

Copyright and use of this thesis

This thesis must be used in accordance with the provisions of the Copyright Act 1968.

Reproduction of material protected by copyright may be an infringement of copyright and copyright owners may be entitled to take legal action against persons who infringe their copyright.

Section 51(2) of the Copyright Act permits an authorized officer of a university library or archives to provide a copy (by communication or otherwise) of an unpublished thesis kept in the library or archives, to a person who satisfies the authorized officer that he or she requires the reproduction for the purposes of research or study.

The Copyright Act grants the creator of a work a number of moral rights, specifically the right of attribution, the right against false attribution and the right of integrity.

You may infringe the author's moral rights if you:

- fail to acknowledge the author of this thesis if you quote sections from the work
- · attribute this thesis to another author
- subject this thesis to derogatory treatment which may prejudice the author's reputation

For further information contact the University's Director of Copyright Services

Telephone: 02 9351 2991 e-mail: copyright@usyd.edu.au



Anti-Money Laundering: A Risk Perspective

Zoë Ruth Lester

A thesis submitted in fulfilment of the requirements for the degree of Doctor of Philosophy

Discipline of Business Law Faculty of Economics and Business University of Sydney February 2010

Table of Contents

Can	didate's Declaration	iv		
Ack	nowledgements	v		
Abs	Abstract			
Glossary of Primary Terms and Acronyms				
1.	Introduction to a new political agenda and a new set of risk management			
	challenges	1		
1.1	A new era	1		
1.2	Money laundering defined	2		
1.3	The purpose of AML/CTF efforts and the shift towards risk-based regimes	4		
1.4	Risk management and meta monitoring	8		
1.5	Research aims, methodology and structure	11		
	1.5.1 Research questions, scope and methodology	11		
	1.5.2 Structure and presentation of research	14		
2.	Looking at money laundering through the lens of risk management	20		
2.1	The big picture	20		
2.2	How risk management has moulded approaches to AML	23		
	2.2.1 The birth of modern risk management (pre 1960s)	23		
	2.2.2 Beyond in-house insurance (the 1960s and 1970s)	24		
	2.2.3 A change in regulatory approach (the 1980s)	25		
	2.2.4 Risk management comes into its own (the 1990s)	27		
	2.2.5 Bang for their buck – The era of the risk-based approach (the 2000s)	29		
2.3	Risk perspectives	34		
2.4	Reputational risk	39		
2.5	Systemic risk	44		
2.6	Credit risk	48		
2.7	Operational risk	50		
2.8	Conclusion	53		
3.	Looking at AML/CTF legal risk through the lens of criminal law	56		
3.1	Introduction	56		
3.2	The concept of corporate criminal liability	58		
3.3	The high price of non-compliance	62		
	3.3.1 Show me the money: criminal fines for non-compliance	63		
	3.3.2 The imposition of imprisonment	70		
3.4		77		
	3.4.1 Widening the posts: The Money Laundering Control Act	79		
	3.4.2 A new regulatory era: The USA PATRIOT Act	81		
	3.4.3 Beyond AML/CTF compliance: Economic and trade sanctions	86		
3.5	Enforcement and AML/CTF legal risk	91		
	3.5.1 The stakes are raised: Increased enforcement	94		
	3.5.2 Tighter crime-fighting networks	96		
	3.5.3 The politics of enforcement	99		
26	Conclusion	102		

4.	Looking at AML/CTF legal risk through the lens of civil law	106 106				
4.1						
4.2	Civil liability & its associated penalties					
	4.2.1 Civil monetary penalties	110				
	4.2.2 Orders and agreements	113				
	4.2.3 Civil forfeiture	114				
	4.2.4 Shareholder derivative suits	116				
	4.2.5 International civil lawsuits	120				
4.3	Civil liability and extraterritorial AML/CTF laws	123				
4.4	When you can't even trust your own bank – financial institutions and					
	constructive trusts	127				
	4.4.1 The twin branches of constructive trust liability	129				
	4.4.2 Knowing assistance	130				
	4.4.3 Knowing receipt	132				
4.5						
	and civil law	134				
	4.5.1 Institutions' various contractual and legislative obligations	135				
	4.5.2 Competing contractual and legislative obligations	140				
	4.5.3 Resolving competing obligations	143				
4.6	Conclusion	150				
5.	Managing and mitigating AML/CTF legal risk	152				
5.1	Introduction	152				
5.2	Methods of managing AML/CTF legal risk	154				
5.3	Minimising the fallout from a compliance failure	158				
	5.3.1 Self-reporting to regulatory authorities	158				
	5.3.2 Deferred and non-prosecution agreements	162				
	5.3.3 Reliance on criminal defences	166				
	5.3.4 Mitigating factors affecting criminal penalties	169				
5.4	Conclusion	171				
6.	Riggs Bank: A criminal exception to civil regulation	174				
6.1	Introduction	174				
6.2	Corporate war crimes: Terrorism and corruption	175				
	6.2.1 Saudi Arabian accounts and the September 11 attacks	176				
	6.2.2 The September 11 lawsuits	179				
	6.2.3 Corruption, profiteering and a dictatorship	180				
	6.2.4 Civil penalties, civil lawsuits and stranded customers	183				
6.3	-	186				
	6.3.1 Repercussions in Spain	188				
	6.3.2 Repercussions in the U.S.	191				
6.4		194				
0.1	6.4.1 The souring of a significant commercial deal	194				
	6.4.2 Shareholder class actions	196				
6.5		199				
6.6	* * .	202				
_		401				
7.	Banco Delta Asia: USA PATRIOT Games	205				
7.1	Introduction B. D. L. A.:	205				
7.2	The beginning of the end for Banco Delta Asia	206				

	7.2.1 Banco Delta Asia's response to the allegations	211		
	7.2.2 The broader attack on Macau	212		
7.3	The fallout from the designation	214		
7.4	All for one and one for all: Unilateral sanctions	216 220		
7.5	PATRIOT Act politics			
	7.5.1 The involvement of North Korea	221		
	7.5.2 A trial with a jury (but without evidence)	224		
	7.5.3 Justification for the lack of evidence	225		
	7.5.4 Banco Delta Asia's legal position	228		
7.6	Risk implications	230		
	7.6.1 Risk management for institutions	232		
7.7	Conclusion	235		
8.	Conclusion	239		
8.1	The front line	239		
8.2	The importance of understanding and assessing ML/TF risk	240		
8.3	The diminishing risk of incurring criminal liability	243		
8.4	The increasing risk of incurring civil liability	246		
8.5	AML/CTF legal risk and enforcement	249		
8.6	Risk-based regimes in theory and practice	253		
	8.6.1 Benchmarking by regulatory authorities and institutions	253		
	8.6.2 Uncertainty around the nature and scope of risk-based requirements	255		
	8.6.3 The retrospective application of rules-based models	257		
	8.6.4 Risk-based approaches and terrorism financing	259		
	8.6.5 Self-regulation	260		
8.7	AML/CTF and the phenomena of risk	260		
9.	References	264		
9.1	Legislation	264		
9.2	Case law	265		
9.3	International instruments and guidance	267		
9.4	Books, articles and theses	267		
9.5	Official government reports and parliamentary testimony	273		
9.6	Other reports and press releases	275		
9.7	Conference papers and speeches	276		
9.8	News/magazine articles and media releases	279		
9.9	Other materials	286		

THE UNIVERSITY OF SYDNEY

Faculty of Economics and Business

CANDIDATE'S DECLARATION

I hereby declare that this thesis, entitled "Anti-Money Laundering: A Risk Perspective" and submitted for the degree of Doctor of Philosophy, contains no material that has been accepted for a degree or diploma at any other university or tertiary institution. This work, to the best of my knowledge and belief contains no material previously published or written by another person, except where due reference has been made in the text and bibliography.

Signed:	
Date:	

Acknowledgments

A number of people have been instrumental in enabling me to undertake – and successfully complete – this dissertation. At first instance, I would like to thank my primary supervisor, Dr. David Chaikin, for his enduring wisdom, professionalism and patience. David- I can never thank you enough for enduring my endless rewrites and Dickens-length emails (and for not pretending that an emergency had come up on those few occasions when I became so stressed that I was *very* close to tears in a public café!) I have learnt so much from you and I know we will remain firm friends years after the drafting of this document becomes a distant (albeit very fond) memory.

Sincere thanks must also go to my co-supervisor, Dr. Jason Sharman, without whose ongoing support and direction I would have stumbled on more than a few occasions. Jason- I am so grateful that you chose to continue supporting my studies even after moving during the early stages of my research. Despite living interstate, your constant availability and encouragement meant that you never felt very far away! Thank you for sticking with me, and going far above and beyond the call of duty.

In my work life, thanks is due to the dozens of banking and AML/CTF compliance professionals who generously shared their advice, guidance and time with me throughout the duration of this project.

Cam, Colin, Tab, Tori and Tim- if there were awards for 'Best Supporting Role in a PhD', you'd all be hot contenders! I am so grateful for your understanding when I cut short social engagements (or missed them altogether), and your patience when I spoke endlessly about the joys (and varied challenges) of writing a dissertation. Thank you for countering my 'ups and downs' with sympathy, understanding, good humour and friendship.

Finally, a hearty serve of gratitude must be dished out to my family. Mum and Dad, Georgi, Charley and Billy- words are not enough to convey how appreciative I am for your support and encouragement over the past few years. Thank you for somehow managing to put up with my PhD-influenced "moods" (read: borderline tantrums) every time my computer froze and/or my internet connection mysteriously failed just after Dad installed some new, fancy,

foreign software on his own computer!	We joke about it	, but I know I	could never h	ave done
this without you.				

This thesis is dedicated to my two beautiful grandmas, Grandma Kessler and Grandma 'Nanna' Sybil, for their inimitable warmth, wisdom, kindness and class ("the one thing you can't buy").

Abstract

Money laundering and terrorism financing are global crimes capable of transcending geographic boundaries. Increasingly sophisticated and transnational in nature, such crimes have the ability to inconspicuously exploit the differences between the laws, regulations and financial systems of different nation states. As such, they are capable of undermining the integrity of the global financial system, heightening the volatility of international capital flows, and destabilising financial institutions.

The events of 11 September 2001 (**September 11**) have had a profound impact on the way that many financial institutions must now conduct their business and manage their money laundering/terrorism financing (**ML/TF**) risk. The terrorist attacks carried out on that day generated unprecedented concern for money laundering and terrorism financing, and became the precursor for a raft of new institutional risk management obligations. They ushered in a new regulatory era and are responsible for the sizeable role that many institutions are now expected to play in protecting the sanctity of national and international financial systems.

Following the September 11 attacks, a number of national governments enacted risk-based Anti-Money Laundering/Counter-Terrorism Financing (AML/CTF) legislation. In recognising their role as gatekeepers of the international financial system, such legislation requires financial institutions to proactively assess their own levels of ML/TF risk, and implement appropriate systems and controls commensurate to that risk. Typically, these systems and controls must include an AML/CTF compliance program, customer due diligence procedures, AML/CTF training, transaction monitoring and regulatory reporting.

Whilst there has been much rhetoric about the risks that institutions face when operating under risk-based AML/CTF regimes, there is seemingly little evidence to support it. Many commentators have held that any involvement in a money laundering or terrorism financing event will carry disastrous, financially debilitating, and at times irreversible consequences for an organisation. However, when the experiences of institutions operating in the U.S. and the U.K. (two of the most developed and long-standing AML/CTF regimes) are reviewed, these claims appear to be largely unfounded.

Whilst there are certainly a number of financial, reputational and legal consequences that may stem from an institution's breach of AML/CTF legislation, these consequences appear to be significantly overstated – least of all by financial institutions themselves. During the past few years, a number of regulatory and law enforcement authorities have deliberately shifted their activities away from the initiation of criminal proceedings, towards the use of cooperative regulatory outcomes and agreements. Thus, the level of risk faced by many institutions is certainly not as pronounced as it was several years ago, in the immediate aftermath of September 11.

That is not to say that financial institutions will always have the ability to avoid the legal penalties, financial loss and reputational damage attached to an AML/CTF compliance failure. Indeed, there are some notable limitations on the ability of institutions to manage their risks, and an unmitigated risk exposure can translate into domestic and/or extraterritorial enforcement actions. Even in risk-based regimes where regulatory authorities display a preference for less intrusive, more cooperative outcomes, decisive action may nevertheless be taken against institutions that have committed legislative contraventions considered to be pervasive, unresolved, or of serious regulatory concern.

A greater understanding of risk-based approaches to AML/CTF can enrich institutional understandings of the phenomena of risk. By gaining greater knowledge about the types and levels of risk apparent in several risk-based regimes, institutions may be better placed to identify and address their individual risk exposures. Further, they may be better able to determine the likely ramifications associated with any breach of risk-based legislative requirements. Without such an acute understanding of the operation of risk-based approaches, institutions may find themselves adopting flawed risk management strategies, spending copious amounts of money on poorly designed AML/CTF controls, and/or otherwise taking steps to undermine the alleged benefits of risk-based regimes – flexibility, cost-effectiveness, and enhanced engagement with the concepts of AML and CTF.

Glossary of Primary Terms and Acronyms

AML Anti-Money Laundering – laws, regulations, rules and practices

associated with combating the crime of money laundering.

AML/CTF Act Anti-Money Laundering and Counter-Terrorism Financing Act

2006 (Cth) – Australia's primary piece of AML/CTF legislation

became effective on 13 December 2006.

AML/CTF Compliance Anti-Money Laundering/Counter-Terrorism Financing

Officer Compliance Officer – under the AML/CTF Act, all regulated

entities must nominate an individual to independently oversee

their AML/CTF compliance.

AML/CTF Program Anti-Money Laundering/Counter-Terrorism Financing Program

> - under many AML/CTF regimes, regulated entities must implement an AML/CTF program that involves undertaking certain levels of customer due diligence, screening employees

and training staff.

APGML Asia-Pacific Group on Money Laundering – a regional

> organisation concerned with assessing the AML/CTF compliance of member states, coordinating AML/CTF technical

assistance and training, and conducting research into ML and TF

trends.

AUSTRAC Australian Transaction Reports and Analysis Centre – Australia's

FIU and federal AML/CTF regulator.

Bank Secrecy Act of 1970 – a U.S. Act that requires U.S. **Bank Secrecy Act**

financial institutions to assist U.S. government agencies to detect

and prevent money laundering.

Basel Committee Basel Committee on Banking Supervision – an international

organisation that seeks to foster cooperation around, and an

understanding of, banking supervisory matters.

Correspondent A banking relationship established to receive deposits from,

make payments on behalf of, or handle other financial

transactions related to, a foreign financial institution.

CTF Counter-Terrorism Financing – laws, regulations, rules and

practices associated with countering the crime of terrorism

financing.

Banking

Constructive Trust A trust that arises by operation of law where an individual or

> institution that has not been appointed as a trustee, nevertheless invokes the liabilities of trusteeship by conducting themselves as

trustees in relation to certain property.

Egmont Group The peak body for FIUs such as AUSTRAC, regulated entities

may decide to use membership of the Egmont Group as one

factor in measuring jurisdiction risk.

Employee Due Diligence

FATF

A risk-based process that generally involves collecting and verifying (and potentially re-verifying) information about an employee, and monitoring their compliance with organizational AML/CTF standards.

Financial Action Task Force – an inter-governmental body that sets standards, and develops and promotes policies relating to

FATF 9 Special Recommendations AML/CTF. Its 40+9 Recommendations are now regarded as international best practice standards for the management of AML/CTF.

Nine special recommendations made by FATF specifically in

relation to the management of CTF.

40 Forty recommendations made by FATF in relation to the

FATF 40 Recommendations

jurisdictional, regulatory and institutional management of AML.

FATF 40+9 A reference to both the FATF's 40 Recommendations and 9 Special Recommendations.

FinCEN Financial Crimes Enforcement Network – an agency established to enhance U.S. national security, deter/detect criminal activity, and safeguard financial systems from abuse.

FIU Financial Intelligence Unit – a central, national agency responsible for receiving, processing, analysing and disseminating information relating to threshold and suspicious transactions.

KYC Know Your Customer – the process of collecting and verifying (and potentially re-verifying) information about a customer in order to reasonably ensure that they are who they represent themselves to be.

MAM Monetary Authority of Macau – a statutory body established to exercise the functions of a central monetary depository, and monitor the stability of Macau's currency and financial system.

MLCA Money Laundering Control Act of 1986 – a U.S. Act that criminalised money laundering as a federal offence.

MLRO Money Laundering Reporting Officer – an individual working for a U.K. regulated entity who is nominated to oversee aspects of the entity's AML/CTF compliance (including the filing of SARs).

ML/TF Risk Money Laundering/Terrorism Financing Risk – the risk that providing financial products/services may facilitate money laundering or terrorism financing activities.

Money Laundering The process of trying to "clean" the proceeds of crime by placing them in the financial system and disguising their source through layers of different transactions, so they can be accessed legitimately thereafter.

Office of Foreign Assets Control - an agency established to **OFAC** administer and enforce economic and trade sanctions based on U.S. foreign policy and national security goals.

PEP Politically Exposed Person – Any individual who is or who has been entrusted with prominent public functions in a foreign country. This includes foreign Heads of State, senior politicians, and important political party officials.

Prescriptive Requirements Legislative AML/CTF requirements that operate, and must be complied with, irrespective of an organisation's ML/TF risk.

Regulated Entity Any individual or legal person that falls under the ambit of AML/CTF legislation.

A regulatory and legislative approach that requires regulated Risk-Based Approach entities to design and implement appropriate risk-based systems and controls. What is appropriate in each case will depend upon a regulated entity's size, complexity, and levels of ML/TF risk.

Legislative AML/CTF requirements that empower regulated Risk-Based entities to consider their ML/TF risk profiles when determining Requirements how to meet their compliance obligations.

SAR Suspicious Activity Report – a report filed by regulated entities with an FIU, to communicate any suspicions around a customer's identity, transactional behaviour, or potential connection to crimes such as money laundering and terrorism financing.

A bank that does not have a physical presence (for instance, a place of business that is located at a fixed address) in any country.

Multilateral negotiations conducted in 2005/2006 with the aim of dismantling North Korea's nuclear weapons development program.

Directly or indirectly providing or collecting funds with the intention/knowledge that they will be used to finance acts of terrorism, or persons associated with terrorists and terrorist organisations.

Three bases of risk – the title used by some banking and AML/CTF professionals to collectively refer to customer risk, product/channel risk and jurisdiction risk.

These cash transactions, which involve at least a specified amount of funds, must be reported to the local FIU within a specified time frame.

The criminal offence of disclosing information about the fruition of a suspicion, or the filing of a SAR.

Systems and/or controls intended to monitor customers' transactional behaviour for the purposes of identifying any suspicious activities.

Shell Bank

Six-party Talks

Terrorism Financing

Three bases

Threshold **Transactions**

Tipping off

Transaction Monitoring **U.K. FSA** United Kingdom Financial Services Authority – a statutory body

established to maintain market confidence, protect consumers

and reduce financial crime.

USA PATRIOT Act Uniting and Strengthening America by Providing Appropriate

Tools Required to Intercept and Obstruct Terrorism Act of 2001 – a U.S. Act that expands the AML/CTF compliance obligations placed upon U.S. regulated entities, and the investigative,

information-sharing and enforcement powers of regulatory/law

enforcement bodies.

Wolfsberg Group An association of twelve global banks that aims to develop

common, industry standards in relation to KYC and AML/CTF.

Chapter 1

Introduction to a New Political Agenda and a New Set of Risk Management Challenges

"The War on Terrorism will not be fought on the battlefield... (It will be) fought in the halls of our financial institutions" – Andrew M. Ayers

1.1 A new era

Money laundering and terrorism financing are global crimes capable of transcending geographic boundaries. Increasingly sophisticated and transnational in nature, such crimes have the ability to inconspicuously exploit the differences between the laws, regulations and financial systems of different nation states. As such, they are capable of undermining the integrity of the global financial system, heightening the volatility of international capital flows, and destabilising financial institutions. Both money laundering and terrorism financing entrench crime by enabling individuals to abuse financial institutions and other entities for the purposes of disguising crimes they have already perpetrated, or are yet to commit.

