actual effect of these laws may be limited. This is especially so when dealing with the issue of jurisdiction over cyber money laundering. The transnational scope of the crime complicates traditional theories of jurisdiction while simultaneously allowing for the possibility of positive jurisdictional conflicts. Encryption, lack of data storage requirements on ISPs and resource constraints placed on those charged with investigating and prosecuting money laundering impedes the fight against cyber money laundering.

In an asset recovery effort pertaining to cyber money laundering, it is the investigation phase which constitutes the core element.²⁶⁶ A country within which funds have been secreted will not confiscate or repatriate those funds to the country of origin unless sufficient evidence is presented. This evidence in turn must link the funds to an illegal activity and be admissible in a court of law.

²⁶⁴ Brenner (2006: 206).

²⁶⁵ Brenner (2006: 206).

²⁶⁶ Basel Institute on Governance (2009: 19).

As the investigation phase of cyber money laundering would constitute also the core element of recovering assets which were laundered, it is necessary to develop efficient investigative and provisional methods to identify, trace and rapidly freeze property in order to facilitate eventual confiscation.

Finally, if positive jurisdictional conflicts do occur, factors such as damage, fairness and nationality of the perpetrator will assist states in the resolution of conflicting claims. Unfortunately, there is no clear hierarchy between all of these factors. It is therefore important to develop ideas on how to resolve positive jurisdictional conflicts, beyond the obvious need for countries consulting each other in particular cases.²⁶⁷



²⁶⁷ Brenner (2004 : 43).

CHAPTER 5

ALTERNATIVE MEASURES TO COMBAT CYBER MONEY LAUNDERING

5.1 Review of Existing Approaches and Ideas

As was seen in Chapter 3, there are numerous international instruments and institutions involved in the fight against money laundering. However, when combating cyber money laundering, the initiatives of these international instruments and institutions fall short of what is required. Regardless of this, the existing principles relating to customer due diligence and the 'know your customer regime' will be appropriate still in combating cyber money laundering.

5.1.1 Know Your Customer Regime

Identifying customers in cyberspace is difficult and knowing how to do it is largely a matter of learning through experience. At the very least, anonymous banking and transacting should be avoided at all costs.²⁶⁸ The improvement of technology makes it even more difficult to identify customers. Cyber money launderers are capable of concealing their identity through encryption technology and financial institutions should be aware of this risk.

The KYC regime originally started out as a mere instruction to financial institutions and then became a key tool to combat money laundering.²⁶⁹ It was aimed originally at financial institutions to motivate them to identify their customers and to report any suspicious transactions.²⁷⁰ These notions would

²⁶⁸ Jaarsveld (2004: 690).

²⁶⁹ Cotteril (2001: 17) and Jaarsveld (2004: 689).

²⁷⁰ Cotteril (2001: 17).

later become mandatory.²⁷¹ However, KYC goes further than simply knowing the names and addresses of customers; it also involves knowing something about their background and activities.²⁷² If transactions then pass through accounts which are inconsistent with what the bank would expect from a customer, then the bank may be required to report such transactions to supervisory authorities.

It must be noted that there is unfortunately no international 'hard law' which contributes to this programme. Nevertheless, international organisations such as the FATF have contributed significantly to its content. For this programme to be successful it must consist of four components: knowledge of your customer, the obligation to report suspicion or knowledge of money laundering, the retention of certain records and, lastly, awareness-raising and training.²⁷³



5.1.2 Customer Due Diligence

The FATF has established certain customer due diligence (CDD) and record-keeping measures to be taken by financial institutions and non-financial businesses and professions to prevent money laundering. CDD is intended to limit criminal access to the financial system and to other means of placing the proceeds of crime.²⁷⁴ Focus should be placed on successfully preventing cyber money laundering at the placement stage, before the layering process can disguise the illegal origin of funds.²⁷⁵ In order successfully to curb new techniques of money laundering while simultaneously promoting technological development, governments should focus on regulating the illegal transaction,

²⁷¹ Jaarsveld (2004: 689).