The events of 11 September 2001 (**September 11**) provide a confronting and inescapable example of the damage that money laundering and terrorism financing can cause when translated into physical, human acts.² Accordingly, the attacks carried out on that day have had a profound impact on the way that many financial institutions must now conduct their business and manage their money laundering/terrorism financing (**ML/TF**) risk. They were the precursor for a raft of new institutional risk management obligations, and are responsible for the sizeable role that many financial institutions are now expected to play in protecting the sanctity of national and international financial systems.

¹ International Monetary Fund, The IMF and the Fight against Money Laundering and the Financing of Terrorism: A Factsheet (2005) http://www.imf.org/external/np/exr/facts/aml.htm at 17 May 2006.

² Godse, V., Anti-Money Laundering, L&T Infotech Confidential 2

http://202.81.207.25/Intinfotech/WhitePapers/AML%20Whitepaper.pdf at 15 June 2007.

September 11 generated unprecedented concern for money laundering and terrorism financing. Although such crimes had previously received some attention from various national and international bodies, it was not until 2001 that a new regulatory era was ushered in and Anti-Money Laundering/Counter-Terrorism Financing (AML/CTF) issues were thrust at the top of the international political agenda. Following the September 11 terrorist attacks, national governments became acutely aware of the fact that the success of their efforts to curb money laundering and terrorism financing hinged largely on the cooperation of financial institutions. In recognising their role as gatekeepers of the international financial system, a number of governments began to make institutions equal partners in AML/CTF regulation. They enacted risk-based AML/CTF legislation and, in many instances, required institutions to start assessing, monitoring, mitigating and managing their individual levels of ML/TF risk for the first time.

1.2 Money laundering defined

As noted by Thomas J in *Humberto Fidel Regalado Cuellar v. United States*, 553 U.S. (2008), legal definitions of money laundering have at times varied widely. Whilst some legal texts have broadly defined money laundering as the process by which the source or nature of illegal funds is disguised, others have defined it more narrowly as "[t]he act of transferring illegally obtained money through legitimate people or accounts so that its original source cannot be traced". To the extent that such legal definitions have been inconsistent, U.S. courts have typically been guided by the wording of the relevant statutory provisions, rather than any common meaning attributed to the process of money laundering.⁴

According to a number of commentators, the last few decades have seen the definition of money laundering significantly widened. They argue that since the enactment of the *Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970* (31 U.S.C. § 1051, et seq.) (Bank Secrecy Act) by the U.S. legislature, the definition of money laundering has departed from its original conceptualisation and been expanded to

³ Garner, B.A., Black's Law Dictionary (8th ed, 2004) 1027.

⁴ For instance, see Pennsylvania Dept. of Corrections v. Yeskey, 524 U. S. 206, 212 (1998).

"cover almost any financial crime". At first glance, the observations of these commentators certainly appear to be correct. As U.S. prosecutors have tried to aggressively interpret and apply money laundering charges (which typically carry far greater penalties than similar charges, such as bulk cash smuggling), the past few years have seen a plethora of criminal activities caught "in the penumbra of money laundering charges". In many instances, the original drafters of U.S. money laundering legislation could not have foreseen the breadth of the criminal activities that may now fall within legislative definitions of money laundering. Whilst cases such as Humberto Fidel Regalado Cuellar v. United States have recently sought to clarify the boundaries of particular money laundering definitions and offences, their impact on future money laundering cases is yet to be seen.

In contrast to potentially complex legal interpretations of money laundering, operational and regulatory definitions are typically clearer and less contentious. Whilst a number of regulatory authorities, including the U.K. Financial Services Authority (**U.K. FSA**), define money laundering relative to their domestic criminal laws and AML/CTF legislation, ⁸ others appear to be comfortable using less technical and more operational definitions of money laundering.

By way of example, Australia's AML/CTF regulator, the Australian Transaction Reports and Analysis Centre (AUSTRAC), simply defines money laundering as "the process by which illegally obtained funds are given the appearance of having been legitimately obtained". Unless otherwise stated, it is this regulatory definition of money laundering that will be used throughout this thesis. Apart from avoiding the potential vagueness around, and divergence between, different legal definitions of money laundering, the use of such an operational definition has greater utility with respect to the identification and investigation of money

⁵ Androphy, J., 'The Government's Dirty Laundry', Forbes, No. 7, 7 April 2008.

⁶ Carrol, D., 'Ambiguity in Contemporary Money Laundering Statutes' (2008) *Illinois Business Law Journal* http://iblsjournal.typepad.com/illinois_business_law_soc/2008/04/i-introductio-2.html at 27 July 2008.

⁷ Op cit n5.

⁸ In its Handbook on Financial Crime, Market Abuse and Money Laundering, the U.K. FSA narrowly defines money laundering to be any act which constitutes an offence (or aiding, abetting, counselling or procuring an offence) under certain provisions of the Terrorism Act 2000 (U.K.) and/or the Proceeds of Crime Act 2002 (U.K.).

See Australian Transaction Reports and Analysis Centre, Introduction to AML/CTF
http://www.austrac.gov.au/elearning/mod1/mod1/mod1/money-laundering-3.html at 27 July 2008.

laundering activities by regulatory and law enforcement bodies. Given both its breadth and its simplicity, it recognises that conduct which may be criminally considered to be money laundering in one country may in fact be legal in another. ¹⁰

Apart from its ease of reference, the use of an operational definition is seemingly more valuable for the purposes of discussing risk-based approaches to AML/CTF. Such approaches are not concerned with how institutions can legally or technically escape culpability in relation to a money laundering offence, but rather how they can effectively implement systems and controls to counter money laundering activities. Accordingly, the use of an operational definition of money laundering will more closely align with the interpretations given to it by many compliance professionals and AML/CTF practitioners. These individuals are typically less concerned with cleverly drafted legal definitions, and more concerned with broader, working definitions which they can operationalise for the purposes of designing internal risk management controls.

1.3 The purpose of AML/CTF efforts and the shift towards risk-based regimes

Given that money laundering and terrorism financing are, fundamentally, flows of funds intended to legitimise monies related to criminal activities (whether or not those activities have already occurred or are yet to occur), it may be argued that – in and of themselves – they are not important harms. As distinct from predicate offences¹¹ and terrorist acts, the 'victims' of money laundering and terrorism financing can often be difficult to identify. Accordingly, it is apparent that the significant AML/CTF efforts undertaken by national governments, regulatory authorities, law enforcement officials and financial institutions in the past few decades, have not solely been geared towards combating these two crimes.

¹⁰ See Chaikin, D., 'Investigating Criminal and Corporate Money Trails' in Fisse, B., Fraser, D., and Coss, G. (eds), *The Money Trail: Confiscation of the Proceeds of Crime, Money Laundering and Cash Transaction Reporting* (1992) 257.

For the purposes of this thesis, a "predicate offence" is defined as the underlying criminal activity that generates proceeds which, when laundered, result in the offence of money laundering. See Schott, P.A., Comprehensive Reference Guide to AML/CTF, World Bank 3

http://www1.worldbank.org/finance/html/amlcft/docs/Ref_Guide_EN/v2/01-Ch01_EN_v2.pdf at 20 December 2008.

A number of regulatory officials, commentators and academics have held that AML/CTF efforts have a number of goals that are far broader than the prevention, identification and prosecution of money laundering and terrorism financing activities. They contend that, primarily, AML/CTF efforts are geared towards the reduction of predicate offences, the protection of financial integrity, and the countering of 'public bads' such as terrorism. ¹² Subsidiary to these goals is the desire for AML/CTF regimes and regulations to inconvenience criminals and terrorists, and render their activities more arduous to orchestrate. Thus, it may be contended that when financial institutions breach applicable AML/CTF legislation, they are not only falling short of their statutory obligations but also committing a public disservice; undermining the attempts of regulatory, law enforcement and government officials to detect, disrupt and deter criminal acts.

Given the importance of AML/CTF efforts, they have become the subject of sustained interest in the aftermath of September 11 terrorist attacks. ¹³ International organisations such as the Financial Action Task Force (**FATF**), Basel Committee on Banking Supervision (**Basel Committee**) and Wolfsberg Group have promulgated a number of best practice standards with respect to the management of money laundering and terrorism financing, and the mitigation of ML/TF risk. In order to incorporate these best practice standards into their municipal legislation, a number of national governments have built risk-based concepts into their AML/CTF statutory definitions and mechanisms. ¹⁴ The result of this has been a deliberate shift away from purely prescriptive AML/CTF regimes, towards risk-based approaches and models of regulation.

In contrast to risk-based approaches to AML/CTF, prescriptive regulatory regimes have often been criticised for their perceived inflexibility, expense and emphasis on legalism rather than regulatory effectiveness.¹⁵ Often considered to be rigid in terms of their requirements,

¹² Reuter. P., 'Assessing the Effects of the AML Regime: Identifying Success, the Relevant Outcomes and Metrics' (Speech delivered at the Anti-Money Laundering and Counter-Terrorism Financing Conference 2009, Sydney, 1 April 2009).

¹³ Stessens, G., Money Laundering: A New International Law Enforcement Model (2008) 84.

¹⁴ Ross, S., and Hannan, M., 'Money Laundering Regulation and Risk-Based Decision-Making' (2007) 10(1) Journal of Money Laundering Control 106.

¹⁵ See Hutter, B.M., The Attractions of Risk-Based Regulation: Accounting for the Emergence of Risk Ideas in Regulation (Discussion Paper 33, London School of Economics and Political Science, London, 2005).

prescriptive approaches to AML/CTF are generally more preoccupied with detailed rules than regulatory outcomes. Unlike risk-based regimes, they set clear legislative expectations for all institutions, regardless of their size, scope of operations, customer base and levels of ML/TF risk. They do not pivot upon the concept of risk, they do not require institutions to assess their own levels of risk, and they certainly do not empower entities to design and implement controls specifically tailored to such risk. As such, they can inadvertently give rise 'tick box' approaches, with institutions focussing more on meeting regulatory demands than combating money laundering or terrorist financing activities.¹⁶

Whilst some regulatory initiatives have previously seen financial institutions placed at the forefront of government efforts to combat money laundering, risk-based approaches to AML/CTF have cemented their position there. They require institutions to proactively identify their own levels of ML/TF risk, and implement systems and controls commensurate to that risk (i.e. over and above a number of minimum legislative requirements). Typically, these systems and controls must include an AML/CTF compliance program, customer due diligence procedures, transaction monitoring and formal regulatory reporting.

Institutions operating under risk-based AML/CTF regimes are neither required, nor expected, to entirely safeguard their businesses from exploitation at the hands of money launderers or terrorism financiers. Risk-based approaches implicitly accept that crime cannot be totally eliminated in a free society, and that institutions will always face a certain degree of ML/TF risk. ¹⁷ Accordingly, they do not seek to entirely eradicate institutions' ML/TF risk. Rather than expecting entities to implement 'zero-failure' controls, such approaches acknowledge the legal and operational limits on the ability of institutions to control their ML/TF risk. They simply seek to ensure that institutions identify their respective levels of ML/TF risk and implement systems and controls stylised to that risk.

Financial Action Task Force, Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing – High Level Principles and Procedures (2007) Organisation for Economic Cooperation and Development 2 http://www.oecd.org/dataoecd/43/46/38960576.pdf at 29 April 2008. The FATF itself has recognised that despite the best efforts of financial institutions, money launderers will at times succeed in moving illicit funds through the financial sector undetected. See Financial Action Task Force, Op cit n16, 3.

Under risk-based approaches to AML/CTF, financial institutions generally assess their levels of ML/TF risk by looking at their customer risk, product/channel risk and jurisdiction risk. Whilst the individual or collective weight given to these three risk criteria will vary amongst regulated entities, it is believed that by assessing their ML/TF risk in terms of these three risk types, financial institutions will be able to identify – and gear their resources towards – the most vulnerable parts of their business. Indeed, the fundamental premise of risk-based approaches is that the implementation and enforcement of AML/CTF laws should be tailored to institutions' individual ML/TF risk profiles.

Often considered critical to the "effective and proportionate functioning" of countries' AML/CTF regimes, ¹⁸ risk-based approaches not only drive the way that institutions discharge their AML/CTF obligations, but also the way in which regulatory authorities carry out their functions. ¹⁹ Just as risk-based approaches do not anticipate that financial institutions will be able to prevent all instances of money laundering/terrorism financing, they do not expect that regulatory authorities will be capable of preventing the failure of all financial institutions. According to the U.K. FSA, it is not only unavoidable that some institutions should fail, but also "undesirable because reward and risk are linked, and an attempt to control risk to the extent of preventing all financial failure would unreasonably constrain financial institutions". ²⁰

Whilst prescriptive regulatory approaches generally see government resources applied evenly across all regulated entities, risk-based approaches allow regulatory authorities to use their resources more effectively by diverting them to those institutions/industries deemed to represent a greater ML/TF risk. Whilst size is not the sole criterion that regulatory authorities will use to determine the ML/TF risk represented by an institution, it is nevertheless an important indicator. At the very least, an institution's size will often be indicative of the diversity in its product offerings/customer base, and the potential consequences that its

¹⁸ Ihid

¹⁹ United Kingdom Financial Services Authority, A Risk-Based Approach to Anti-Money Laundering Supervision in the U.K. (2008) 1

< http://www.fsa.gov.uk/pages/About/What/financial_crime/pdf/amlsf_mar08.pdf> at 20 January 2009.

McCarthy, C., 'Risk Based Regulation: The FSA's Experience' (Speech delivered via videolink to the Australian Securities & Investment Commission, Sydney, 13 February 2006).

failure may have for customers, employees, other institutions and, in some circumstances, a country's economy.

Indeed, risk-based regulation typically sees regulatory authorities spending more time on larger institutions and those that have previously experienced significant AML/CTF compliance failures (i.e. committed notable breaches of AML/CTF legislation). Whilst institutions deemed to represent a higher risk will often attract "close and continuous" regulation,²¹ those representing a much lower risk will generally only be subject to periodic, themed reviews and ad hoc regulatory engagement.

1.4 Risk management and meta monitoring

According to the International Organisation for Standardisation (**ISO**), 'risk' is the "effect of uncertainty on objectives" or, phrased another way, the likelihood that a particular event may happen and the degree of damage or loss that may result from its occurrence.²³ Following on from this:

- 'risk assessment' is considered to be the overall process of identifying, analysing and evaluating risks;²⁴ and
- 'risk management' is regarded as the process of addressing uncertainty²⁵ by identifying,
 assessing and prioritising risks, and applying resources to minimise, monitor and control them.²⁶

Although risk has long been integral to ways of thinking about money laundering, it is only during the past decade that the concepts of 'risk', 'risk assessment' and 'risk management' have become central components of achieving AML/CTF compliance.²⁷ Whilst not formally

²¹ Ibid.

International Organization for Standardization, Committee Draft of ISO 31000 Risk Management (2009) 1 http://www.npc-se.co.th/pdf/iso31000/ISO FDIS 31000 (E).pdf> at 6 October 2009.

See International Organization for Standardization, Risk Management – Vocabulary – Guidelines for Use in Standards (2002).

²⁴ Op cit n22, 4.

²⁵ Op cit n22, 7.

²⁶ Hubbard, D., The Failure of Risk Management: Why It's Broken and How to Fix It (2009) 46.

²⁷ Op cit n14, 107.

defined in the risk management literature produced by organisations such as the ISO, the terms 'ML/TF risk' and 'ML/TF risk assessment' have now become common parlance amongst many risk management and AML/CTF compliance professionals. Although two of the peak international AML/CTF bodies, the FATF and the Wolfsberg Group, have yet to specifically define these terms (despite referencing them heavily in their publications and best practice standards for addressing money laundering and terrorism financing), ²⁸ international consensus has been building regarding their meaning. Indeed, the need for clarity around the concept of ML/TF risk and ML/TF risk assessment has only become more pronounced with the growing popularity of risk-based regulatory approaches.

In accordance with the concept of the 'risk society' devised by Ulrich Beck, risk-based approaches have effectively seen AML/CTF compliance reflexively remade into a risk paradigm. In jurisdictions with risk-based regimes, the activities of regulatory authorities have shifted steadily towards "externally monitored self-coordination".²⁹

To use terms coined by academics John Braithwaite and Peter Grabosky, risk-based approaches to AML/CTF seemingly foster a regulatory environment characterised by 'meta risk management' and 'meta monitoring'. ³⁰ In jurisdictions with risk-based regimes, regulatory authorities generally appear to be regulating institutions' self-regulation. Rather than necessarily enforcing legislative requirements directly, many regulatory officials are now simply ensuring that institutions are internally monitoring, reviewing and enforcing compliance with their AML/CTF legislative obligations. Institutions are expected to be largely self-auditing, with regulatory authorities maintaining the ability to monitor, review and redesign their internal risk management controls, as appropriate. In many ways, risk-based approaches to AML/CTF have seen the 'regulated' become the 'regulating'.

²⁸ For instance, in its report "Risk-Based Approach: Guidance for Money Services Businesses", the FATF refers to the concept of ML/TF risk no less than nine times, but neglects to define the term (along with the many others its defines) in the document's glossary. See Financial Action Task Force, *Risk-Based Approach: Guidance for Money Services Businesses* (2009) < http://www.fatf-gafi.org/dataoecd/45/1/43249256.pdf> at 7 October 2009.

²⁹ Beck, U., Risk Society: Towards a New Modernity (1992) 232.

³⁰ See Braithewaite, J., 'Meta Risk Management and Responsive Governance' (Paper presented at the Risk Regulation, Accountability and Development Conference, Manchester, 26 June 2003).

Given this transfer of responsibility from regulatory authorities to financial institutions, the effectiveness of risk-based regulation may depend upon the existence of a clear understanding of how various ML/TF risks should be assessed, prioritised and mitigated.³¹ However, such an understanding may at times be elusive or difficult to achieve, considering that ML/TF risk can be framed in one or more of the following ways:

- probabilistic risk the risk represented by the strength of the relationship between certain attributes (for instance, identity fraud) and a money laundering/terrorism financing event or activity;
- consequence risk the risk represented by the potential seriousness of a money laundering/terrorism financing event or activity; and
- regulatory risk the risk represented by an institution's vulnerability to a money laundering/terrorism financing event or activity.³²

The emphasis placed on the three abovementioned constructions of ML/TF risk by an individual or entity, may depend upon their position within the broader regulatory system.³³ For instance, given their varying aims and responsibilities, regulatory officials, law enforcement authorities and financial institutions may invariably focus on very different types of risks and institutional behaviours. Whilst law enforcement officials might be primarily concerned with those activities that are associated with important predicate offences (probabilistic risk), regulatory authorities may focus on those business areas/functions that are easier to subvert and/or more difficult to monitor (regulatory risk). Further, whilst financial institutions must necessarily have regard to all three constructions of ML/TF risk, some may gear their compliance efforts towards identifying and managing those activities that carry the most financial, reputational and/or legal risk (consequence risk).

Nevertheless, despite the divergence that might exist between the way that different individuals and entities construct ML/TF risk, risk-based regimes require regulatory authorities to understand how institutions frame, assess and manage their levels of ML/TF risk. Indeed, one premise of risk-based approaches is that regulators should judge the

³¹ Op cit n14, 114.

³² Op cit n14, 110.
³³ Op cit n14, 111.

proportionality and appropriateness (or otherwise) of an institution's AML/CTF controls in light of its ML/TF risk profile and the manner in which it has assessed its risk. This is the regulatory flexibility that has previously seen risk-based AML/CTF approaches replace more prescriptive, mechanical approaches to AML/CTF regulation and compliance.

1.5 Research aims, methodology and structure

1.5.1 Research questions, scope and methodology

Through the use of qualitative research techniques, this thesis seeks to assist in an understanding of the phenomenon of risk.³⁴ By synthesising and collating a significant number of materials in a new way, it seeks to improve the risk identification, assessment, evaluation³⁵ and treatment³⁶ activities of financial institutions by answering the following research questions:

- what are the various types of risk that institutions may face (either locally or extraterritorially) when operating in jurisdictions with risk-based approaches to AML/CTF;
- what are some of the more likely consequences of non-compliance with AML/CTF legislation;
- have the risks and consequences commonly associated with non-compliance been misrepresented or otherwise overstated/understated; and
- what are the practical approaches and strategies that institutions can employ to manage their ML/TF risk and/or mitigate the fallout stemming from any money laundering or terrorism financing event?

³⁴ For a discussion on the advantages and potential limitations of using qualitative research techniques, see Moll, J., Major, M., and Hoque, Z., 'The Qualitative Research Tradition', Chapter 18 in Hoque, Z. (ed), *Methodological Issues in Accounting Research: Theories and Methods* (2006) 375.

³⁵ Based on the outcomes of risk analysis/assessment activities, 'risk evaluation' seeks to assist in making decisions about which risks need treatment and should be prioritised in terms of treatment implementation. See International Organization for Standardization, Op cit n22, 18.

³⁶ 'Risk treatment' involves selecting one or more options for modifying risks, and implementing those options. Examples of risk treatment options include avoiding the risk, taking or increasing the risk, removing the risk source, and sharing the risk with other parties. See International Organization for Standardization, Op cit n22, 19.

Given the nature of money laundering and terrorism financing activities, and the lack of reliable statistics available in relation to both the prevalence of such crimes and the number of institutions formally reprimanded for AML/CTF compliance failures, ³⁷ quantitative research methods were deemed to be unsuitable for the purposes of this research. Accordingly, this thesis relies heavily upon qualitative research techniques. It draws upon both primary materials (including AML/CTF legislation and court documents) and secondary, supporting materials (such as journal and newspaper articles). Aside from drawing on personal industry insights gained through years of experience as both an AML/CTF consultant and an AML/CTF Compliance Officer for a large Australian retail bank, this thesis relies on informal discussions with AML/CTF and banking professionals to provide clarity and context around the otherwise unchecked and untested claims of some commentators.

Though this thesis tends to address the issues of money laundering and terrorism financing simultaneously, the clear focus is on money laundering and the applicability of risk-based approaches to AML. As discussed in subsequent Chapters of this thesis, the inherent nature of terrorism financing renders it difficult for institutions to proactively detect, identify and address. Though risk-based regimes are typically held to apply to both AML and CTF, the inability of regulated entities (and indeed, regulatory authorities) to identify transactions that might relate to future acts of terrorism, certainly limits their applicability – and the applicability of this research – to issues solely relating to CTF.

Whilst the research contained herein is primarily concerned with the consequence risk and regulatory risk apparent in several risk-based regimes, it does not seek to provide a detailed evaluation of the relative success or appropriateness of those regimes. Such analysis falls outside the scope of this thesis and should be the subject of further research. Nevertheless, by assessing the potential ramifications attached to non-compliance with AML/CTF legislation, some reflections on the apparent effectiveness of risk-based approaches can be made. These relate to the levels of visible regulation in risk-based regimes, the alignment between such

As noted in subsequent Chapters of this thesis, in many jurisdictions enforcement proceedings for breaches of AML/CTF legislation can remain confidential and shrouded in secrecy.

regulation and risk-based legislative provisions, and the extent to which risk-based regimes actually fulfil their desired aims and objectives.

Given that they are two of the most developed and long-standing risk-based AML/CTF regimes, this thesis significantly focuses on the U.S. and the U.K. As opposed to less developed and more nascent regimes, both jurisdictions have seen several iterations of their AML/CTF laws, a development of their regulatory environments, and the initiation of several AML/CTF enforcement actions. Whilst this thesis contains discussion on the emerging AML/CTF regimes in Australia and a number of other Asia-Pacific nations, the U.S. and the U.K. provide a wealth of information relevant to the analysis of the levels and types of risk faced by institutions operating under risk-based approaches to AML/CTF. Both jurisdictions have some of the most onerous and visibly enforced AML/CTF laws, as well as some of the strongest legislative expressions of extraterritoriality. They have not only hosted many of the most highly publicised AML/CTF enforcement actions, but have also seen some of the more damaging penalties given to institutions for such breaches.

This thesis primarily considers the concept of ML/TF risk, as well as the operation of various AML/CTF regimes, from an *institutionalist* perspective. Accordingly, much of the analysis contained herein is limited to financial institutions. Defined broadly to encompass all types of corporate organisations involved in the provision of financial products/services, "financial institutions" have often been expected to act as the first line of defence in government efforts to curb money laundering and terrorism financing. They have often been subject to the most expansive AML/CTF requirements, and been key players (either actively or passively) in some of the most notable money laundering operations. As such, the risks faced by financial institutions operating under risk-based approaches to AML/CTF are more visible and readily assessable than the risks faced by organisational types not commonly considered to be conduits for financial crime.

1.5.2 Structure and presentation of research

Through the use of a detailed literature review, this thesis begins by charting the development of risk management as an independent discipline and, more specifically, its application to the concepts of AML and CTF. **Chapter 2** details the growing emergence of risk-based approaches to AML/CTF, and explains why they are often considered to be the "best possible means by which to identify potential money laundering" and the "most effective and relevant response to the way in which [a] business operates". By providing an introduction to the concept of ML/TF risk and attempting to contextualise such risk in terms of older, more traditional risk types, the Chapter seeks to identify the various risks that institutions may face when operating under risk-based AML/CTF regimes. Whilst it ultimately acknowledges that the concept of ML/TF risk will not always fit neatly within the confines of traditional risk types, the Chapter asserts that attempting to frame it in such a way may better enable institutions to:

- identify their AML/CTF-related risk exposures; and
- quantify the potential consequences of a money laundering/terrorism financing event,
 and/or an AML/CTF compliance failure.

In addition to contextualising the concept of ML/TF risk in terms of several traditional risk types, **Chapter 2** outlines the oft-cited consequences of an AML/CTF compliance failure. It notes that during the past decade, many commentators and industry participants have claimed that institutions connected to money laundering or terrorism financing activities (whether or not due to their ineptitude, malfeasance or bad luck)³⁹ are likely to incur significant financial damage and irreparable reputational damage.⁴⁰ It observes that others still have held that in

³⁸ SAS Institute and Lepus, Anti-Money Laundering Reappraised: The Benefits of a Holistic, Risk Based Approach (2006) West Coast Anti-Money Laundering Forum 28 < http://www.wcamlforum.org/pdf/Anti-Money%20Laundering%20Reappraised%20-%20SAS%20-%202006-05.pdf> at 30 April 2008.

Harris, R., Picking Up the Pieces (2004) CFO Magazine

<http://www.cfo.com/printable/article.cfm/3015379?f=options> at 19 April 2006.

⁴⁰ PricewaterhouseCoopers, Anti-Money Laundering: A Global Financial Services Issue (2005) http://www.pwc.com/extweb/pwcpublications.nsf/docid/E8069E5A5B82FDDD8525706F00567905/\$file/aml.pdf at 1 April 2006.

more severe cases, an institution associated with poor AML/CTF controls or the active facilitation of money laundering/terrorism financing might even face closure.⁴¹

Whilst there appears to have been an almost unquestioned acceptance of the claims that any involvement in a money laundering or terrorism financing event will carry disastrous and, at times, irreversible consequences for an institution, **Chapters 3 and 4** of this thesis seek to test their veracity. Firstly, **Chapter 3** starts by introducing the concept of legal risk and discussing the levels of 'AML/CTF legal risk' that institutions have seemingly faced following the enactment of the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (P.L. 107-56, 115 Stat. 272) (USA PATRIOT Act). Focussing primarily on an institution's potential criminal liability under municipal and/or extraterritorial AML/CTF legislation, it then moves on to identify the types of criminal penalties available for certain AML/CTF offences.*

By outlining the types of criminal penalties that may attach to an AML/CTF compliance failure, and analysing the frequency with which they are invoked, the Chapter seeks to assess the validity of the widely publicised claims that non-compliance with AML/CTF legislation will be tenaciously enforced by regulators and the courts. Contrary to popular belief, it finds that in several risk-based regimes, criminal enforcement actions are only pursued in the most brazen cases of money laundering or terrorism financing. Due to the commercial consequences and collateral damage that may stem from the indictment of a large financial institution, many regulatory and prosecutorial officials now appear to be relying heavily on civil courses of action to address institutions' AML/CTF compliance failures and money laundering offences. With their lower standard of proof, such actions can be effectively used to secure positive regulatory results without the disruption, delay and expense often attached to criminal prosecutions.

In extending the analysis contained in **Chapter 3** of this thesis, **Chapter 4** views AML/CTF legal risk in terms of the civil law repercussions that may stem from an institution's

⁴¹ Ginzl, D., Risk Management and the Money Laundering Challenge (2005) 20(4) Commercial Lending Review 41.

involvement in a money laundering or terrorism financing event, and/or contravention of AML/CTF legislation. Throughout the Chapter, the term "civil" is used in an inclusionary fashion; encompassing all legal courses of action, types of legal proceedings and penalties that are not strictly "criminal" in nature. Thus, unless otherwise stated, the definition of civil law necessarily includes those areas of the law that might otherwise be considered to fall under the umbrella of equity.

In **Chapter 4**, consideration of an institution's AML/CTF legal risk falls into several parts. After initially discussing the kinds of civil enforcement actions and civil penalties that might accompany a contravention of AML/CTF legislation, the Chapter details how an institution's AML/CTF legal risk may be heightened as a result of tension between its AML/CTF obligations at civil and criminal law. Drawing on the experiences of institutions in the U.K., the Chapter determines that regulated entities can find themselves in a precarious legal position (and find that their AML/CTF legal risk at civil law is increased) in circumstances where there is a lack of clarity around the interplay between their legislative requirements, contractual obligations, and constructive trust principles. Any uncertainty around their obligations and, more specifically, which obligations should take precedence in terms of their compliance efforts, can create a situation where some entities are compelled to trade off compliance with their civil obligations in order to avoid incurring liability at criminal law (or vice versa).

Whilst **Chapters 3 and 4** discuss the concept of AML/CTF legal risk, detail the likely consequences of non-compliance with AML/CTF laws, and assess the levels of risk faced by institutions operating under risk-based regimes, **Chapter 5** of this thesis addresses the ways in which an institution might seek to mitigate its ongoing AML/CTF legal risk in the aftermath of an AML/CTF compliance failure. It identifies a number of practical risk mitigation strategies for institutions, and outlines the types of regulatory outcomes that may arise where an institution is prepared to voluntarily report its legislative breaches and implement corrective actions.

Whilst the Chapter looks at several ways that institutions can manage their reputational and financial risk, it primarily focuses on the ongoing management and mitigation of AML/CTF legal risk. It discusses a number of risk management strategies but ultimately recognises that the most prudent way for an institution to manage its AML/CTF legal risk is through the adoption of an avoidance strategy (and therefore, compliance with all relevant AML/CTF laws). That said, the Chapter questions whether such a strategy is the most cost effective way for an institution to address its risk, given that the pursuit of formal enforcement proceedings appears to be relatively infrequent in many risk-based AML/CTF regimes. Though some institutions may believe that the potential consequences of an AML/CTF compliance failure make a compelling case in favour of avoidance risk management strategies, the Chapter canvasses a number of reasons why others may consider that the costs of achieving AML/CTF compliance considerably outweigh the penalties that they are likely to face for legislative non-compliance.

In continuing to identify and assess the levels of risk faced by institutions operating in risk-based regimes, **Chapters 6 and 7** of this thesis use detailed case studies to highlight the potential inability of institutions to effectively manage and mitigate their AML/CTF-related risks. Whilst one of the case studies relates to a clear case of institutional money laundering, and the other relates to a *perceived* case of institutional money laundering, they both provide a number of practical teachings relative to the concept of risk. They address the limitations of institutions' risk management strategies, and demonstrate how an institution's unmitigated risk can translate into domestic and/or extraterritorial enforcement actions. Further, they illustrate that whilst regulatory authorities might display a preference for less intrusive, more cooperative regulatory outcomes, decisive action may nevertheless be taken against institutions involved in legislative contraventions that pervasive, unresolved, or of serious regulatory concern.

Firstly, using Riggs Bank as a case study, **Chapter 6** highlights the financial, reputational and legal risks that an institution might face as a result of its lax AML/CTF controls. It analyses the apparent levels of AML/CTF regulation in the U.S., and the circumstances in which U.S. regulatory and law enforcement authorities will seemingly be prepared to launch

criminal enforcement proceedings against a bank in breach of its legislative obligations. Riggs Bank was specifically chosen as a case study for inclusion in this thesis because it has become emblematic of how public and wanton AML/CTF compliance failures can transform an institution often billed as "the most important bank in the most important city in the world", ⁴² into the most criticised bank in the most unforgiving city in the world. It illustrates not only how AML/CTF compliance failures can arise, but also how risk-based regulation can work in practice.

Secondly, using Banco Delta Asia a case study, **Chapter 7** details the potential consequences of non-compliance – or alleged non-compliance – with AML/CTF legislation and international best practice standards. Given the action taken against Banco Delta Asia by the U.S. government under *Section 311* of the *USA PATRIOT Act*, the Macau bank was selected for inclusion in this thesis because it demonstrates an institution's potential AML/CTF legal risk under extraterritorial legislation, and highlights the significant role that perception can play in sculpting an institution's legal, reputational and financial risk. It also illustrates the potential limits of an institution's risk management capabilities, and the way in which AML/CTF regulation and enforcement may be influenced by international relations and the delicate political relationships between particular nation states.

Finally, **Chapter 8** of this thesis addresses each of the previously identified research questions. Drawing on the conclusions reached in the preceding Chapters, it identifies the various risks and the levels of risk that institutions operating under certain risk-based regimes are likely to face. In doing so, it challenges the common assertion that breaches of AML/CTF legislation may lead to the imposition of financially debilitating, or even commercially fatal, penalties.

Indeed, **Chapter 8** finds that whilst AML/CTF compliance failures might theoretically carry heavy penalties, these penalties are rarely invoked in practice. During the past few years, a

⁴² O'Brien, T.L., 'At Riggs Bank, a Tangled Path Led to Scandal', *The New York Times* (New York), 19 July 2004

<http://www.nytimes.com/2004/07/19/business/19BANK.final.html?ex=1247976000&en=cb5f669d9fc948cd &ei=5088&partner=rssnyt> at 15 December 2006.

number of regulatory and law enforcement authorities appear to have deliberately shifted their activities away from the initiation of criminal proceedings, towards the use of cooperative regulatory outcomes and agreements. Accordingly, many assessments of AML/CTF legal risk appear to be overstated, not least of all by financial institutions themselves. Whilst certain types of offences seemingly carry heavier penalties and a greater level of AML/CTF legal risk than others, the level of AML/CTF risk generally faced by institutions is not as pronounced as it was several years ago, in the immediate aftermath of September 11.

Whilst risk-based approaches to AML/CTF have become increasingly popular since the 2001 terrorist attacks, the Chapter offers a number of reflections on their relative effectiveness. It discusses the perceived benefits of risk-based regimes, and notes that such benefits will not always be apparent when the operation of these regimes is observed. In practice, it appears that the flexibility and cost-savings often attributed to risk-based regimes may be somewhat undermined by the use of benchmarking exercises, uncertainty around risk-based requirements, and retrospective application of rules-based compliance models.

Despite some of their potential shortcomings however, **Chapter 8** concludes that a greater understanding of risk-based approaches to AML/CTF can enrich institutional understandings of the phenomena of risk. By gaining greater knowledge about the types and levels of risk apparent in several risk-based regimes, institutions may be better placed to identify and address their individual risk exposures. Further, they may be better able to determine the potential consequence risk represented by any non-compliance with risk-based legislation. Without such an acute understanding of the operation of risk-based approaches, institutions may find themselves adopting flawed risk management strategies, spending copious amounts of money on poorly designed AML/CTF programs, and/or otherwise taking steps to undermine the alleged benefits of risk-based regimes – flexibility, cost-effectiveness, and enhanced engagement with the concepts of AML and CTF.

Chapter 2

Looking at Money Laundering through the Lens of Risk Management

"The first step in the risk management process is to acknowledge the reality of risk. Denial is a common tactic that substitutes deliberate ignorance for thoughtful planning" — Charles Tremper

2.1 The big picture

Whilst there are no reliable figures available with respect to the scale of international money laundering activities, figures suggest that organised crime has become an industry – and money laundering has become a business – capable of "rivalling multinational corporations as an economic power". Estimates of annual money laundering flows range from USD\$1 trillion to USD\$2 trillion, or about 2-5 per cent of global Gross Domestic Product. Of this total amount, it is believed that approximately AUD\$4.5-11.5billion is laundered through Australia each year. 46

Money laundering enables people to integrate illegally obtained funds into the financial system and, through a series of transactions and financial flows designed to distance them from the underlying predicate offences, access the funds legitimately thereafter.⁴⁷
Operationally, the process of laundering 'dirty' money involves the following three stages:

New York, 1999) 5.

⁴⁷ Russel, P.S., 'Money Laundering: A Global Challenge' (2004) 5(1/2) Journal of American Academy of Business 260.

Reuter, P., and Truman, E.M., Chasing Dirty Money: The Fight Against Money Laundering (2004) 4.
 United Nations Development Programme, Human Development Report 1999 (Oxford University Press,

⁴⁵ See KPMG, Global Anti-Money Laundering Survey 2007 (2007) http://www.kpmg.com/SiteCollectionDocuments/Global%20Anti-money%20laundering%20survey%202007.pdf at 9 June 2008.

Whilst the Federal Attorney-General's Department believes that AUD\$11.5 billion is laundered through Australia each year, research released by the Australian Institute of Criminology in October 2007 indicates that approximately AUD\$4.5 billion is laundered through the country annually. See Fagg, S., \$4.5 Billion Laundering Estimate (2007) Lawyers Weekly http://www.lawyersweekly.com.au/articles/4-5-billion-laundering-estimate z137203.htm> at 9 June 2008.

- (i) placement where the illegal funds are placed in the financial system, typically by being deposited in a domestic or offshore financial institution, or used to purchase expensive goods which may subsequently be resold to obtain payment;
- (ii) layering where the illegitimate source of the funds is obscured through a complex maze of transactions (often involving electronic funds transfers or investments in shell operations) designed to effectively destroy any audit trail; and
- (iii) integration where the 'cleaned' funds are finally incorporated into the monetary system so that they can be freely accessed thereafter.

In comparison to money laundering, which seeks to hide the origin of illegally obtained funds, terrorism financing aims to disguise the destination of funds that may be derived from either legitimate or illegitimate sources. Accordingly, when compared to money laundering, the prevention and detection of terrorism financing presents an array of different challenges for governments, regulatory authorities and institutions. Even where terrorism financing involves ill-gotten funds, the transactions involving those funds may evade detection because they concern small amounts of money and are therefore able to circumvent the AML monitoring systems and controls in place at many institutions. As stated by the FATF in its Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing - High Level Principles and Procedures, identifying terrorism financing is often significantly more difficult than identifying money laundering and other suspicious activities (especially in circumstances where there is a lack of typologies and related guidance/intelligence from regulatory authorities). 48 Thus, although recent policy responses to AML and CTF have generally been fused, the AML/CTF controls implemented by institutions will typically be geared more heavily towards the prevention and detection of money laundering activities, and may therefore be unable to identify those terrorism financing activities that do not display the traditional hallmarks of money laundering.