²⁷² Cotteril (2001: 17).

²⁷³ Jaarsveld (2004: 689).

²⁷⁴ Reuter (2004: 46).

²⁷⁵ Straub (2001: 528).

rather than the technology of online-banking.²⁷⁶ As a starting point, the FATF recommends that:

countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.²⁷⁷

The FATF customer due diligence measures to be taken are as follows:

1. Identifying the customer and verifying his or her identity using reliable and independent data or information;
2. Identifying the beneficial owner, and taking reasonable measures to verify his or her identity such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements the financial institutions should take reasonable measures to understand the ownership and control structure of the customer;
3. Obtaining information on the purpose and intended nature of the business relationship; and
4. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship.²⁷⁸

In addition, the FATF requires financial institutions to perform enhanced due diligence for high risk categories. Recommendation 8 of the FATF is of vital importance in the fight against cyber money laundering. It requires financial institutions to pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity. As a result, financial institutions should have policies and procedures in place to address any specific risks associated with business relationships or transactions which are not face-to-face. As the internet provides high degrees of anonymity, financial institutions should be in a position to identify cases of cyber money laundering. Unfortunately, criminals who abuse technology are always at the forefront of new technological developments. Because of this, vulnerable institutions and law enforcement agencies should ensure that they have personnel who are highly skilled in these areas.

²⁷⁶ Straub (2001: 528).

²⁷⁷ FATF Recommendation 4.

²⁷⁸ FATF Recommendation 5.

5.2 A New Approach

Traditional methods of combating money laundering are no longer effective. Cyber money laundering has shown just how easy it is for criminals to launder proceeds of crime quickly and with relatively low risk by using the internet. The difficulty in monitoring crimes committed over the internet is evident from the fact that internet-based financial crimes are almost invisible.²⁷⁹ Because of this, funding which was spent on identifying criminals and proceeds of crime now would be spent better on preventing computer-generated crime.

In Chapter 4 the fragility of digital evidence was discussed. Ease of manipulation and advances in encryption technology are factors which ultimately affect the reliability of digital evidence. Because of this, focus should be shifted from identifying money laundering towards the prevention thereof. This could be accomplished by focusing on commercial and legal awareness.²⁸⁰ However, encryption software could be used also to the advantage of those wishing to fight cyber money laundering. Financial institutions should be in a position to encrypt information which is vulnerable to cyber money laundering.

Because it is possible for banks to serve their customers from anywhere in the world through the internet, national regulators cannot prevent financial institutions from setting up business in inadequately regulated areas. This practice questions the credibility of banking regulation in general.²⁸¹ By addressing this issue, it is possible that some of the barriers to fighting cyber money laundering could be overcome. Here, a two-pronged approach has been

²⁷⁹ Lilley (2009: 109).

²⁸⁰ Jaarsveld (2004: 701).

²⁸¹ Jaarsveld (2004: 701).

suggested.²⁸²

Firstly, by allowing the financial industry to regulate itself, clearer guidelines on how to identify cyber money laundering may come from the industry itself.

Secondly, regulators could experiment with these guidelines by creating conditions for the approval of bank applications for product expansion.²⁸³

Preventing cyber money laundering is a daunting task for any law enforcement agency or organisation. However, given the difficulties of fragile digital evidence, prevention is the only feasible technique against cyber money laundering.

Prevention initiatives are designed to deter criminals from using private individuals and institutions to launder the proceeds of their crimes.²⁸⁴ Law enforcement agencies and other institutions dealing with cyber money laundering thus should take adequate steps to identify weaknesses in security systems which could be infiltrated via the internet. By using advanced and updated computer software, financial institutions would be able to prohibit access to any vulnerable information which could be reached through the internet.