Despite their inherent differences, money laundering and terrorism financing share a number of similarities. Firstly, their common goal is to conceal illegal activities that have already occurred or are yet to occur. Secondly, neither money laundering nor terrorism financing

⁴⁸ Op cit n 16, 8.

actually targets financial institutions per se; both crimes use such institutions as vehicles for transferring and obscuring tainted funds. As financial institutions are simply a means to an end for money launderers and terrorism financiers, the primary risks posed by these crimes are generally legal and reputational in nature.

Although money laundering and terrorism financing have long posed risks to financial institutions, such risks appear to have been exacerbated in recent years as a result of rapid advances in technology, the globalisation of the financial services industry, ⁴⁹ heightened levels of regulation, and increased penalties for non-compliance with AML/CTF legislation. ⁵⁰ According to many media commentators and industry participants (including regulatory officials, lawyers, consultants and others practising in the field of AML/CTF compliance), the stakes for combating money laundering and terrorism financing have never been higher. They allege that institutions in breach of AML/CTF legislation are likely to suffer incalculable reputational damage⁵¹ and, in more severe cases, even closure as a result of their compliance failures. ⁵²

Over the past few years, increasing regulatory and industry attention has led to an apparent paradigm shift in the way that many financial institutions regard their AML/CTF obligations. Despite previously regarding their AML/CTF compliance programs as a mere regulatory exercise, many institutions now recognise that such programs might prove to be critical in safeguarding their commercial integrity, reputation and financial standing.⁵³ This Chapter seeks to:

- contextualise AML/CTF within the broader development of risk management as an independent discipline;
- further develop an understanding of the operation and perceived benefits of risk-based approaches to AML/CTF;

⁴⁹ Fisher, B., Money Laundering – What You Don't Know Can Hurt You, ACI Worldwide, <http://www.aciworldwide.com/pdfs/aci_trends_frauddetect.pdf> at 13 March 2006.

ACI and TowerGroup, Money Laundering: Preserving the Integrity of Financial Institutions (2002) http://www.aciworldwide.com/pdfs/aci trends frauddetect2.pdf> at 1 April 2006.

⁵¹ Op cit n41.

⁵² Op cit n49.

⁵³ Op cit n49.

- detail the way in which institutions typically seek to assess their ML/TF risk;
- frame the concept of ML/TF risk in terms of traditional risk types (with the exception of legal risk, which is addressed separately in subsequent Chapters); and
- address the consequence risk that may stem from an institution's involvement in a money laundering or terrorism financing offence and/or contravention of AML/CTF legislation.

2.2 How risk management has moulded approaches to AML

Although risk management is not a new phenomenon, the concept of ML/TF risk has only gained wide recognition during the last decade. However, given that risk management and regulatory trends have generally determined the attitudes of financial institutions to risk taking at any point in time, it is useful to frame ML/TF risk in terms of the broader, historical development of risk management. Indeed, it appears that key developments in risk management – particularly those that occurred in the U.S. – have influenced modern day approaches and attitudes to the risks represented by money laundering and terrorism financing.

2.2.1 The birth of modern risk management (pre 1960s)

The early Twentieth Century was a formative time for risk management; characterised by burgeoning enterprise, the identification of new risks and the aggravation of older exposures. Following the U.S. stock market crash in 1929, there was a strong public interest in ensuring that regulation of financial markets was effective. This created a greater appreciation of systemic risk and, in turn, prompted the U.S. government to enact a spate of related federal laws. These laws, which included the *Banking Act of 1933* (P.L. 73-66, 48 Stat. 162) and the *Bank Holding Company Act of 1956* (P.L. 84-511, 70 Stat. 133), sought to reduce banking risks and protect the soundness of the U.S. banking system by preventing financial institutions from expanding their activities into new and potentially risky areas.

⁵⁴ Barlow, D., 'The Evolution of Risk Management' (1993) 40(4) Risk Management 38.

Thel, S., 'The Original Conception of Section 10(b) of the Securities Exchange Act' (1990) 42 Stanford Law Review 385, 394.

⁵⁶ For example, in 1933 Regulation Q capped the interest rate that could be paid on savings accounts.

Prior to the 1960s, risk management was largely dictated and controlled by government authorities. Most institutions had no formal way of managing their risk, and those that did tended to delegate the totality of their risk management functions to internal purchasers of insurance.⁵⁷ This is despite the fact that awareness of the field of risk management had grown during the 1950s after two academics, Wayne Snider and Russell Gallagher, separately published articles which, for the first time in business literature, used the terms 'risk managers' and 'risk management'.⁵⁸

2.2.2 Beyond in-house insurance (the 1960s and 1970s)

As recognition of the field of risk management grew during the 1960s and 1970s, the role of organisational insurance clerks evolved to that of insurance buyers, and then to insurance managers. Reliance on insurance companies as the sole providers of risk services began to wane, and risk management started to move away from a narrow, insurance-based discipline. Prompted by several events, including the release of the first risk management texts, increasing numbers of institutions looked beyond insurance for other methods of managing their commercial risks. Management teams started searching for more innovative risk-shifting activities and widened their focus beyond profit making to include risk intermediation.

During this period, some jurisdictions enacted AML legislation requiring "financial institutions to help [their government(s)] catch money launderers". ⁶³ For instance, U.S. Congress enacted the Bank Secrecy Act after domestic law enforcement bodies claimed that internal bank procedures were hampering their ability to access confidential account information, and identify and prosecute organised crime. ⁶⁴ The Act required financial institutions to report suspicious transactions, cash transactions in excess of USD\$5,000, and

⁵⁷ Leimberg, S.R. et al, The Tools & Techniques of Risk Management & Insurance (2002).

Whilst insurance buyers are involved in choosing the desired insurers and insurance coverage, insurance managers are generally in charge of a department dedicated to insurance.

⁶⁰ Thompson, D., 'Risk Management: A Brief History' (2003) Journal of Banking and Financial Services 30.

⁶¹ Englehart, J.P., 'A Historical Look at Risk Management' (1994) 41(3) Risk Management 65.

⁶² Crouhy, M., Galai, D., and Mark, R., Risk Management (2001).

⁶³ Op cit n5.

⁶⁴ Ibid.

the transportation of currency across U.S. borders.⁶⁵ Whilst its prescriptive obligations did not necessarily encourage U.S. institutions to consider their individual risk profiles or risk management practices, they certainly required them to actively consider AML (as well as their accompanying obligations) for the first time.

2.2.3 A change in regulatory approach (the 1980s)

The early 1980s marked a dramatic change in regulatory philosophy, especially in the U.S. where the enactment of the *Depository Institutions Deregulation and Monetary Control Act of 1980* (P.L. 96-221, 94 Stat. 132) and *Depository Institutions Act of 1982* (P.L. 97-320, 96 Stat. 1469) substantially deregulated and liberalised the country's banking system. These pieces of legislation not only changed the roles and responsibilities of U.S. banking regulators, but also significantly increased the regulatory and legal pressure placed upon U.S. financial institutions to implement internal risk management measures.

As opposed to simply setting a broad, industry-based risk management agenda for financial institutions, regulatory authorities started to monitor banks' internal risk management systems. However, given that the requests of U.K. and U.S. regulators for streamlined international capital adequacy standards were largely ignored, the internal risk management standards expected of financial institutions continued to be addressed in an ad hoc fashion by national governments. It was not until 1988, when the Basel Committee⁶⁶ released *Basel 1* (i.e. an accord requiring banks to hold at least 8 per cent capital to mitigate their credit and market risk) that this situation began to change.

Shortly after the release of *Basel I*, the Basel Committee published the *Basel Statement of Principles* – a set of best practice guidelines designed to increase the soundness of the international banking system and assist financial institutions to avoid being stained with the opprobrium of money laundering.⁶⁷ These Principles, coupled with the Basel Committee's

⁶⁵ See the Bank Secrecy Act of 1970, 31 U.S.C. §§ 5311-5312, 5316-5324.

⁶⁶ The Committee was comprised of the central bank governors of Belgium, Canada, France, Germany, Italy, Japan, Netherlands, Sweden, Switzerland, and the United States.

⁶⁷ Manger, G., 'Commentary - Part 2' (Speech delivered at the Anti-Money Laundering Symposium, Canberra, September/October 2002) 12.

statement on the *Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering*, encouraged institutions to implement customer identification procedures, comply with all relevant AML laws and regulations, and cooperate with law enforcement authorities in any related investigation. Together, the documents signalled a growing recognition – on both a national and an international level – of the role that financial institutions must play in combating money laundering activities.

In addition to the release of risk management and money laundering publications by the Basel Committee, the 1980s saw the United Nations take a heightened interest in the issue of money laundering. In what ultimately proved to be a significant step forward in the international fight against money laundering, ⁶⁸ the *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances* (**Vienna Convention**) was adopted in 1988. This Convention, which became effective on 11 November 1990, made money laundering an internationally extraditable offence and obliged all ratifying countries to criminalise drug trafficking and associated money laundering. As at September 2008, the convention had a significant degree of universal acceptance, with 153 State Parties. ⁶⁹

The 1980s were not only characterised by international efforts to address money laundering though. The decade also ushered in the enactment of many municipal AML laws, such as the U.S. Money Laundering Control Act of 1986 (P.L. 99-570, 100 Stat. 3207-18) (MLCA)⁷⁰ and the Criminal Justice Act 1988 (U.K.), amongst others. Although these pieces of legislation were largely concerned with the criminalisation of money laundering, as opposed to the management of its related risks, they nevertheless marked an increased political interest in money laundering. At that time, drug use and drug-related crime were politicised 'problems', ⁷¹ and national governments were under immense pressure to provide voters with

⁶⁸ Hopton, D., Money Laundering: A Concise Guide for all Business (2006) 7.

⁶⁹ See United Nations Information Service, Countries Invited to Sign, Ratify or Accede to Multilateral Treaties During the Treaty Event 23-25 and 29 September and 1 October 2008, UNIS/INF/281, 22 September 2008.

⁷⁰ See Money Laundering Control Act of 1986 (P.L. 99-570, 100 Stat. 3207-18).

Australian Institute of Criminology, The Global Response to Money Laundering: How Global Politics Shaped the Result (2002) http://www.aic.gov.au/conferences/2002-ml/broome.pdf> at 17 February 2008.

legal 'solutions' to them. It was not until the following decade that the broader management of money laundering risk began to receive more legislative and regulatory attention.⁷²

2.2.4 Risk management comes into its own (the 1990s)

During the 1990s, risk management again received attention after a spate of high-profile corporate collapses was attributed to poor corporate governance.⁷³ Risk minimisation became a desirable objective of sound financial management,⁷⁴ and risk management emerged as an integral part of company planning and strategy. In following on from this, institutions increasingly integrated risk management into their corporate functions, and the role of risk management expanded to encompass organisation-wide programs.⁷⁵

Throughout this decade, the management of money laundering risk gained worldwide recognition after a number of international bodies released guidance – aimed at both institutions and national governments – with respect to the to the identification, mitigation and management of money laundering. Until this time, many national governments had perceived AML as a local issue and an issue that did not represent a priority for the banking industry. However, the international attention it received during the 1990s further elevated the issue of money laundering to the global stage, and heightened awareness of the ability for money laundering activities to undermine the stability, integrity and governance of the international financial system.

The 1990s saw the FATF begin to cement its role as an influential, multi-disciplinary body concerned with money laundering trends, the adoption of streamlined AML standards, and the progress of member states in implementing AML measures. In April 1990, the body

⁷² For instance, whilst Australia first enacted laws covering a number of money laundering offences in 1987, it was not until January 2003, when *Division 400* of the *Criminal Code Act 1995* (Cth) was amended, that such offences received greater legislative attention and money laundering was further criminalised.

⁷³ Lam, J., 'A New Role: Chief Risk Officer' (1999) 64(2) *Ivey Business Journal* 55.

Manger, G., 'Risk Management and Reputation, Commentary – Part 3' (Speech delivered at the Anti-Money Laundering Symposium, Canberra, September/October 2002) 23.

⁷⁵ Heir, K., Encyclopaedia of Management, Reference for Business

http://www.referenceforbusiness.com/management/Pr-Sa/Risk-Management.html at 14 August 2006. KPMG, Global Anti-Money Laundering Survey: How Banks Are Facing up to the Challenge (2004)

http://www.kpmg.ca/en/industries/fs/banking/documents/globalAntiMoneyLaunderingSurvey.pdf at 1 September 2006.

released the FATF 40 Recommendations; arguably the most significant AML instrument created up until that time. The Recommendations outlined a set of money laundering countermeasures covering law enforcement and the criminal justice system, the financial system and its regulation, and international cooperation. They sought to increase financial transparency, improve regulatory oversight and streamline approaches to AML by encouraging:

- *jurisdictions* to ratify the *Vienna Convention*, reduce their bank secrecy laws and cooperate with other nations in the investigation and prosecution of money laundering offences; and
- *institutions* to implement a number of internal controls including transaction reporting, AML training, record keeping and customer due diligence.

Although the FATF 40 Recommendations were initially intended to combat the misuse of the international financial system by people laundering drug money, it quickly became apparent that money laundering activities are not confined to the proceeds of the drug trade. National banking regulators urged the FATF to extend the Recommendations beyond those situations where drug trafficking was the predicate offence, and the FATF responded by releasing a revised version of its Recommendations in 1996. These new Recommendations were quickly regarded as global best practice standards for AML, and several countries (including Brazil, Germany, Hong Kong, Nigeria, Switzerland, South Africa and the U.K.) subsequently enacted municipal AML legislation modelled on them.

In addition to prompting the creation of AML legislative regimes in a number of jurisdictions, the *FATF 40 Recommendations* led to the establishment of several other regional and international bodies also seeking to assist with the design of AML risk management practices. These included the Caribbean Financial Action Task Force, Egmont Group of Financial Intelligence Units, Asia-Pacific Group on Money Laundering (**APGML**), and the Eastern and Southern African Anti-Money Laundering Group.

2.2.5 Bang for their buck - The era of the risk-based approach (the 2000s)

Following the turn of the century, the continued development of AML risk management was initially marked by the release of *Anti-Money Laundering Principles for Private Banking* by the Wolfsberg Group. ⁷⁷ Published in October 2000 (and subsequently revised in May 2002), these Principles were created to address the growing dissatisfaction with the *Basel Statement of Principles*. They recognised the differential treatment of high net-worth individuals in private banking, and acknowledged the higher ML risk typically associated with private banking activities. Whilst they have only been accepted by a limited number of financial intuitions, the adoption of the Principles by a number of large, multinational banks has seen them become the standard for reputable banks operating internationally. As such, they have played a role in modernising AML risk management practices with respect to the acceptance of new clients, identification of unusual or suspicious transactions, and education of bank staff ⁷⁸

However, whilst the Wolfsberg Group's *Principles for Private Banking* have influenced the way that many institutions currently address their AML obligations, no single event has had a more sizeable impact on modern day approaches to the identification and management of ML/TF risk than the September 11 attacks. Those attacks immediately ushered in a new regulatory and legislative era with respect to money laundering. They redefined international politics, thrust AML/CTF issues at the top of government agendas, and drove – perhaps with a mixture of fear and vengeance – a U.S.-led assault on acts of terrorism and terrorism financing.

Arguably, the events of September 11 marked the first global acknowledgement of terrorism financing and the importance of financial institutions in combating acts of terrorism. Whilst terrorism financing had garnered minimal government interest until that time, the images of the crumbling World Trade Centre towers – beamed to an ever-watchful international audience via television, radio and the internet – provided the impetus for intense legislative

The Wolfsberg Group is a body comprised of twelve leading international private banks, including ABN Amro, Banco Santander, Bank of Tokyo-Mitsubishi-UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JP Morgan Chase, Société Générale, and UBS.
 Op cit n67, 17.

reform. A number of clear links between money laundering and terrorism financing were established, and it became clear that the key to some terrorism investigations could be the financial transactions that enabled such acts of terrorism to occur in the first place. In the case of the 2001 attacks, several debit cards, AUD\$600,000 and twenty-four accounts opened with fictitious names/social security numbers, had cost thousands of lives, sent the largest international financial centre into hiatus, and destroyed or damaged more than USD\$16 billion worth of physical assets.

In the immediate aftermath of the September 11 attacks, a number of national governments passed legislation to better control and curtail potential terrorism financing activity. For instance, whilst the U.K. government swiftly enacted the *Anti-Terrorism, Crime and Security Act 2001* (U.K.), the U.S. government enacted the *USA PATRIOT Act* to amend the *Bank Secrecy Act* and impose a wide range of onerous AML/CTF obligations upon institutions operating in the U.S. Whilst the U.S. legislation relates to both AML and CTF, its drafting was primarily geared towards combating the financing of terrorism and removing the major barriers that historically prevented law enforcement, intelligence and defence agencies from sharing certain types of information. The legal impediments that previously separated criminal and intelligence investigations were blamed for the failure of the Federal Bureau of Investigation (**F.B.I.**) to identify and detain two of the September 11 hijackers; Nawaf al-Hazmi and Khalid al-Midhar, prior to the attacks. In order to prevent such discord from arising again, *Sections 203(b)* and *203(d)* of the *USA PATRIOT Act* were broadly drafted to enable (and in some circumstances, enhance) information sharing with the F.B.I and the intelligence community more generally.

Australian Transaction Reports and Analysis Centre, *Introduction to AML/CTF*: Terrorism Financing http://www.austrac.gov.au/elearning/pdf/mod terrorism financing.pdf> at 18 February 2008.

The destruction of physical assets caused by the attacks has been estimated at USD\$14 billion for private businesses, USD \$1.5 billion for state and local government enterprises, and USD\$0.7 billion for federal enterprises. Including the related rescue and clean up costs (estimated at USD\$11 billion), this is an estimated total direct cost of USD\$27.2 billion. See Looney, R., 'Economic Costs to the United States Stemming From the 9/11 Attacks' (2002) 1(6) Strategic Insights.

⁸¹ The Act not only targets banks and non-bank financial intermediaries, but affects almost every other type of financial service institution operating in the U.S., including broker-dealers, investment companies, money service bureaus, and life insurers.

Abramson, L., and Godoy, M., *The Patriot Act: Key Controversies* (2006) NPR http://www.npr.org/news/specials/patriotact/patriotactprovisions.html at 1 May 2008.

Beyond enhancing the powers of several U.S. government authorities, the *USA PATRIOT Act* is largely responsible for sculpting current approaches to the management of ML/TF risk. The legislation clearly recognises the importance of recruiting financial institutions in the fight against illicit financial activities. It acknowledges that such institutions are the gatekeepers to the international financial system and that without their cooperation and support, government efforts aimed at curbing money laundering and terrorism financing may be futile. The Act enshrines a risk-based approach to AML/CTF, which requires financial institutions to identify their own levels of ML/TF risk, and allocate their compliance resources to those areas of their business representing the greatest ML/TF risk. Over and above a number of minimum legislative requirements, ⁸⁴ it essentially empowers institutions to define the extent to which they mitigate or tolerate their ML/TF risk.

Whilst the *USA PATRIOT Act* marked the first legislatively enshrined risk-based approach to AML/CTF, it is important to note that risk-based legislation and regulation were not new concepts at the time of its enactment. Following the collapse of several large financial services firms during the 1990s (for instance, the 1996 collapse of Barings Bank in the U.K. and the 1999 collapse of HIH in Australia), risk-based approaches had already started to find some favour amongst national governments prior to 2001. In the years immediately preceding the September 11 attacks, regulatory authorities such as the U.K. FSA, Australian Prudential Regulation Authority, and Canadian Office of the Superintendent of Financial Institutions, had started to develop new regulatory methods that built upon the sophisticated risk management tools already in use by many financial institutions. These methods advocated meta monitoring and regulation, and placed greater emphasis on the organisational control of inherent risks. Institutions were expected to identify and assess certain risks, and to manage and mitigate such risks through the use of internal controls and governance

Fox, W.J., (Untitled speech delivered at the Financial Services Roundtable, Washington D.C., 29 January 2004). See also Robinson, P., 'Effective AML – the UK Story' (Speech delivered at the Asia-Pacific Financial Crime Conference & Exhibition, Singapore, July 27 2006).

For instance, institutions are required to implement an AML/CTF compliance program, undertake more onerous 'due diligence' with respect to correspondent and private banking relationships, and conduct certain customer identification/verification procedures for all new account openings.

⁸⁵ Black, J., The Development of Risk-Based Regulation in Financial Services: Canada, the U.K. and Australia (London School of Economics and Political Science, London, 2004) 48.

structures. Those deemed by regulatory authorities to represent a lower risk received less supervisory attention than those considered to carry a much higher risk.

Whilst these regulatory regimes (and their accompanying institutional responsibilities) signified a shift towards risk-based regulatory regimes prior to 2001, it was not until the terrorist attacks that risk-based approaches to AML/CTF were acknowledged and implemented in a number of jurisdictions. The events of September 11 led to the swift enactment of the *USA PATRIOT Act* and, in turn, the endorsement of risk-based AML/CTF regimes. They set the international pace for the adoption of broad AML/CTF legislation, and created a renewed concern for AML amongst various international bodies.

Following the events of September 11, the FATF expanded its mandate and released the FATF 9 Special Recommendations. Specifically tailored to terrorism financing, these Recommendations supplemented the FATF 40 Recommendations (which were again revised in 2003) and urged jurisdictions to ratify the 1999 United Nations Convention on Terrorist Financing, criminalise terrorist financing, and create a regime for institutions to report suspicious transactions. Collectively, the FATF 40+9 Recommendations have today become a driving force behind the adoption of risk-based regimes. This is despite the fact that only six of the revised FATF 40 Recommendations explicitly consider the concept of risk and the importance of institutions identifying their own levels of ML/TF risk, and implementing measures commensurate to that risk.⁸⁶

Given the international importance of the *FATF 40+9 Recommendations* and the broad public interest in money laundering and terrorism financing post-September 11, AML/CTF has seemingly become the subject of meta monitoring and regulation during the past decade. ⁸⁷ Though they do not constitute a binding international convention, many of the Recommendations have formed the basis of the risk-based AML/CTF regimes now adopted in a many jurisdictions.

⁸⁶ See revised FATF Recommendations 5, 6, 8, 20, 23 and 24.

As noted in **Chapter 1** of this thesis, the concept of meta regulation refers to the governmental monitoring of others' self monitoring. See Braithwaite, J., *Markets in Vice, Markets in Virtue* (2005) 85.

The FATF periodically subjects jurisdictions to mutual evaluations with respect to how well they have adopted and implemented the FATF 40+9 Recommendations. Where a jurisdiction is found to have disregarded the Recommendations and/or otherwise failed to create an adequate AML/CTF legislative/regulatory environment, that jurisdiction may be included in the FATF's List of Non-Cooperative Countries and Territories. Although the use of this list is largely redundant now, any jurisdiction identified by the FATF as having a lax AML/CTF regime may nevertheless face significant pressure from the international community to formally adopt the Recommendations. This is clear from the Australian Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (AML/CTF Act 2006 (Cth)), which was primarily enacted by the country's government in response to an unflattering 2005 FATF Mutual Evaluation report that found Australia was only fully compliant with nine of the FATF 40 Recommendations.

However, whilst the FATF 40+9 Recommendations have played a significant role in the development of national AML/CTF legislation and global AML/CTF best practice standards, other guidance documents have also played a role in sculpting current AML/CTF regimes and risk management methods. For instance, the Wolfsberg Group's Anti-Money Laundering Principles for Correspondent Banking have provided institutions with guidance on managing their correspondent banking relationships, and preventing other entities with inadequate AML controls from accessing the international banking system. ⁹⁰ They endorse the adoption of a risk-based approach to AML/CTF by encouraging institutions to pay particular attention to 'country risk' and 'customer risk' when assessing the ML/TF risk represented by a correspondent banking relationship. Further, they outline a number of jurisdictional and customer-based risk factors that might indicate that a certain correspondent banking relationship represents a higher ML/TF risk. Although these factors are neither exhaustive nor prescriptive, they have nevertheless assisted many institutions to develop their internal risk-based approaches and design risk-sensitive correspondent banking programs.

⁸⁸ See Sharman, J.C., 'International Organisations, Blacklisting and Tax Haven Regulation' (Paper presented at the International Studies Association Meeting, Montreal, 18 March 2004).

⁸⁹ See Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Combating the Financing of Terrorism - Australia* (2005) Organisation for Economic Cooperation and Development http://www.oecd.org/dataoecd/60/33/35528955.pdf at 3 May 2008.

Wolfsberg Group, Anti-Money Laundering Principles for Correspondent Banking (2002) http://www.wolfsberg-principles.com/faq-correspondent-banking.html at 3 September 2006.

In addition to its *Principles for Correspondent Banking*, the most notable AML/CTF paper released by the Wolfsberg Group is its *Guidance on a Risk Based Approach for Managing Money Laundering Risks*. Published in March 2006, the Guidance states that whilst there is no generally agreed methodology for implementing a risk-based approach to AML/CTF, institutions should ideally assess their ML/TF risk profile on the basis of their country risk, customer risk and product risk. ⁹¹ To this end, it outlines a number of risk variables that institutions can consider when assessing the money laundering risk represented by a certain customer or transaction. These include, amongst other things:

- the size and frequency of transactions undertaken by a customer;
- the level of regulation, oversight or governance to which a customer is subject; and
- any unnecessary use of intermediate corporate vehicles by a customer.

2.3 Risk perspectives

As increasing numbers of jurisdictions have adopted risk-based AML/CTF regimes, institutions have needed to find ways of accurately assessing, mitigating and managing their ML/TF risk. 92 Whilst many regulatory bodies (including AUSTRAC) have explicitly acknowledged the inability of institutions to "operate in a completely risk-free environment in terms of ML/TF", 93 they nevertheless expect organisations to properly identify and control the ML/TF risks that they might face through their provision of financial products/services.

Although risk literature has tended to focus heavily on traditional types of risk, such as credit risk and financial risk, risk-based approaches generally view ML/TF risk through the lens of very different risk types. In alignment with guidance from international bodies such as the Wolfsberg Group, ML/TF risk is typically assessed using three primary risk criteria; namely, customer risk, product/channel risk and jurisdiction risk. Whilst these "three bases" of

⁹¹ Wolfsberg Group, Wolfsberg Statement – Guidance on a Risk Based Approach for Managing Money Laundering Risks (2006) http://www.wolfsberg-principles.com/risk-based-approach.html at 24 May 2006. 92 Despite the documented differences between money laundering and terrorism financing, and the difficulties often associated with identifying terrorism financing activities, institutions often assess their ML and TF risk collectively. Accordingly, the term "ML/TF risk" is used throughout this dissertation, even though it is recognised that some of the analysis contained herein is more applicable to ML risk alone.
93 Australian Transaction Reports and Analysis Centre, Risk Management: A Tool for Small-to-Medium Sized Businesses http://www.austrac.gov.au/risk_management.html at 6 October 2009.

ML/TF risk⁹⁴ have been frequently propounded by bodies such as the FATF, 95 the individual or collective weight given to them by different institutions is likely to vary. 96

The assessment of ML/TF risk is largely an introspective, or inward-looking, process. It is not particularly concerned with the external regulatory environment, or even specific regulatory obligations per se. Rather, it is fundamentally concerned with assessing what some regulatory bodies have termed "business risk", or the internal risk that a particular entity will be exploited by money launderers or terrorism financiers.⁹⁷

Whilst there is no universally accepted standard regarding when a customer, product/channel or jurisdiction represents a higher ML/TF risk, several factors are commonly used to indicate the presence of increased risk. These factors include, but are not limited to, the following:

- customer risk customers are generally viewed as representing a higher ML/TF risk if (i) they
 - conduct frequent or unusual transactions with no legitimate or commercial purpose;
 - operate in a cash-intensive industry or an industry which deals primarily in high value goods; and/or
 - are identified as a "politically exposed person" (PEP).98
- product/channel risk financial products/services are generally viewed as representing a higher ML/TF risk if they are
 - heavily reliant upon remote and/or automated technology for their delivery;
 - provided via a delivery channel that shrouds customers' identities in anonymity; and/or

⁹⁴ Op cit n40.

⁹⁵ According to para 1.9 of the FATF's Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing - High Level Principles and Procedures, institutions operating under risk-based regimes should identify their "higher risk customers, products and services, including delivery channels, and geographical locations." See Financial Action Task Force, Op cit n16, 2.

96 Op cit n16, 22.

⁹⁷ Op cit n93.

⁹⁸ Whilst there is no single, globally accepted definition of a PEP, the FATF definition (which is widely employed by most international financial institution) is any individual who is or who has been entrusted with prominent public functions in a foreign country (e.g. a Head of State or of government, a senior politician, or a senior executive of a state-owned corporation).

- able to swiftly facilitate transfers of funds across national geographic boundaries
 (e.g. international wire transfers).
- (iii) jurisdiction risk countries are generally viewed as representing a higher ML/TF risk if they are-
 - deemed by international organisations such as the FATF to be lacking appropriate
 AML/CFT laws and adequate AML regulation;
 - subject to any sanctions, embargoes or similar measures issued by the United
 Nations or comparable bodies; and/or
 - regarded as a drug-producing or drug-transit nation.

As opposed to customer risk and product/channel risk, it is interesting to note that jurisdiction risk can be largely driven by cultural and political influences. In the context of credit risk, jurisdiction risk has a high level of clarity; often being objectively determined by statistical data about a country's finances and credit history. However, in the context of ML/TF risk, the assessment of jurisdiction risk may be hinged upon the subjective interests of national governments. For instance, when determining whether a certain country represents a higher ML/TF risk due to its status as either a drug-producing or drug-transit nation, institutions often consult the U.S. Department of State's Annual Presidential Determinations of Major Illicit Drug-Producing and Drug-Transit Countries. This document currently cites a number of countries, including Afghanistan, Colombia and Pakistan, held by U.S. authorities to be heavily involved in the production or transportation of illicit substances. Whilst it remains a common point of reference for institutions seeking to assess their jurisdiction risk, the U.S. government will (either deliberately or inadvertently) continue to influence what others consider to be higher risk countries. Arguably however, if the scope of the document was expanded to include drug-consuming nations, many wealthy Western nations – including the U.S. – might also find themselves condemned in its pages.

Nevertheless, it is perhaps unsurprising that customer risk, product/channel risk and jurisdiction risk are driving risk-based approaches to AML/CTF. Risk-based approaches compel institutions to holistically assess the risk represented by their businesses, and international guidance released by the Wolfsberg Group explicitly urges institutions to assess

the ML/TF risk represented by their customers, product offerings and different jurisdictions. Further, the FATF and the Basel Committee encourage institutions to assess their ML/TF risk in terms of the 'three bases' by publishing lists of the types of financial products and countries considered to be more susceptible to money laundering activity.⁹⁹

By framing their overall ML/TF risk in terms of customer risk, product/channel risk and jurisdiction risk, it is believed that institutions can effectively identify and focus on those parts of their business most vulnerable to abuse at the hands of money launderers and terrorism financiers. Many commentators and international bodies have noted that, when applied effectively, risk-based approaches should ensure that those areas of an institution carrying the highest levels of ML/TF risk receive the greatest attention 100 and the largest proportion of institutional resources. This is in contrast to other, more prescriptive approaches to AML/CTF, which have been criticised for requiring institutions to apply their resources evenly to all customers, transactions and products, irrespective of their varying degrees of risk.

At first glance, the 'three bases' of risk used by many institutions to assess their ML/TF risk, do not fit neatly into the framework of traditional banking risks. At the most basic level, they are seemingly much narrower in terms of both their scope and application than more traditional banking risks. As risk-based approaches to AML/CTF have elevated awareness of relatively new risks, they have shifted focus away from more traditional risks and diminished the relevance of the four traditional risk management strategies outlined on the following page in Table 1.

⁹⁹ Op cit n47, 263.
¹⁰⁰ Op cit n16, 2.

Table 1 - Traditional risk management strategies 101

Strategy	Description
Acceptance	A strategy that involves accepting the likelihood and consequences of a certain risk. An institution's decision to adopt this strategy may be based upon several factors, including the amount of risk inherent in its usual business activities.
Transfer	A strategy that involves shifting (in whole or in part) a risk from one individual, entity or activity to another. Importantly, a transfer of an institution's risk will not always entail a corresponding transfer of its accountability for that risk.
Mitigation	A strategy that involves undertaking additional efforts to lower the likelihood and/or lessen the impact of a risk event occurring. The relevant risk is not entirely eliminated, but is monitored, managed and minimised.
Avoidance	A strategy that involves avoiding the likelihood of a risk arising – generally by absteining from any activity that carries such risk. Whilst avoiding a risk may protect an institution from incurring the negative impacts attached to it, it may also deny an entity the possible benefits attached to acceptance of the risk.

Whilst traditional risk management strategies may be readily applied to prescriptive AML/CTF obligations (for example, the requirement to screen customers against certain sanctions and watch lists), their potential application to ML/TF risk and risk-based legislative requirements is unclear. As risk-based approaches enable institutions to choose the extent to which they address their ML/TF risk, any decision to implement particularly extensive or lax risk management controls may not be framed at all in terms of traditional risk management strategies. Rather than making a conscious decision to employ a 'risk avoidance' or 'risk mitigation' strategy for instance, an institution may simply contextualise its decision to adopt tight risk management controls, in terms of its overall risk-based approach. Likewise, an institution that implements minimal or relatively skeletal risk management controls is unlikely to view its actions in the context of a 'risk acceptance' strategy. Presumably, it will simply frame its actions in terms of its overarching risk-based approach, albeit that such an approach demonstrates a greater propensity for risk-taking and a greater tolerance of ML/TF risk.

As previously noted, one of the aims of this Chapter is to examine the risks that money laundering and terrorism financing pose to financial institutions; not strictly through the lens

¹⁰¹ See Bowden, A.R., Lane, M.R., and Martin, J.H., Triple Bottom Line Risk Management: Enhancing Profit, Environmental Performance and Community Benefit (2001) 111. See also O'Regan, D., *Auditor's Dictionary: Terms, Concepts, Processes* (2004) 230.

of the 'three bases' of ML/TF risk, but within the context of broader, more traditionally recognised categories of risk. A discussion of these risks and their applicability (or otherwise) to the risk represented by money laundering and terrorism financing, is contained on the following pages.

2.4 Reputational risk

In today's competitive financial services market, many corporate executives regard their institution's reputation as "an independent good or an instrumental good" that is fundamental in attracting and retaining customers, and enhancing profit margins. Accordingly, reputational risk refers to the possibility that negative publicity regarding an institution's business practices, whether founded or not, will result in a loss of revenue, a loss of customers, a loss of jobs and, in more severe cases, even closure. Whilst money laundering and terrorism financing have long posed reputational risk to financial institutions, such risk has been heightened in recent years by rapid technological developments. In today's high-speed and interconnected environment, money laundering and terrorism financing scandals can be instantaneously broadcast to the world.

Whilst reputation is generally important for all industry sectors and organisational types, it may be argued that it is particularly critical to the ongoing operation of financial institutions. As opposed to some organisations based in manufacturing and other industries, banks are quasi-public utilities¹⁰⁴ and highly dependent on maintaining a certain level of public confidence. This is particularly so in the current economic environment, where customers are placing increased importance on the safety and security of their funds, and banks may not be in a position to refund their customers in the event that there is a run on deposits.

As far as an institution's reputation is concerned, perception is reality. Consequently, the way an institution's constituents *perceive* what it is doing in the fight against money

104 Op cit n43.

¹⁰² Fisse, B., and Braithwaite, J., The Impact of Publicity on Corporate Offenders (1983) 289.

¹⁰³ Argenti, P.A., 'The Challenge of Protecting Reputation', *Financial Times* (London), 30 September 2005 http://news.ft.com/cms/s/7da92b26-3107-11da-ac1b-00000e2511c8,dwp_uuid=358e659a-2068-11da-b59e-00000e2511c8.html at 19 April 2006.

laundering and terrorism financing, is equally important as what it is *actually* doing. Claims that a financial institution has been involved with money laundering or terrorism financing do not need to be publicly substantiated or legally proven to wreak havoc on its reputation. As is further explored in **Chapter 7** of this thesis, this fact has been demonstrated in recent years by largely unsubstantiated claims involving Banco Delta Asia, a financial institution based in Macau.

Over the past decade, many consultants, AML/CTF practitioners and regulatory officials have touted the potential reputational costs associated with poor AML/CTF controls and/or the commission of a money laundering or terrorism financing offence. They have held that even where an institution's reputation has been polished for several years, adverse publicity tying it to money laundering or terrorism financing activities (whether or not due to ineptitude, malfeasance or simply bad luck on the part of the institution)¹⁰⁶ may undermine public confidence in its integrity and destabilise its operations.¹⁰⁷ Some industry experts have gone further and claimed that an institution that fails to identify its ML/TF risk and/or implement appropriate AML/CTF controls may develop an "adverse reputation among money launderers or financers of terrorism as being an easy channel through which to operate".¹⁰⁸

The theory that money launderers and terrorism financiers may flock to institutions considered to be non-compliant with AML/CTF regulations, is relatively common. However, it is largely untested (presumably due to the inherent difficulties in measuring its accuracy) and as a result, its validity remains questionable. Contrary to popular belief, it might be that money launderers and terrorism financiers actually prefer to conduct their activities through institutions that are perceived by regulators to be 'clean'. Whilst it may prove more difficult to place 'dirty' funds with AML/CTF compliant institutions, such entities are unlikely to

Economist Intelligence Unit and PricewaterhouseCoopers, Taming Uncertainty: Risk Management for the Entire Enterprise (2002) PricewaterhouseCoopers 2

http://www.pwc.com/images/gx/eng/fs/111802taming.pdf at 11 August 2006.

¹⁰⁶ Op cit n39.

¹⁰⁷ On cit n49

See O'Callaghan, T., and Alfano, J., Money Laundering and the Financing of Terrorism: Back to Basics (2007) Money Management http://www.moneymanagement.com.au/Article.aspx?ArticleID=215380 on 23 March 2008.

attract the kind of unwanted regulatory scrutiny and/or review that may uncover the illicit source of those funds. Though it may be contrary to common perceptions of reputational risk, further research is required to determine if in some cases, a positive reputation may actually heighten an institution's vulnerability to more sophisticated money laundering and terrorism financing techniques.

Whilst further study is necessary to determine whether a financial institution's exposure to money laundering and terrorism financing will typically be increased or decreased by an unfavourable corporate reputation, it is clear that an institution's reputation may be its greatest asset. As the business models typically used by financial services firms are founded on safety and security, any shadow cast on their integrity can give rise to both reputational and financial damage.

As an institution's reputation is simply a reflection of facts, perceptions and expectations, a number of risk management texts claim that it may be a key factor in determining its share price. According to some estimates, an entity's reputation may account for as much as four per cent of its share price. Given that the value of an institution's shares represents the present value of its expected future dividend stream (discounted at a rate which takes into account related risk and expected growth) plus its additional reputational assets, it follows that an institution's association with money laundering or terrorism financing can potentially weaken its share price. Non-compliance with AML/CTF regulations may lead to a perception within the market that an institution has a poor control environment that might ultimately erode its expected future cash flows or increase its rate of return. It may give

¹⁰⁹ Doerig, H., Operational Risks in Financial Services: An Old Challenge in a New Environment (Credit Suisse Group, Switzerland, 2001) 24.