The discussion of CDD highlights the role which financial and non-financial institutions could play in preventing cyber money laundering. However, the scope of the FATF due diligence and record-keeping measures should be broadened in order to counter cyber money laundering effectively. For example, requiring ISPs to implement the CDD and record-keeping measures of the FATF would facilitate the tracing of those responsible for cyber money laundering.

²⁸² Jaarsveld (2004: 702).

²⁸³ Jaarsveld (2004: 702).

²⁸⁴ Reuter (2004: 46).

Unfortunately, requiring ISPs to identify each of their customers would be a herculean task, as preserving high volumes of data is extremely expensive. Nevertheless, the advantages gained by applying the FATF Recommendations to all institutions and businesses vulnerable to cyber money laundering cannot be overlooked.

5.2.1 Undercover Investigations

Cyber money launderers often use false identities while conducting their laundering activities over the internet in order to offer an extra barrier of protection against investigators. In some jurisdictions, it is possible for law enforcement agencies to impersonate private citizens in the course of investigations on the internet. For example, it is common in the United States for investigators to develop elaborate traps in order to identify possible cyber criminals. As early as 1995, the United States Security Service launched an investigation codenamed Operation Cybersnare. Investigators established an internet discussion group from which individuals could purchase stolen cellular phone access numbers and credit card numbers. Criminals who joined the group and then offered illegal products for sale were identified and prosecuted.²⁸⁵

Other countries do not permit internet investigations as they can, and often do, infringe on privacy rights and freedom of expression.²⁸⁶ However, the advantages that undercover internet-based investigations can contribute to the fight against cyber money laundering cannot be ignored.

²⁸⁵ Grabosky (2007: 211).

²⁸⁶ Grabosky (2007: 211).

Allowing investigators to create and monitor environments on the internet which are conducive to money laundering attacks would assist in the prevention of cyber money laundering at an early stage. But, as there is a real threat of violating privacy and other rights of innocent individuals, online undercover investigations should be subject to strict guidelines and vigorous oversight.²⁸⁷

5.2.2 Remote Searches

Improvements in technology have complicated traditional search and seizure measures. Often with cyber money laundering, the evidence required for investigation and eventual prosecution may be dispersed across an entire computer network stretching over multiple countries. This evidence may be far removed from the physical location of a search, but still may be accessible from digital devices at a particular location.²⁸⁸ While investigators may not be concerned that their cyberspace investigations are taking them into the jurisdictions of another country, authorities in that country may be very concerned.²⁸⁹ As cyber money laundering often is concluded in or routed through other countries, such searches will be necessary in the fight against it. Australia has recognised this need for 'remote transnational internet searches'. According to Australian law, there are no geographical limits upon the investigation of cybercrime, nor is there any obligation to acquire consent from third parties.²⁹⁰

²⁸⁷ Grabosky (2007: 212).

²⁸⁸ Grabosky (2007: 212).

²⁸⁹ Grabosky (2007: 212).

²⁹⁰ Section 15 of the Australian Cybercrime Act 161 Of 2001.

Although remote searches may interfere with the sovereignty of states to some degree, they are necessary in the fight against cyber money laundering. If investigators had to be mindful of accidentally traversing the 'cyberspace jurisdiction' of another country, attempts to bring cyber money launderers to justice surely would be impeded.



CHAPTER 6

CONCLUSION

Unlike other areas of cybercrime law, a country's ability to assert jurisdiction over cyber money launderers sometimes may seem problematic. Cyber money laundering encompasses elements from both cybercrimes and the traditional concept of money laundering. While most international instruments focus either on cybercrime or money laundering in isolation, none of them specifically addresses the issue of cyber money laundering. Although traditional principles relating to real-world crimes can be used to justify jurisdiction over cyber criminals, no real progress has been made in determining cases of positive jurisdictional conflicts. For this reason, the issue of prioritising claims of competing jurisdictions needs to be resolved by the international community.