Cowan, A., 'Scarlet Letters for Corporations? Punishment by Publicity under the New Sentencing Guidelines' (1992) 65 Southern California Law Review 2367.

See Louisot, J., 'Risk Management in Practice: Reputation' (2004) 6(3) Risk Management: An International Journal 35.

¹¹² Aon Corporation, Corporate Reputation: Not Worth Risking (2003)

http://www.aon.com/about/publications/pdf/issues/wharton_corp_rep_r040303.pdf at 19 April 2006.

Perry, J., and de Fontnouvelle, P., Measuring Reputational Risk: The Market Reaction to Operational Loss Announcements (2005) Federal Reserve Bank of Boston

<http://www.bos.frb.org/bankinfo/qau/jppd1005.pdf> at 30 March 2006.

rise to a loss of current or future customers, an exodus of staff, ¹¹⁴ a reduction in current or future business partners, and increased costs associated with fines and other remedial actions. ¹¹⁵

The ability of reputational damage to cause corresponding financial damage highlights the need for institutions to adopt and execute a strategy for managing the reputational risk they face as a result of money laundering and terrorism financing. That said, not all of the traditional risk management strategies will be appropriate for managing such risk. For instance, given that a financial institution's competitiveness is likely to be hinged somewhat upon its reputation for safety and security, ¹¹⁶ it would not be commercially sagacious for a bank to simply 'accept' its ML/TF risk. Rebuilding a tarnished reputation may be a lengthy, arduous and costly process, ¹¹⁷ and it would be commercially unwise (if not altogether reckless) for an institution to identify – but do little about – the risk posed to its reputation by money laundering and terrorism financing.

In addition to an acceptance risk management strategy, risk transfer is also unlikely to offer institutions a comprehensive solution to managing their reputational risk. Although insurance may address certain facets of reputational damage, ¹¹⁸ no comprehensive coverage is yet available for reputational risk due to the inherent difficulties in determining the value of an institution's reputation, and the possible cost of restoring it. ¹¹⁹ Similarly, risk avoidance also does not offer financial institutions a complete solution to managing their reputational risk. As money launderers and terrorism financiers can theoretically infiltrate any area of an institution's business, an institution cannot entirely avoid its related reputational risk without foregoing all of its operations. Clearly, this is an impossible outcome for institutions and an

¹¹⁴ Op cit n103.

¹¹⁵ Op cit n113.

¹¹⁶ Op cit n109.

Lowthers, B., and Shultz, C., 'Integrating Identity Verification into Risk Management' (2004) 25(11) ABA Bank Compliance 36.

¹¹⁸ For instance, liability insurance may cover the costs of any arising litigation, additional coverage may cover the costs of business interruption, and limited crisis-communication coverage may cover some of the costs associated with necessary public relations and advertising campaigns.

119 The cost of restoring a company's reputation may be dependent upon factors such as the size of the

The cost of restoring a company's reputation may be dependent upon factors such as the size of the company, the number and nature of markets the company operates in, and the crisis management skills of the company's senior management team. See Harris, R., Op cit n39.

undesirable one for AML/CTF regulators. Risk-based approaches to AML/CTF do not seek to prohibit institutions from conducting business in higher risk areas. On the contrary, they enable institutions to conduct activities and enter into relationships representing a higher ML/TF risk, provided that the risk is addressed through appropriate risk-based systems and controls.

Although an avoidance strategy does not offer institutions a holistic solution to managing their reputational risk, institutions may nevertheless limit their exposure by ceasing to operate those parts of their business representing the greatest ML/TF risk. Whilst this might cause a significant loss of funds for an institution, it nevertheless appears possible for an entity to discontinue its riskiest business activities and still exploit their potential to generate profits. To illustrate, private banking is generally regarded as carrying a greater exposure to money laundering because it involves the discrete delivery of financial services to high networth individuals. 120 In September 2005, banking giant Union Bank of Switzerland (UBS) sold its upmarket funds management group and three Swiss private banks to Bank Julius Baer for CHF3.8 billion (AUD\$3.5 billion) in cash and a 21.5 per cent stake in the Julius Baer Group. 121 Presumably, the primary motivation behind this sale had little to do with the mitigation of ML/TF risk. However, by selling these higher risk businesses and maintaining a financial stake in them, UBS has effectively shifted some of its ML/TF reputational risk to another entity whilst still financially benefiting from their operation. If any of the private banking accounts sold to Julius Baer were subsequently tied to money laundering or terrorism financing, Julius Baer would likely bear the brunt of any resulting reputational damage. Although UBS would likely be financially affected by such an occurrence, the bank's brand would presumably be left unscathed due to the fact that Julius Baer maintained operational responsibility for those businesses.

Thus, given that institutions are currently unable to holistically manage their reputational risk through acceptance, transfer or avoidance strategies, their most viable option is to mitigate such risk. Though unable to eliminate the reputational risk they face as a result of money

¹²⁰ See Small, R.A, 'Vulnerability of Private Banking to Money Laundering Activities' (Testimony before the Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate, 10 November 1999).

Wright, T., 'UBS Sells 3 Private Banks to Another Unit of a Rival', *The New York Times* (New York), 6 September 2005, C.2.

laundering and terrorism financing activities, institutions will nevertheless be capable of reducing their risk by encouraging sound project management ¹²² and implementing AML/CTF controls commensurate to their risk. By establishing an appropriate AML/CTF program, an institution may go beyond simply maintaining its reputation, to enhancing it in the eyes of both the public and regulatory authorities.

2.5 Systemic risk

The concept of systemic risk recognises that risk cannot be compartmentalised because it is innately endogenous and capable of being transmitted amongst institutions and between markets. According to the Bank for International Settlements, the term 'systemic risk' refers to the possibility that a market participant's failure to meet its contractual obligations may cause other participants to default and, through a chain reaction, lead to broader financial difficulties. However, in recent years that definition has been extended beyond the risk inherent in traditional lending, to embrace market participants' interdependencies and common risk factors in a far more general sense. The concept of systemic risk now embraces the risk attached to a range of operational activities and exposures, including exposure to reputational risk.

Financial institutions are *directly* linked through interbank deposits, loans and payment system clearings, and *indirectly* linked through their operation in the same (or similar) markets. Due to the existence of these complex financial interrelationships, systemic risk is particularly prevalent within the financial services sector. Adverse shocks are typically transmitted more rapidly within the financial services industry than many others industry

¹²² Op cit n111

¹²³ Systemic risk recognises that risk is not independent of market participants' own actions but rather, is determined by the *collective* behaviour of individual market players. See Crockett, A., 'Introductory Remarks' (Speech delivered at the Third Joint Central Bank Research Conference on Risk Measurement and Systemic Risk, Basel, 7 March 2002) 2.

Bank for International Settlements, 64th Annual Report (BIS, Switzerland, 1994) 177.

¹²⁵ Icard, A., 'Risk Measurement and Systemic Risk' (Speech delivered at the Fourth Joint Central Bank Research Conference on Risk Measurement and Systemic Risk, Frankfurt, 8 November 2005).

¹²⁶ Kaufman, G.G, and Scott, E.E., *Does Bank Regulation Retard or Contribute to Systemic Risk?* (Working Paper No. 211, Stanford Law School, California, 2000), 6.

sectors 127 and as a result, the impact of a major bank's indiscretions may cause a "rippling" effect, 128 that proves to be catastrophic for other institutions. 129 If regulatory authorities were to freeze a large proportion of an institution's funds because they were connected to money laundering or terrorism financing, other institutions relying on those funds may be unable to honour their own debts¹³⁰ and/or facilitate their own operations/other transactions, as planned.

An institution that suffers an adverse shock due to money laundering or terrorism financing activities may systemically impact other institutions and/or financial markets in two conflicting ways. 131 The affected financial institution may:

- reduce the aggregate investment in the economy and create a recessionary spill over which decreases the profitability of other banks: 132 and/or
- confer a strategic benefit on remaining banks by enabling them to increase the scope of their operations, build their customer base, and lower their operational costs by acquiring further lending facilities. 133

Indeed, the strength and scope of the two aforementioned impacts will hinge upon the size and importance of the relevant institution adversely impacted by money laundering or terrorism financing. 134 Logically, the larger and more significant a financial institution is, the greater is its systemic importance and the power of any 'ripple effect' arising from its activities. Evidently, the failure of a global financial conglomerate would pose more systemic risk and have greater ramifications for the rest of the financial system than the failure of a small community bank. 135

¹²⁷ Op cit n126, 4.

Baldwin, F.N., 'Exposure of Financial Institutions to Criminal Liability' (2006) 13(4) Journal of Financial Crime 387.

Alexander, K., 'UK Corporate Governance and Banking Regulation: The Regulator's Role as Stakeholder' (2004) 33 Stetson Law Review 991.

Ewing, M.A., Essays in Banking and Systemic Risk (Ph.D., Princeton University, 1998) 3.

Eatwell, J., 'International Regulation, Risk Management and the Creation of Instability' (Speech delivered at the International Monetary Fund, Washington, 1 October 2004) 2.

A recessionary spill over might occur due to a reduction of the aggregate supply of deposits.

Acharya, V.V., Essays in Regulation of Banks and Financial Institutions (Ph.D., New York University, 2001) 4.

Op cit n127, 6.

Herring, R., International Financial Conglomerates: Implications for Bank Insolvency Regimes (Wharton School, Pennsylvania, 2003) 3.

Despite the clear impacts that an institution's failure may have upon other entities conducting similar activities or servicing the same markets, a number of institutions may not acknowledge the possible systemic implications arising from another entity's association with money laundering or terrorism financing. ¹³⁶ Traditionally, some institutions have regarded systemic risk as a negative externality ¹³⁷ that does not need to be priced into their speculative activities. ¹³⁸ Although several international bodies have tried to counter this trend by addressing systemic risk through regulation, risk-based approaches to AML/CTF arguably reinforce such introspective views of risk. They seemingly encourage microeconomic approaches to risk and it is therefore somewhat paradoxical that regulators may seek to use them to inadvertently regulate systemic risk when systemic risk is, by definition, an externality that institutions cannot completely control. ¹³⁹

Given that systemic risk pervades financial markets and the banking industry, individual institutions cannot altogether control or eradicate it through an avoidance, acceptance or risk transfer strategy. However, they can seek to mitigate their systemic risk by instituting controls that minimise the possible effects that another bank's failure may have on it, and the possible effects that its own operations or ultimate failure may have on other banks. Even when operating in jurisdictions with risk-based approaches to AML/CTF, institutions should still assess whether the actions and policies that seem desirable for them individually, might result in adverse consequences systemically. ¹⁴⁰

One of the most pertinent examples of the systemic risk that may flow from a financial institution's facilitation of money laundering activities, is the Bank of Credit and Commerce International (**BCCI**). BCCI operated under a dual banking structure, through an impenetrable series of holding companies, affiliates, subsidiaries, insider dealings and

Davis, H., 'A New Regulator for the New Millenium' (Speech delivered at the Proceedings of Financial Services Authority Conference: A Radical New Approach to Regulation, London, 11 December 2000).

Externalities may be defined as those costs and benefits accruing to society which are *external* to the calculations of the individual investor, and not accounted for in the market place. See Eatwell, J., Op cit n131. ¹³⁸ Eatwell, J. and Taylor, L., *Global Finance at Risk: The Case for International Regulation* (2000) 7-10.

Op cit n131, 5.

¹⁴⁰ Op cit n123.

nominee relationships.¹⁴¹ This complex and convoluted corporate structure not only increased the bank's risk of being exploited for money laundering purposes, but hindered the ability of regulatory authorities to identify if this was in fact occurring. This became apparent after regulatory and law enforcement officials identified that BCCI had a history of:

- evading legal restrictions on cross border movements of currency;
- maintaining offshore accounts holding large and undetected sums of money; and
- laundering millions of U.S. dollars for its customers, many of whom were high net-worth individuals seeking to hide the proceeds of their illegal enterprises. 142

Once BCCl's money laundering activities were brought to light in 1991, the central banks of various countries blocked the institution's transactions and froze its accounts in order to limit the systemic risk stemming from its failure. However, this did not prevent substantial damage occurring to many smaller financial sectors where the bank operated, ¹⁴³ or spare BCCl's customers from having to deal with the disarray of international bankruptcy proceedings. BCCl's money laundering activities not only impacted its own customers, but also had broad consequences for other institutions without any direct, commercial ties to the bank. By way of example, following the BCCl scandal, a number of foreign institutions found it considerably more difficult to obtain approval to operate in the U.S. Those that were able to do so, faced more onerous legislative requirements and levels of regulation. ¹⁴⁴ Evidently, in the financial services industry, where institutions are often interlinked and interconnected on a number of levels, the involvement of one large bank in a money laundering or terrorism financing scandal can have far-reaching and potentially unforeseen implications for consumers, institutions, financial markets and jurisdictions alike.

The non-bank holding company, BCCI Holdings SA, owned two separate banks that serviced two separate jurisdictions. Whilst one of the banks conducted business through 47 branches in 13 countries, the other operated 63 bank branches in 28 countries.

¹⁴² Kerry, J., and Brown, H., *The BCCI Affair*, Report to the Committee on Foreign Relations, United States Senate, 102d Congress 2d Session Senate Print 102-140, 1992.

¹⁴³ Countries including Bangladesh, Bahrain and Cyprus all suffered significantly as a result of BCCI's AML/CTF failures. Op cit n135, 17. See also International Monetary Fund, Offshore Financial Centers: The Role of the IMF (2000) < http://www.imf.org/external/np/mae/oshore/2000/eng/role.htm at 13 May 2006.

¹⁴⁴ United States Congress, Office of Technology Assessment, Information Technologies for Control of Money Laundering, OTA-ITC-630 (U.S. Government Printing Office, Washington D.C., 1995) 15.

2.6 Credit risk

Credit risk is considered the oldest banking risk¹⁴⁵ and it concerns the possibility that borrowers may default on their loans.¹⁴⁶ Although generally overlooked in AML/CTF literature, there are three primary types of credit risk – consumer risk, company risk and country risk.¹⁴⁷ Interestingly, two of these appear to align neatly with the 'three bases' of risk commonly used by financial institutions to assess their ML/TF risk.

Though it may not otherwise be readily applicable to the advent of money laundering or terrorism financing, credit risk nevertheless bears some relevance to institutions trying to mitigate the risks represented by such crimes. The relevance of credit risk is perhaps most apparent where a financial institution has a number of accounts/transactions frozen under AML/CTF legislation because they relate to persons involved with, or involve funds traceable to, illicit activities. In such a scenario, the freezing of the relevant funds might have credit implications both for the institution at hand, and any other entity seeking to lay claim to those now irretrievable funds.

An institution's credit risk in relation to money laundering and terrorism financing will clearly be heightened where it lacks adequate knowledge regarding its customers' identities, businesses, and relationships with other borrowers. A complex lending transaction, coupled with inadequate or poorly executed Know Your Customer (**KYC**) procedures, may lead to loan arrangements with undesirable or fictitious customers. Loan arrangements involving "related counterparties, connected borrowers, and a common source of income or assets for repayment" will not only increase an institution's credit risk, 149 but also its risk of

¹⁴⁵ Caruana, J., 'Contemporary Issues in Credit Risk', (Speech delivered at the Credit Risk Summit USA 2003, New York, 27 October 2003).

In this context, 'default' means failing to fulfil contractual obligations in a timely manner, due to inability and/or unwillingness. See Lam, J., Enterprise Risk Management: From Incentives to Controls (2003).

World Bank, Analyzing and Managing Banking Risk: A Framework for Assessing Corporate Governance and Financial Risk (2nd ed, 2003) 135.

¹⁴⁸ World Bank, Money Laundering Impacts Development

<hathered="http://www1.worldbank.org/finance/html/amlCTF/docs/Ref Guide_EN/v2/02-Ch02_EN_v2.pdf">http://www1.worldbank.org/finance/html/amlCTF/docs/Ref Guide_EN/v2/02-Ch02_EN_v2.pdf</hd>
at 1 April 2006

The greater the number of parties involved in any loan transaction, the more difficult it will potentially be for the lending institution to recoup its funds. In the event that the primary borrower defaults, any related counterparties and/or connect borrowers may be given first priority in terms of their claim to the monies owed.

conducting business with money launderers and terrorism financiers. Identifying the ultimate or beneficial owners of certain accounts/transactions has occasionally proven to be a difficult exercise for financial institutions, particularly in relation to complex corporate structures. Thus, in order to mitigate their ML/TF risk, as well as their exposure to customers engaged in activities such as fraud and tax evasion, it is necessary for institutions to conduct the necessary due diligence to identify these individuals.

Whilst a number of the traditional techniques for credit risk minimisation are not applicable to the issues of AML/CTF (e.g. the taking of security facilities), financial institutions can still minimise their credit risk exposure through the use of a risk mitigation strategy. By establishing an effective due diligence regime aimed at understanding their customers' business interests and accurately identifying the beneficial owners of accounts, institutions can decrease their risk of engaging in loan arrangements with known criminals or terrorists. Further, they can minimise their credit risk by pinpointing the existing and potential risks inherent in their lending activities, 150 and addressing them through diversification and the underwriting of loans.¹⁵¹

Unlike the assessment of ML/TF risk, the measurement of credit risk has developed into a relatively precise science. Institutions now have access to significant amounts of statistical and historical data when calculating the credit risk associated with a particular borrower. By comparison, ML/TF risk does not lend itself to such methodical assessment. Firstly, there are limited amounts of data available with respect to ML/TF risk so its measurement is far more subjective than credit risk. Whilst there are accepted methodologies for the assessment of credit risk, ML/TF risk cannot be mathematically calculated. Even with the availability of money laundering typologies and a number of guidance notes from international bodies, there is no globally accepted standard with respect to accurately gauging ML/TF risk. Unlike credit risk, the methods used to assess the ML/TF risk attached to a particular customer or jurisdiction are more imprecise – potentially varying widely and drawing on subjective assessments of risk.

¹⁵⁰ Op cit n147. 151 Op cit n146.

2.7 Operational risk

According to the Basel Committee, 'operational risk' is the risk of directly or indirectly suffering loss as a consequence of inadequate internal processes, people and systems, or external events. Since it rose to prominence in the early 1990s following a series of operational failures by several financial institutions (most notably, Barings Bank), the need for institutions to address their operational risk has steadily escalated. This is largely due to the introduction of international capital adequacy regulations, the growing diversity of financial products/services, and the increasingly automated environment in which such products/services are delivered.

Unlike many other traditional types of risk, operational risk can itself give rise to the commission of money laundering or terrorism financing activities. Rather than the risk and damage that may result from an institution's alleged or actual involvement in a ML/TF offence, it is concerned with the possibility that an institution's internal weaknesses may create an 'operational failure risk' or an 'operational strategic risk' that leads to an AML/CTF compliance failure and an array of other risks (e.g. reputational risk). Whilst an operational failure risk arises internally as a result of an institution's people, processes or technology, an operational strategic risk arises externally from environmental factors beyond an institution's control. Is should be noted however that an operational strategic risk linked to ML/TF can inevitably translate into an operational failure risk. For example, whilst amendments to AML/CTF legislation will represent a strategic risk for an institution, any failure on the part of that institution to comply with the revised legislation will constitute an operational failure risk.

Suresha, R., and Karthik, K.V., *Mitigating Operational Risk – An Approach to Countering Money Laundering*, Iflex Consulting http://www.iflexconsulting.com/Expertise/mitigate.pdf at 2 June 2006.

Keenan, C., 'Overview: Will Risk Fixes Boost Competitive Edge?' (2003) 168(235) American Banker 12.

Herbert, C., Five Ways to Manage Operational Risk in an Even Riskier World, IBM Australia http://www-8.ibm.com/nz/media/downloads/IBMarticles/Operational_risk.pdf at 23 May 2006.