Although some progress has been made in the furtherance of international co-operation to combat cybercrime in general, a great deal more remains to be accomplished. There remains a need for expeditious preservation orders of digital evidence, consistency in substantive and procedural law that would permit real time tracing of cyber money laundering trails, and the possibility of requesting mutual legal assistance via e-mail.²⁹¹

The use of multiple jurisdictions increases problems of investigation and prosecution. However, in most jurisdictions, serious problems of investigation begin long before money is moved to other jurisdictions.²⁹² Many police forces are equipped too poorly to investigate sophisticated forms of money laundering.

²⁹¹ Grabosky (2007: 218).

²⁹² Evans (1995: 15).

In developing countries, resource constraints on investigators and prosecutors aggravate the problem. With some notable exceptions, they do not have the resources either to employ or buy the forensic accounting, financial analysis, computer skills, and ongoing legal advice needed to unravel sophisticated and new forms of crimes.²⁹³

While the laws of some countries allow for general search warrants, others require a great amount of detail about the property to be searched or seized.²⁹⁴

This inevitably creates difficulties in combating cyber money laundering.

Because of its transnational scope, countries ideally should have similar provisions relating to the search and seizure of property used in the commission of an act of cyber money laundering. In the absence of uniformity among countries, the prosecution and investigation of cyber money laundering would be unpredictable and sluggish. As cyber money laundering necessitates rapid preservation orders for property used in the money laundering scheme, the time wasted by authorities applying for search warrants could be spent better. After all, the internet would allow cyber money launderers to transfer funds instantaneously from one end of the world to another. The use of traditional methods thus is inadequate in the fight against cyber money laundering. While these methods do protect against the violation of the rule of law, they are outdated and new methods need to be developed.

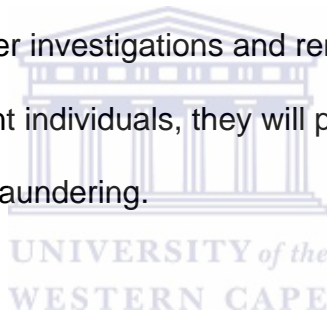
Although there is no magic formula which could cure the internet of cyber money laundering, it can be combated and diminished. The first step towards that objective may be a wider acceptance of the Convention on Cybercrime which

²⁹³ Evans (1995: 15).

²⁹⁴ Grabosky (2007: 211).

allows for expedient international co-operation and harmonisation of cybercriminal offences among legal systems.

However, this would require wider public awareness and would take time and effort. What is more, a Convention alone would not suffice to address the issue of cyber money laundering effectively. It must be accompanied by the political will of government actually to implement its provisions. This is especially true for emerging economies, where financial havens for money laundering have been embedded in the economic structure of the country. Focus should be placed on developing traditional approaches while simultaneously allowing for the development of new techniques in order effectively to combat cyber money laundering. While undercover investigations and remote searches are likely to infringe the rights of innocent individuals, they will prove most useful in the prevention of cyber money laundering.



Unfortunately, civil forfeiture remains a highly contested means of asset forfeiture and as a result countries have been slow in adopting its remedies. As Cassela has noted:

The point of all of this is that it is not enough for all of us to agree that the asset forfeiture laws are an important means of recovering the proceeds of crime, if all we mean by that is that we should have the ability to make a confiscation order part of the defendant's sentence in a criminal case. There is a significant and essential role to be played by civil forfeiture actions directed at the property itself. Many countries have enacted such laws, and I would urge others to do so.

Properly managed and directed, the recovery of stolen assets through the use of civil remedies available can be expeditious, cost effective and extremely detrimental for the criminals involved in cyber money laundering.²⁹⁵

²⁹⁵ Basel Institute on Governance (2009: 95).

Once the proceeds of the crime are integrated successfully into the financial system, many laundering operators take the precaution of moving money through more than one tax haven and shell company.²⁹⁶ If a cyber money laundering operation has not been detected before the proceeds of crime are moved to other jurisdictions, there will be little chance of a successful prosecution or forfeiture of proceeds.