¹⁵⁵ Mantas Inc. and Celent Communications, White Paper: Using Behaviour Detection to Identify Operational Risk (2003)

http://www.mantas.com/GlobalAssets/PDF/WhitePapers/CelentOperationalRisk.pdf> at 1 April 2006. 156 Op cit n62.

As evidenced by a number of AML/CTF compliance failures, ML/TF risk may be closely related to operational risk. In several highly publicised cases, an institution's facilitation of money laundering activities has been attributed to its employees, technology or inadequate AML/CTF program. Given that no AML/CTF compliance program can be entirely technological, it is often the interaction between its technological and human components that carries the greatest operational risk. As later discussed in this thesis, some of the most notable penalties incurred by institutions under AML/CTF legislation have stemmed from the non-compliant activities of particular employees, and the inability of poorly implemented systems/compliance programs to prevent or detect their behaviour.

Operational risk can arise in unpredictable circumstances and is, to differing degrees, inherent in all business activities. Thus, whilst institutions can never eradicate their operational risk, they can nevertheless mitigate such risk by implementing an AML/CTF program, conducting appropriate staff training, and periodically subjecting their AML/CTF systems and controls to independent reviews. Further, they can seek to minimise their exposure by attempting to periodically quantify the operational risk they face in relation to money laundering and terrorism financing.

Financial institutions traditionally measured their operational risk using subjective selfassessments. However, given that several large banks have suffered significant financial loss during the past decade as a result of inaccurate self-assessments, more sophisticated institutions are now attempting to develop more reliable methods of measuring their operational risk. 157 Nevertheless, the quantification of operational risk still remains inherently difficult because such risk is generally context dependent and its primary drivers – institutional staff and institutions themselves – are unique and ever evolving. Only 'high probability/low impact' events with little context dependency will provide institutions with enough observable data to measure their operational risk level. ¹⁵⁸ Such events may lend

Op cit n156.
Op cit n109, 94.

themselves to statistical analysis and enable institutions to identify their prevalence by collecting data on their occurrence over an extended period.¹⁵⁹

By comparison, statistical analysis cannot be usefully applied to 'low probability/high impact' loss events. ¹⁶⁰ Large money laundering and terrorism financing scandals arguably fall within this category of events because they are so highly context dependent that institutions may only be capable of tracking the associated changes in their operational risk levels over time. In any event, it is unlikely that any institution could effectively gauge its own operational risk by simply monitoring the highly publicised AML/CTF scandals involving other institutions. Low probability/high impact loss events are hinged upon an institution's particular circumstances and the nature of the individuals involved. Consequently, the context dependency of operational risk means that such events do not generally provide reliable indicators of the risk that other institutions may face in the future.

However, it is perhaps unimportant that institutions are largely incapable of quantifying their operational risk in relation to low probability/high impact money laundering events. Whilst it is important for institutions to identify their potential exposure to such events, it is not always necessary that they precisely calculate the operational risk they face as a result of such events. Indeed, risk-based approaches to AML/CTF only require institutions to create an internal control environment that is commensurate to the level of ML/TF risk that they might *reasonably* face. Requiring institutions to specifically tailor their AML programs to low probability/high impact loss events would likely be a costly and resource-intensive exercise – and potentially one that provides little benefit to regulatory authorities.

It is clear that measuring the operational risk attached to money laundering and terrorism financing events will often prove to be difficult for institutions. Such crimes typically involve tangled webs of complex behaviours, ¹⁶¹ and the overriding risk level can only be assessed once an overall behaviour (or pattern of behaviour) is identified. Whilst many institutions are trying to assess their levels of operational and ML/TF risk by building

¹⁵⁹ Op cit n155.

¹⁶⁰ Ibid.

¹⁶¹ Ibid.

behavioural and transaction monitoring into their compliance programs, detection can still be problematic. The individual transactions used to facilitate money laundering or terrorism financing may occur over a period of time and be buried amongst millions of similar transactions. They might also be obscured by the ability of money launderers and terrorism financiers to continually alter their behaviour and evade older, outdated detection techniques. Thus, although behavioural and transaction monitoring systems cannot eliminate the operational risk represented by money laundering and terrorism financing activities, such technologies can assist institutions to better understand their risk levels and mitigate them accordingly.

2.8 Conclusion

Over the past few decades, money laundering and terrorism financing have emerged as significant political and international issues. Whilst AML attracted a degree of attention during the 1980s and 1990s, the events of September 11 provided a graphic demonstration of the need for governmental AML/CTF efforts to be cohesive and coordinated. It is now widely accepted that any strategies aimed at addressing money laundering and terrorism financing must involve the cooperation of financial institutions, regulatory authorities and law enforcement officials if they are to be successful. Accordingly, financial institutions can no longer sit idly and expect national governments to combat money laundering and terrorism financing activities without private sector engagement. Indeed, many international bodies and national governments now recognise the integral role that financial institutions must play in safeguarding the international financial system, and assisting governments to identify (and combat) predicate offences.

Since 2001, a number of jurisdictions have enacted risk-based AML/CTF legislation requiring institutions to assess their individual levels of ML/TF risk. To fulfil their legislative AML/CTF obligations, many institutions are now framing their overall ML/TF risk in terms

¹⁶² Ihid.

of their customer risk, product/channel risk and jurisdiction risk.¹⁶³ It is believed that by using these 'three bases' of risk, institutions can identify, manage and mitigate their areas of greatest money laundering and terrorism financing exposure.

However, whilst customer risk, product/channel risk and jurisdiction risk typically underpin risk-based approaches to AML/CTF, there appears to be some value in contextualising ML/TF risk in terms of older, more traditional types of risk. Though ML/TF risk might not fit neatly within the confines of all such risk types, viewing it through the lens of traditional risks will enable institutions to better understand the broader consequence risk that money laundering and terrorism financing represent to their businesses. It will allow them to extend their analysis beyond the likelihood of money laundering and terrorism financing infiltrating their operations (which is inherently what the 'three bases' of risk seek to identify), to the possible ramifications attached to such an occurrence. By contextualising ML/TF risk in terms of traditional risk types, institutions may also gain a better insight into the practical approaches and strategies that they may employ to manage their ML/TF risk and/or mitigate the fallout stemming from any money laundering or terrorism financing event.

A number of AML/CTF professionals, media commentators and regulatory authorities have emphasised the potential damage that an institution may sustain following the commission of a money laundering or terrorism financing offence and/or an AML/CTF compliance failure. Many have repeatedly held that an institution connected to money laundering or terrorism financing activities may incur significant financial damage and irreparable reputational damage. In today's increasingly diverse and regulated financial markets, it is clear that money laundering and terrorism financing pose an array of risks for financial institutions. However, due to the fiercely competitive nature of the financial services industry, the speed with which AML/CTF compliance failures can be broadcast to a global audience, and the lack of clarity regarding what some regulators will deem to be appropriate risk-based systems and controls, the extent of (and potential consequences attached to) an institution's ML/TF risk remains largely unquantifiable. This is perhaps one of the primary reasons for

¹⁶³ It should be noted that in certain jurisdictions, AML/CTF legislative instruments actually require financial institutions to assess their ML/TF in terms of these separate types of risk. For instance, see Australia's Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) (Cth).

the almost unquestioned acceptance of widely publicised claims that involvement in a money laundering or terrorism financing scandal may carry disastrous consequences and, in some cases, prove to be institutionally fatal.

Chapter 3

Looking at AML/CTF Legal Risk through the Lens of Criminal Law

"He who profits by a crime, commits it" - Sir Walter Scott

3.1 Introduction

Since the events of September 11, a number of significant changes have been made to the U.S. political and regulatory landscape. Expansive AML/CTF laws have been enacted, harsher criminal sanctions have accompanied AML/CTF compliance failures, and institutions have been confronted with a spate of new corporate responsibilities. According to some commentators, these changes have meant that financial institutions are now exposed to an increased risk of incurring criminal liability in relation to money laundering and terrorism financing offences, and/or breaches of AML/CTF legislation.

Since the enactment of the *USA PATRIOT Act* in 2001, financial institutions operating in the U.S. have been required to implement an effective AML/CTF compliance program, comply with additional reporting and KYC requirements, and employ a range of other AML/CTF controls. Whilst these extended obligations have certainly heightened the regulatory burden placed upon financial institutions, the AML/CTF legal risk faced by organisations has also increased, at least theoretically, as a result of the allegedly more aggressive enforcement of AML/CTF laws by U.S. regulatory authorities.¹⁶⁴

In general terms, an institution's AML/CTF legal risk is the chance of it facing litigation (including civil actions and criminal prosecution), adverse legal judgments, unenforceable contracts, fines and other legal penalties as a result of non-compliance with AML/CTF legislation. As opposed to ML/TF risk, which is solely concerned with the risk represented by money laundering and terrorism financing (i.e. in and of themselves), AML/CTF legal

Vartanian, T.P., 'Money Laundering Dominates Bank Enforcement Actions' (2004) 169(185) American Banker 10.

¹⁶⁵ Op cit n148.

risk is more outward-looking as it concerns the risk represented by non-compliance with municipal and/or extraterritorial AML/CTF laws. In the context of risk-based approaches to AML/CTF, such non-compliance is not limited to the deliberate facilitation of money laundering or terrorism financing, or even the inadvertent contravention of prescriptive legislative requirements. It can also arise as a consequence of an institution's failure to identify, mitigate and manage its ongoing ML/TF risk.

Whilst **Chapter 4** of this thesis explores AML/CTF legal risk in the context of civil law, this Chapter focuses on an institution's risk in relation to the initiation of criminal enforcement proceedings and the imposition of criminal penalties. It provides an overview of the ways in which an institution and/or its employees may be held criminally liable for non-compliance with local or foreign AML/CTF laws. Further, it assesses the veracity of the oft-published claims that an institution linked to a money laundering or terrorism event is likely to face criminal charges, financial damage and a loss of market share. For the purposes of discussion, this Chapter is divided into several broad topic areas, including the:

- principles underpinning the imputation of criminal liability to corporate entities;
- criminal penalties that can accompany a money laundering or terrorism financing offence and/or a breach of AML/CTF legislation;
- apparent frequency (or otherwise) with which criminal proceedings are invoked and criminal penalties are imposed upon a non-compliant institution;
- extraterritorial laws and sanctions creating an additional layer of regulatory requirements for institutions; and
- willingness of regulatory authorities and the courts to pursue criminal breaches of AML/CTF legislation.

As discussed in **Chapter 1** of this thesis, the U.S. is predominantly used as a case study for AML/CTF regulation because it has some of the most visibly enforced AML/CTF laws, as well as some of the strongest legislative expressions of extraterritoriality. In recent years, the U.S. has hosted some of the most highly publicised criminal enforcement actions for breaches of AML/CTF laws. Further, it has seen some of the most damaging penalties given to institutions for such breaches. As opposed to a number of other jurisdictions such as

Australia, where no institution has yet been criminally prosecuted for breaches of the country's *AML/CTF Act 2006* (Cth), there is a wealth of information available for the purposes of analysing the levels and types of risk faced by institutions operating under the U.S. AML/CTF regime.

Given the nuances of U.S. AML/CTF laws and the U.S. enforcement environment, it is recognised that the analysis contained in this Chapter will not be equally relevant to determining the AML/CTF legal risk faced by institutions operating under different AML/CTF regimes. Similarly, where analysis is provided with respect to the AML/CTF legal risk faced by institutions in other countries, this will not necessarily be applicable to the experiences of those operating in the U.S. Nevertheless, whilst a number of nation states are still in the process of drafting, enacting and implementing their AML/CTF laws, and/or otherwise developing their enforcement environments, the U.S. experience provides an interesting case study for determining just how great the AML/CTF legal risk faced by institutions can actually be. This is particularly so, given that the country is often considered to be (whether rightly or wrongly) the international vanguard in terms of AML/CTF regulation and enforcement.

3.2 The concept of corporate criminal liability

Though once considered to be incapable of committing crimes in their own capacity, it is now well established that corporate entities are legal persons capable of holding property, suing and being sued, conducting transactions and, in certain jurisdictions, committing criminal offences and being punished for those offences. Whilst civil law obligations (e.g. contract, tort and restitution) have generally been applied to corporate entities with relative ease, the application of criminal law obligations to such entities has often proved to be more controversial. This is primarily due to the inherent nature of corporate entities (i.e. the fact they are essentially collections of individuals bound together by complex webs of legal rights and duties) and the fact that criminal liability will often hinge upon the existence of 'fault',

Wells, C., Criminal Responsibility of Legal Persons in Common Law Jurisdictions, Paper prepared for OECD Anti-Corruption Unit, Paris, 4 October 2000, 2.

generally in the form of intention, knowledge or subjective recklessness. Nevertheless, at common law there has been a gradual expansion of corporate criminal liability, both in terms of the range of offences that a corporation is capable of committing, and the way in which liability may be imputed to a corporation for such offences.¹⁶⁷

Today, there are a number of legal principles being used by different jurisdictions for the purposes of attributing criminal liability to corporate or legal persons. Firstly, the concept of vicarious liability (referred to in the U.S. as *respondeat superior*) is currently used in many countries to hold a corporation criminally liable for offences committed by its employees/agents in circumstances where:

- such employees/agents had the requisite mens rea; 168 and
- the relevant offences were within the scope of their employment and intended to benefit the corporation.

Transplanted from civil law, the doctrine of vicarious liability is a derivative form of liability because it seeks to equate corporate culpability with that of an individual.¹⁶⁹

For the purposes of finding a corporation vicariously liable for the criminal acts of its employees, it will often be inconsequential whether the conduct of the relevant individual(s) violated corporate policy. In many jurisdictions, a corporation can be held criminally responsible for the activities of its employees even where it had a pristine corporate culture and its executive had taken reasonable steps to prevent their employees from violating the law.¹⁷⁰ In other words, a corporation can be held strictly liable for the crimes of its employees. Although some jurisdictions (such as the U.S.) have endorsed the application of vicarious liability to both strict liability offences and those requiring subjective knowledge,

¹⁶⁷ Op cit n166, 10.

^{168 &}quot;Mens rea" refers to the requisite mental state for a particular offence, e.g. intention or knowledge.

¹⁶⁹ On cit n166 4

Hasnas, J., Rethinking Vicarious Criminal Liability: Corporate Culpability for White-Collar Crime (2006) The Heritage Foundation http://www.heritage.org/Research/LegalIssues/wml195.cfm at 30 December 2008.

others (including England) have restricted the use of vicarious liability to a limited number of strict liability and/or regulatory offences. ¹⁷¹

Secondly, to a theory more widely endorsed in Australian, English and Canadian law, a corporation may be held liable for the culpable transgressions of certain senior corporate officers, i.e. those senior managers regarded as the 'directing mind' of the corporation. Typically referred to as the 'alter ego' or 'identification' theory, this theory was developed by the U.K. courts in the 1940s to overcome the challenges associated with assigning criminal liability to corporate entities for serious offences requiring *mens rea*. Under it, certain key personnel are held to act *as* the company (rather than *on its behalf*, which is the case with vicarious liability).

Indeed, the underlying premise of the identification theory is that a dichotomy exists with respect to those employees who act as the 'hands' of a corporation, and those who act as its 'brains'. It has leading case of *Tesco Supermarkets v. Nattrass* [1972] AC 153, the U.K. House of Lords sought to clarify the types of personnel that may be considered to be at the centre of corporate power. It held that only those individuals who control or manage the affairs of a company will be regarded as embodying or acting as the company itself for the purposes of determining criminal liability. However, whilst this decision has been referred to and relied upon many times, it is uncertain how appropriate its anthropomorphic view of company decision-making and it conceptualisation of corporate 'command and control' now are in respect of the diverse, decentralised models of corporate organisation now being adopted by many entities. 173

Until recently, the only legally recognised ways of attributing criminal fault to a corporate entity were through the concepts of vicarious liability and identification. In the past few years however, a number of jurisdictions have introduced more modern liability rules. These rules

¹⁷¹ The U.S. Supreme Court first accepted the constitutionality of using agency principles to impute criminal responsibility to corporations in N.Y. Central and Hudson River R.R. Co. v. United States, 212 U.S. 509 (1909).

¹⁷² Op cit n166, 5.

This issue, and the various questions it raises, falls outside the scope and purpose of this thesis.

Accordingly, it will not be addressed in this paper and should instead form the subject of further research.

enable corporations in some countries to be imputed with criminal liability as a result of their internal procedures, operating systems or corporate culture. This 'corporate culture' theory differs significantly from the principles of vicarious liability and identification. Rather than equating the acts of certain individuals with those of a corporation, it exploits the distinction between natural and legal persons and focuses on a corporation's liability in its own right.

The most significant aspect of Australia's corporate criminal liability regime is believed to be the statutory provisions providing for organisational liability in relation to federal offences, including on the basis of "corporate culture". ¹⁷⁴ Under Section 12.3 of the federal Criminal Code, a corporation may be deemed to have formed the necessary fault element for a Commonwealth offence if it has "expressly, tacitly or impliedly authorised or permitted the commission of the offence". This will be the case where the:

- corporate culture directed, encouraged, tolerated or led to non-compliance; or
- relevant corporation failed to create and maintain a corporate culture that required compliance.

For the purposes of the legislation, corporate culture is defined as "an attitude, policy, rule, course of conduct or practice existing within the body corporate generally or in the part of the body corporate in which the relevant activities take place".

Whilst the aforementioned methods of attributing criminal liability to a corporate entity are now cemented within the laws of many jurisdictions, it is important to note that corporate criminal liability is not a universal feature of modern legal systems. This is particularly apparent in relation to many civil law countries, where the concept of holding corporations liable for criminal acts is historically unknown. Whilst one of the major impacts of international AML/CTF standards has been a greater acceptance by civil law countries of the need to introduce concepts of corporate criminal liability (for instance, in Switzerland), a number of countries have yet to legislatively provide for the notion of corporate criminal liability. Countries such as Brazil, Bulgaria and Luxembourg currently do not recognise any

Allens Arthur Robinson, 'Corporate Culture' as a Basis for the Criminal Liability of Corporations (2008) 10 < http://198.170.85.29/Allens-Arthur-Robinson-Corporate-Culture-paper-for-Ruggie-Feb-2008.pdf> at 2 January 2009.

¹⁷⁵ Op cit n 174, 4.

form of corporate criminal liability, whilst others including Germany, Mexico and Sweden, only allow for administrative penalties to be imposed on corporations for the criminal acts of certain employees.

3.3 The high price of non-compliance

According to FATF Recommendation 29, effective AML/CTF regulation necessarily relies upon regulators having an appropriate range of supervisory tools available to them. ¹⁷⁶ These tools should ensure that institutions in breach of their AML/CTF obligations are subject to "effective, proportionate and dissuasive criminal, civil or administrative sanctions". ¹⁷⁷ As global concern for money laundering and terrorism financing has increased sharply over the past decade, jurisdictions have sought to comply with FATF Recommendation 29 by providing tougher penalties for non-compliance with AML/CTF laws.

Given that corporate entities are only 'persons' in a strict legal sense, the criminal penalties that may be imposed upon them are somewhat limited. A financial institution cannot be imprisoned, for instance. Traditionally, the penalties attached to non-compliance were relatively insignificant criminal fines. Hand institutions made little effort to meet their AML/CTF legislative obligations, presumably because the seemingly minor consequences associated with non-compliance justified the risk of deviating from their requirements. However, this situation began to change in 1985 following the successful (and highly publicised) U.S. prosecution of the Bank of Boston for tax evasion and violations of federal money laundering regulations. The bank was fined USD\$500,000 for failing to report USD\$1,200 million in cash transactions with foreign banks. Whilst this financial penalty

¹⁷⁶ Op cit n16, 18.

Financial Action Task Force Secretariat, Interpretative Note to Special Recommendation II: Criminalising the Financing of Terrorism and Associated Money Laundering (2004) Asia-Pacific Group on Money Laundering

< http://apgml.org/issues/docs/14/FATF%20Interpretative%20Note%20to%20Sp%20Rec%20II.doc> at 26 July 2007.