Although the most sophisticated cyber money laundering operations effectively may be immune from prosecution, there is room for optimism. While the advancement of technology has created countless opportunities for cyber money launderers, criminals have gone free only because the substantive criminal law has yet to be brought into the digital age. However, this too will change as consensus grows on the detrimental effects of money laundering and the relative ease with which it can now be conducted over the internet.

²⁹⁶ Evans (1995: 15).

LIST OF REFERENCES

Primary Sources

Australia

The Cybercrime Act 161 of 2001.

Europe

Directive 91/308/EEC of the European Union on the Prevention of the Use of the Financial System for the Purpose of Money Laundering (The First Money Laundering Directive).

Directive 2001/97/EC of the European Parliament and the European Union on the Prevention of the Use of the Financial System for the Purpose of Money Laundering (The Second Money Laundering Directive).

Directive 2005/60/EC of the European Parliament and the Council of Europe on the Prevention of the Use of the Financial System for the Purpose of Money Laundering (The Third Money Laundering Directive).

The Council of Europe Convention on Cybercrime of November 2001.

The Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime of 1990.

South Africa

Prevention of Organised Crime Act (POCA) 121 of 1998.

United Kingdom

Computer Misuse Act of 1990.

Proceeds of Crime Act of 2002.

United Nations



United Nations Convention against Corruption of 2005.

United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention) of 19 December 1988.

United Nations Convention against Transnational Organised Crime of 2000.

Other

Statement of Principles of the Basel Committee on Banking Supervision and Regulation.

40 Recommendations and 9 Special Recommendations of the Financial Action Task Force.

Secondary Sources

Books

Chaikin D (2007) *Network Investigations of Cyber Attacks: the Limits of Digital Evidence* Springer Science: Published Online.

Grabosky P (2007) *Requirements of Prosecution Services to Deal with Cyber Crime* Springer Science: Published Online.

Kochan N (2006) *The Washing Machine: How Money Laundering and Terrorist Financing Soils Us* Texere Publishing: Published Online.

McCusker R (2007) *Transnational Organised Cyber Crime: Distinguishing Threat from Reality* Springer Science: Published Online.



Muller WH, Kalin CH & Goldsworth JG (2007) *Anti-Money Laundering: International Law and Practice* John Wiley & Sons Ltd: England.

Rahn RW (2002) *Why the War on Money Laundering Should be Abandoned* Springer Publishers: Berlin.

Shams H (2004) *Legal Globalization: Money Laundering Law and Other Cases* The British Institute of International and Comparative Law: London.

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

Lilley P (2009) *Dirty Dealing: The Untold Truth about Global Money Laundering, International Crime and Terrorism* Kogan Page Limited: United States.

Martin AE & Law J (2006) *Oxford Dictionary of Law* Oxford University Press: United States.

Reuter P & Truman EM (2004) *Chasing Dirty Money: The Fight Against Money Laundering* Institute for International Economics: United States.

Gilmore WC (1999) *Dirty Money: The Evolution of Money Laundering Counter-Measures* Council of Europe Publishing: Belgium.

Articles



UNIVERSITY of the
WESTERN CAPE

Bachus AS (2004) 'From Drugs to Terrorism: The Focus Shifts in the International Fight against Money Laundering after September 11, 2001' 21(3) *Arizona Journal of International and Comparative Law* 835.

Bantekas I (2003) 'Current Developments: The International Law of Terrorist Financing' 97(2) *The American Journal of International Law* 315.

Bell RE (1999) 'Prosecuting the Money Launderers Who Act for Organised Crime' 3 *Journal of Money Laundering Control* 104.

Bowers CB (2009) 'Hawala, Money Laundering and Terrorism Finance: Micro-Lending as an End to Illicit Remittance' 37 *Denver Journal of International Law and Policy* 379.

Brenner SW (2006) 'Cybercrime Jurisdiction' 46 *Crime, Law and Social Change* 189.

Brenner SW & Koops BJ (2004) 'Approaches to Cybercrime Jurisdiction' 4(1) *Journal of High Technology Law* 1.

Carrier B (2003) 'Getting Physical with the Digital Investigation Process' 2(2) *International Journal of Digital Evidence* 1.

Cassella SD (2008) 'The Case for Civil Forfeiture: Why *in Rem* Proceedings are an Essential Tool for Recovering the Proceeds of Crime' 11 *Journal of Money Laundering Control* 8.

Casey E (2002) 'Error, Uncertainty, and Loss in Digital Evidence' 1(2) *International Journal of Digital Evidence* 1.



Clark RS (2004) 'The United Nations Convention against Transnational Organised Crime' 50 *Wayne Law Review* 161.

Hinterseer K (2001) 'The Wolfsberg Anti-Money Laundering Principles' 5 *Journal of Money Laundering Control* 25.

Leong AVM (2007) 'Chasing Dirty Money: Domestic and International Measures against Money Laundering' 10(2) *Journal of Money Laundering Control* 140.

Panurach P (1996) 'Money in Electronic Commerce: Digital Cash, Electronic Fund Transfer, and Ecash' 39(6) *Communications of the ACM* 1.

Poremská M (2009) 'Money Laundering as a Cybercrime of White-Collars' 3(3) *Masaryk University Journal of Law and Technology* 387.

Pieth M (2002) 'Financing of Terrorism: Following the Money' 4 *European Journal of Law Reform* 365.

Pieth M (2007) 'The Wolfsberg Process' in WH Muller CH Kalin and JG Goldsworth (eds) *Anti-Money Laundering: International Law and Practice* John Wiley & Sons: Chichester.

Smellie A (2004) 'Prosecutorial Challenges in Freezing and Forfeiting Proceeds of Transnational Crime and the Use of International Asset Sharing to Promote International Cooperation' 8 *Journal of Money Laundering Control* 104.

Sommer P (1998) 'Digital Footprints: Assessing Computer Evidence' *Criminal Law Review Special Edition* 61.

Straub JP (2001) 'The Prevention of E-Money Laundering: Tracking the Elusive Audit Trail' 25 *Suffolk Transnational Law Review* 515.

Van Jaarsveld I (2004) 'Following the Money across Cyber Highways: A Herculean Task or International Challenge - Some Thoughts on Money Laundering on the Internet' 16(4) *South African Mercantile Law Journal* 685.

Watson GR (1993) 'The Passive Personality Principle' 28 *Texas International Law Journal* 1.

Internet Sources

Aiolfi G & Pieth M (2006) 'The Private Sector Becomes Active: The Wolfsberg Process' <http://www.wolfsberg-principles.com/pdf/Wolfsberg-Process.pdf> [accessed 10 November 2010].

Alweendo TK (2005) 'Crime and Money Laundering' <https://www.bon.com.na/docs/spr/Crime%20and%20money%20laundering.pdf> [accessed on 9 November 2010]

Archick K (2006) 'Cybercrime: The Council of Europe Convention' italy.usembassy.gov/pdf/other/RS21208.pdf [accessed on 7 August 2010].

Bartlett BL (2002) 'The Negative Effects of Money Laundering on Economic Development' http://www.adb.org/documents/Others/OGC-Toolkits/Anti-Money-Laundering/documents/money_laundering_neg_effects.pdf [accessed on 17 March 2010].

Basel Institute on Governance (2009) 'Tracing Stolen Assets: A Practitioner's Handbook' www.baselgovernance.org [accessed 7 August 2010].

Bortner RM (1996) 'Cyberlaundering: Anonymous Digital Cash and Money Laundering' <http://osaka.law.miami.edu/~froomkin/seminar/papers/bortner.htm> [accessed on 15 March 2010].

Cotteril NM (2001) 'Money Laundering' <http://www.jstor.org/stable/3183186?seq=2> [accessed on 11 November 2010].

Evans JL (1995) 'International Money Laundering: Enforcement Challenges and Opportunities' www.icclr.law.ubc.ca/Publications/.../Enforcement_Challenges.pdf [accessed 15 August 2010].

FATF (2003) 'Combating the Abuse of Alternative Remittance Systems: International Best Practices' <http://www.fatf-gafi.org/dataoecd/32/15/34255005.pdf> [accessed 10 November 2010].

Fera L, Hu M, Cheung G & Soper M (1996) 'Digital Cash Payment Systems' <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.51.5749&rep=rep1&type=pdf> [accessed 10 November 2010].

Kellerman T (2004) 'Money Laundering in Cyberspace: World Bank Financial Sector Working Paper' http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2006/04/21/000012009_20060421140305/Rendered/INDEX/359050rev0Mone1nCyberspace01PUBLIC1.txt [accessed on 9 November 2010].

Kerwer D (2005) 'Rules that Many Use: Standards and Global Regulation' http://en.wikipedia.org/wiki/Basel_Committee_on_Banking_Supervision#cite_note-1 [accessed 10 November 2010].

Katz E (2007) 'Implementation of the Third Money Laundering Directive – An Overview' www.anti-moneylaundering.org/Document/Default.aspx [accessed 10 November 2010].

Lewis BC (2004) 'Prevention of Computer Crime Amidst International Anarchy'
<https://litigationessentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctdoc=cite&docid=41+Am.+Crim.+L.+Rev.+1353&srctype=smi&srcid=3B15&key=f0bc8ed799ab7e1bf8276c3b80cc8f1a> [accessed 10 November 2010].

Lovet G (2009) 'Fighting Cybercrime: Technical, Juridical and Ethical Challenges' <http://whitepapers.hackerjournals.com/wp-content/uploads/2009/12/FIGHTING-CYBERCRIME.pdf> [accessed 7 August 2010].

Moshi PB (2007) 'Fighting Money Laundering: The Challenges in Africa'
se1.isn.ch/serviceengine/Files/ISN/98940/...8B54.../PAPER152.pdf
[accessed 1 October 2010].

Philippsohn S (2001) 'Money Laundering on the Internet'
<http://www.sciencedirect.com/science/article/B6V8G-44416WY-6/2/c6c2ea35a4f1db4dff547a9b36fe5ad>
[accessed on 15 March 2010].

Pieth M (2003) 'Anti-Money Laundering: Levelling the Playing Field'
<http://www.swissbanking.org/geldwaesche-brosh-03-06-05.pdf>
[accessed on 9 November 2010].

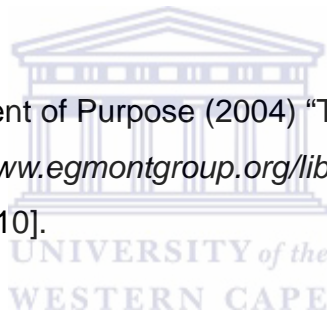
Public Accountants' and Auditors' Board (2003) 'Money Laundering Control: A Guide for Registered Accountants and Auditors'
www.paab.co.za/index.php?option=com_docman&task=doc
[accessed on 15 March 2010].

Shehu AY (2000) 'Money Laundering: The Challenge of Global Enforcement'
www.crime.hku.hk/moneylaundering.doc [accessed on 9 November 2010].

SWIFT (2010) 'Homepage'
http://www.swift.com/about_swift/company_information/index.page
[accessed 10 November 2010].

The Egmont Group (1999) '100 cases from the Egmont Group'
<http://www.fincen.gov/international/files/fiuiaction.pdf>
[accessed 10 November 2010].

The Egmont Group Statement of Purpose (2004) "The Egmont Group Statement of Purpose of June 2004" www.egmontgroup.org/library/download/4
[accessed 10 November 2010].



The European Convention on Cybercrime Explanatory Report
<http://conventions.coe.int/treaty/en/reports/html/185.htm>
[accessed 10 November 2010].