Alexander, R.C., Arlen, J., and Cohen, M.A., 'Regulating Corporate Criminal Sanctions: Federal Guidelines and the Sentencing of Public Firms' (1999) 42(1), *Journal of Law & Economics* 393, 395.

Mercator Advisory Group, *Anti-Money Laundering Technology* (2005)

< http://mercatoradvisorygroup.com/index.php?doc=news&action=view_item&type=2&id=156> at 16 October 2006.

may seem relatively immaterial when compared to the profits currently being generated by many financial institutions, it was significantly greater than the fines ordered under AML laws prior to that time. Essentially, the Bank of Boston case put other institutions on notice that non-compliance with AML regulations could result in criminal enforcement proceedings and large financial penalties.

Today, many pieces of municipal and extraterritorial legislation provide criminal penalties for breaches of certain AML/CTF obligations. Institutions may face fines and other criminal repercussions for actively facilitating money laundering or terrorism financing activities and/or otherwise failing to comply with their AML/CTF obligations. Under some AML/CTF regulations, their officers and employees may also be exposed to fines or terms of imprisonment for wilful non-compliance with their obligations.

During the past few years, a number of jurisdictions have started to impose criminal penalties for AML/CTF offences in the upper range of their sentencing guidelines. This is particularly apparent in Europe, where a number of banking regulators have recently imposed the maximum fines possible upon several institutions for breaches of their AML/CTF requirements. However, whilst this indicates that institutions and individuals may face considerable legal risk should they fall foul of applicable AML/CTF laws, it is still questionable how frequently these penalties are invoked.

3.3.1 Show me the money: criminal fines for non-compliance

Fines for institutions

Fines have typically been imposed upon non-compliant institutions to admonish them for their offences, and demonstrate to other entities that AML/CTF compliance failures will not

¹⁸⁰ Op cit n128, 388.

For instance, in October 2008 Sweden's financial regulator, Finansinspektionen, imposed the maximum fine possible upon Forex (a bank operating in Sweden, Denmark, Norway and Finland). The bank had a number of deficiencies in its AML/CTF procedures, and the fine was intended to reflect the graveness of those deficiencies. See Swedish Regulator Fines Forex AB Over \$7 Million for AML Deficiencies (2008) Moneylaundering.com http://www.moneylaundering.com/NewsBriefDisplay.aspx?id=1794 at 16 March 2009.

be tolerated. Regulatory authorities have seemingly been transparent and open about the dual purpose of such criminal penalties. When discussing the USD\$25 million fine imposed upon Riggs Bank in May 2004 for its violations of the *Bank Secrecy Act*, former Financial Crimes Enforcement Network (**FinCEN**) Director, William J. Fox, stated that FinCEN "wanted [the] penalty to hurt" Riggs Bank and send a strong warning to other banks that non-compliance with AML/CTF laws may carry criminal and financial consequences. ¹⁸²

In the U.S., institutions convicted of certain types of federal money laundering offences are sentenced pursuant to the *Organizational Sentencing Guidelines* contained in *Chapter 8* of the *United States Sentencing Guidelines* (**U.S. Sentencing Guidelines**). As outlined in *Chapter 2*, *Part S* (§ 2S) of the 2008 Federal Sentencing Guideline Manual, these Guidelines apply to the following types of money laundering offences:

- under § 2S1.1. of the Guidelines laundering monetary instruments and/or engaging in monetary transactions in property derived from unlawful activity, in contravention of 18 U.S.C. §§ 1956, 1957, 1960; and
- under § 2S1.3. of the Guidelines structuring transactions to evade reporting requirements, failing to report cash or monetary transactions, failing to file currency and monetary instrument reports, knowingly filing false reports, bulk cash smuggling and/or establishing and maintaining prohibited accounts involving certain foreign jurisdictions, institutions or banks, in contravention of various statutory provisions.

Whilst ruling in *United States v. Booker*, 543 U.S. 220 (2005) that the *U.S. Sentencing Guidelines* are merely advisory, the U.S. Supreme Court has held that U.S. District Courts must nevertheless "consult [the Guidelines] and take them into account when sentencing". Thus, as articulated in 18 U.S.C. § 3553(a) and cases such as *United States v. McBride*, 434 F.3d 470, 474 (6th Cir. 2006), the *U.S. Sentencing Guidelines* are simply one

Cocheo, S., 'Dear Director: Watch Out For Tougher Moves When Examiners Review Anti-Money-Laundering Effort' (2004) 24(4-8) ABA Bank Directors Briefing 1, 3.

¹⁸³ These Guidelines are promulgated by the United States Sentencing Commission.

These provisions include, but are not limited to, the following: 18 U.S.C. § 1960, 26 U.S.C. §§ 7203 and 7206, and 31 U.S.C. §§ 5313, 5314, 5316, 5318, 5318A(b), 5322, 5324, 5326, 5331 and 5332.

185 See United States v. Booker, 543 U.S. 220 (2005) at 264.

of a number of factors that the courts must consider when sentencing an individual or an institution for criminal violations of federal AML/CTF laws.

Under the Organizational Sentencing Guidelines, institutions convicted of an offence contained in § 2S of the U.S. Sentencing Guidelines may be ordered to make restitution, adhere to a period of corporate probation for up to five years, 186 and/or pay a fine. Where a fine is imposed, the quantum of that fine will rest upon the perceived severity of the offence(s) and culpability of the defendant institution. In relation to those money laundering and reporting offences covered by §§ 2S1.1. and 2S1.3. of the U.S. Sentencing Guidelines, the severity of an offence will be greater where a defendant:

- committed the underlying predicate offence(s);
- knew or believed that the laundered funds were the proceeds of crime, or otherwise intended to promote unlawful activity;¹⁸⁷
- engaged in the business of laundering funds; ¹⁸⁸ and/or
- conducted "sophisticated laundering". 189

Determining the *culpability of a defendant* is a separate process from determining the *severity of an offence*. Whilst the severity of an offence is determined by reference to the relevant portions of *Chapter 2* of the *U.S. Sentencing Guidelines*, the culpability of a defendant institution is assessed under *Chapter 8* of the Guidelines. In accordance with $\S 8C2.5.$, an institution's culpability is assessed by weighing up a number of different factors. These factors relate not only to the behaviour of (and the controls/programs implemented by) a defendant institution prior to its criminal activity, but to the steps taken

¹⁸⁶ A period of corporate probation may be required where the court wants to secure the payment of restitution/a monetary penalty, improve external monitoring and oversight of an institution's activities, and/or ensure that an institution implements appropriate corrective measures. See § 8D1.1. of the U.S. Sentencing Guidelines.

Under § 2S1.1. specifically, the 'severity' of a money laundering offence will be greater where a defendant knew or believed that any of the laundered funds were the proceeds of, or were intended to promote (i) an offence involving the manufacture, importation or distribution of a controlled substance or a listed chemical; (ii) a crime of violence; or (iii) an offence involving firearms, explosives, national security, or the sexual exploitation of a minor.

In determining whether a defendant institution was in the 'business' of laundering funds, the court may consider a range of factors, including whether the institution regularly laundered funds, laundered funds over an extended period of time, and/or generated revenues in return for laundering funds.

Sophisticated laundering typically involves the creation/use of fictitious entities, shell banks, offshore financial accounts, and/or layers of transactions.

by that institution following the commission/identification of such activity. Whilst different factors have the ability to increase or decrease a defendant's culpability, an institution's culpability will be greater where:

- high level personnel were involved in, or wilfully blind to, the criminal conduct $(\$ 8C2.5(b));^{190}$
- there is a recent history of similar misconduct ($\S 8C2.5(c)$);
- the offence constitutes a violation of a previous court order or a period of corporate probation ($\S 8C2.5(d)$); and/or
- there has been wilful obstruction or a deliberate attempt to obstruct justice during any investigation, prosecution or sentencing of the alleged offence(s) ($\S 8C2.5(e)$).

In 2002, Broadway National Bank became the first U.S. financial institution following the enactment of the *USA PATRIOT Act* to be criminally prosecuted for breaching federal AML/CTF laws. The bank pleaded guilty to a three-count felony Information that charged it with failing to maintain an AML/CTF program, failing to report USD\$123 million in suspicious cash deposits, and structuring USD\$76 million in transactions to evade currency reporting requirements. ¹⁹¹ After considering the institution's modest revenues, the seriousness of its conduct and its attempts at reform, a U.S. District Court fined Broadway National Bank USD\$4 million; making it also the first institution to incur a criminal fine for an AML/CTF compliance failure post-September 11.

Whilst the USD\$4 million fine imposed might appear meagre when compared to the USD\$199 million involved in Broadway National Bank's offences, the fine was simply the 'tip of the iceberg' in terms of the penalties that U.S. regulatory and judicial officials would subsequently impose upon institutions for AML/CTF compliance failures. More recent regulatory actions have seen some institutions incur fines more than 20 times that imposed upon Broadway National Bank just several years ago. For instance, on 20 December 2005, a

¹⁹⁰ See also Van Cleef, C.R., Silets, H.M., and Motz, P., 'Does the Punishment Fit the Crime?' (2004) 12(1) *Journal of Financial Crime* 56, 57.

¹⁹¹ United States Customs and Border Protection, Manhattan Bank Pleads Guilty to U.S. Criminal Charges for Failure to Report \$123 Million in Suspicious Cash Deposits (2002)

http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/legacy/2002/112002/11272002.xml at 25 July 2007.

U.S. court ordered ABN Amro N.V. to pay USD\$80 million in fines and penalties for failing to prevent money laundering, failing to report suspicious activity, violating U.S. Office of Foreign Assets Control (**OFAC**) sanctions and inadequately training staff in relation to their AML/CTF obligations. ¹⁹²

Though it tends to undercut much of the rhetoric about the aggressive regulatory pursuit of AML/CFT compliance, the sizeable criminal fines imposed upon institutions such as ABN Amro N.V. appear to be the exception rather than the rule as far as AML/CTF enforcement is concerned. Whilst the size of the penalties imposed upon Riggs Bank, the Bank of New York and ABN Amro might suggest that all institutions operating in the U.S. face relatively high levels of AML/CTF legal risk, U.S. sentencing statistics do not readily support this view. Official reports released by the U.S.S.C. indicate that whilst the risk of incurring a large criminal fine for money laundering offences is rising for institutions in the U.S., a successful prosecution will not necessarily result in the payment of a large monetary penalty.

According to Table 51¹⁹³ in the U. S. Sentencing Commission's 2006 Sourcebook of Federal Sentencing Statistics (**U.S.S.C. 2006 Sourcebook**), during the 2006 fiscal year¹⁹⁴ there were ten corporate defendants sentenced under the Organizational Sentencing Guidelines where money laundering was their sole, or primary, criminal offence.¹⁹⁵ Of these defendants, only one was ordered to pay a monetary fine (the quantum of which is not outlined in the U.S.S.C. 2006 Sourcebook) and only one was required to make restitution. The remaining eight were neither ordered to pay a fine, nor ordered to make any restitution for their criminal conduct.

However, whilst these figures imply that the risk of an institution being fined and/or ordered to make restitution for a money laundering offence is negligible in the U.S., the U.S.

Simpson, G.R., 'ABN Amro to Pay \$80 Million Fine Over Iran, Libya', *The Wall Street Journal* (New York), 20 December 2005, A.3.

¹⁹³ This table is formally titled "Organizations Receiving Fines or Restitution by Primary Offense Category and Applicability of Chapter 8 Fine Guidelines".

¹⁹⁴ The 2006 fiscal year ran from 1 October 2005 to 30 September 2006 inclusive.

These ten cases constituted 4.6% of the total cases sentenced in accordance with Chapter 8 of the U.S. Sentencing Guidelines that year. See United States Sentencing Commission, Sourcebook of Federal Sentencing Statistics (2006) Table 51 http://www.ussc.gov/ANNRPT/2006/SBTOC06.htm at 10 October 2007.

Sourcebook) indicates that this risk has risen during the past few years. According to Table 51 in that document, during the 2008 fiscal year ¹⁹⁶ there were sixteen corporate defendants sentenced under the *Organizational Sentencing Guidelines* where money laundering was their sole, or primary, criminal offence. ¹⁹⁷ Of these defendants, which collectively accounted for 8.1% of all corporations sentenced under the *U.S. Sentencing Guidelines* that year (an increase of 3.5% since 2006), eight were ordered to pay a monetary fine and six were required to make restitution. The remaining two were neither ordered to pay a fine, nor ordered to make any restitution for their criminal conduct.

Whilst the figures in the *U.S.S.C. 2008 Sourcebook* certainly demonstrate that between the 2006 and 2008 fiscal years, the probability of an organisation being ordered to pay a fine or make restitution for a money laundering offence increased, the actual risk now faced by institutions should not be overstated. Indeed, for those eight organisations ordered to pay a fine during the 2008 fiscal year, the average fine imposed upon them was a mere USD\$35,663. Further, for those six organisations ordered to make restitution, the average cost of their efforts was only USD\$89,325. Thus, whilst an institution convicted of a money laundering offence and/or an AML/CTF compliance failure may technically be exposed to significant criminal fines, the likelihood of it actually incurring such a fine appears to be minimal judging by the most recent sentencing statistics.

Fines for individuals

Whilst defendant institutions in the U.S. are to be sentenced in accordance with the Organizational Sentencing Guidelines, their officers and employees may be sentenced under the remaining Chapters of the U.S. Sentencing Guidelines. As previously noted, the decision in United States v. Booker, 543 U.S. 220 (2005) requires District Courts to consider the U.S. Sentencing Guidelines when sentencing an individual with respect to a money laundering offence under $\S 2S$. In addition to these Guidelines however, they must have regard to a number of other factors outlined in 18 U.S.C. $\S 3553(a)$. These factors include the:

¹⁹⁶ The 2008 fiscal year ran from 1 October 2007 to 30 September 2008 inclusive.

See United States Sentencing Commission, Sourcebook of Federal Sentencing Statistics (2008) Table 51 http://www.ussc.gov/ANNRPT/2006/SBTOC08.htm at 3 October 2009.

- nature and circumstance of the offence, and the history and characteristics of the individual defendant; and
- need for the individual's sentence to:
 - (i) reflect the seriousness of the offence and provide just punishment for its commission:
 - (ii) deter criminal conduct;
 - (iii) protect the public from further crimes committed by the defendant; and
 - (iv) provide the defendant with any necessary correctional treatment.

According to the *U.S.S.C. 2008 Sourcebook*, during the 2008 fiscal year there were 893 individuals sentenced under the *U.S. Sentencing Guidelines* where money laundering was their primary criminal offence. Whilst there are no figures available with respect to how many of these individuals committed their offence(s) whilst employed by an institution covered by U.S. AML/CTF laws, the nature and type of money laundering offences covered in § 2S of the Guidelines (particularly those contained in § 2S1.3.), suggest that a considerable number might have.

As outlined in Table 15 of the *U.S.S.C. 2008 Sourcebook*, of the 893 individuals sentenced for a money laundering offence during the 2008 fiscal year, 573 (64.2 per cent) were not ordered to pay a fine or make any restitution. Of those remaining, only 152 (17.0 per cent) were ordered to pay a criminal fine, and only 19 (2.1 per cent) were ordered to both pay a fine and make restitution. 199

For those individuals who were ordered during the 2008 fiscal year to pay a fine or make restitution for a money laundering offence, they were required to pay an average of

This number is relatively consistent with the 901 individuals sentenced for a money laundering offence under the U.S. Sentencing Guidelines during the 2006 fiscal year.

Again, these figures are relatively consistent with the statistics for the 2006 fiscal year, during which 562 defendants (62.4 per cent) were not ordered to pay a fine or make any restitution, 182 defendants (20.2 per cent) were ordered to pay a criminal fine, and 12 defendants (1.3 per cent) were ordered to both pay a fine and make restitution. See United States Sentencing Commission, Sourcebook of Federal Sentencing Statistics (2006) Table 15 http://www.ussc.gov/ANNRPT/2006/SBTOC06.htm at 10 October 2007.

USD\$3,286,380.²⁰⁰ This amount is more than 5.8 times greater than the average payment ordered for other types of offences that year.²⁰¹ Further, it is more than USD\$1,730,000 greater than the average payment ordered in the next highest payment category (i.e. the average payment for fraud offences).²⁰² These figures demonstrate that whilst individuals sentenced for a money laundering offence under the *U.S. Sentencing Guidelines* may face a comparable risk to institutions of incurring a criminal fine or being ordered to make restitution, they face a significantly higher risk of paying dearly for their misdeeds.

3.3.2 The imposition of imprisonment

Given the global importance that AML/CTF issues have assumed in recent years, a number of related offences now carry a period of imprisonment instead of, or in addition to, other penalties. In risk-based AML/CTF regimes, criminal liability is generally far more likely to attach itself to breaches of the minimum, prescriptive requirements contained in AML/CTF legislation. For instance, it often applies to statutory tipping off provisions, and any failure to properly report suspicious or significant cash transactions (otherwise referred to in Australia as 'Suspicious Matters' and 'Threshold Transactions' respectively). In certain regimes, criminal liability and terms of imprisonment might also extend to circumstances where an individual deliberately seeks to avoid or circumvent their AML/CTF obligations. In the U.S. for instance, any individual who structures a transaction to avoid federal reporting requirements under the *Bank Secrecy Act* may be imprisoned for up to five years and fined up to USD\$250,000.²⁰³

²⁰⁰ In total, individuals were collectively sentenced to pay a total of USD\$1,012,205,051 during the 2008 fiscal year. This is markedly more than the USD\$454,523,087 that individuals sentenced for similar offences were ordered to pay during the 2006 fiscal year. See United States Sentencing Commission, *Sourcebook of Federal Sentencing Statistics* (2006) Table 15 http://www.ussc.gov/ANNRPT/2006/SBTOC06.htm at 10 October 2007.

The average payment ordered in cases sentenced under the Guidelines during the 2008 fiscal year was USD\$557,367. See United States Sentencing Commission, Sourcebook of Federal Sentencing Statistics (2008) Table 15 http://www.ussc.gov/ANNRPT/2006/SBTOC08.htm at 3 October 2009.

⁽²⁰⁰⁸⁾ Table 15 < http://www.ussc.gov/ANNRPT/2006/SBTOC08.htm at 3 October 2009.

After money laundering cases, fraud cases and arson cases had the next highest average payments (i.e. USD\$1,555,627 and USD\$570,516 respectively).

Other more egregious criminal offences under the Act may carry a term of imprisonment up to ten years and/or a fine up to USD\$500,000, depending upon the particular AML/CTF provisions that have been violated.

The length of imprisonment imposed upon an individual for a money laundering offence will vary between different jurisdictions and AML/CTF statutes. Research conducted by Michael Levi and Peter Reuter suggests that during the 2000 fiscal year, the average term of imprisonment imposed upon the 590 individuals sentenced in the U.S. for a money laundering offence was 36 months. ²⁰⁴ However, individuals that played leadership roles in money laundering activities typically received lengthier sentences. The average sentence for cash or monetary instrument smuggling was 19.6 months, compared with 13.4 months for structuring transactions and 8.5 months for failing to properly file a transaction report. ²⁰⁵ Whilst these sentences may appear to be relatively minimal, it should be noted that they relate only to standalone money laundering offences, and not money laundering offences coupled with some kind of underlying predicate offence. Further, they were imposed prior to the enactment of the *USA PATRIOT Act* and the bolstering of the country's AML/CTF legislative framework.

Despite the potential sentences attached to money laundering offences and/or breaches of AML/CTF legislation, the risk of an individual actually being imprisoned appears to be higher in some jurisdictions than others. For instance, individuals in the U.S. arguably face greater AML/CTF legal risk than many of their foreign counterparts due to the belief of the country's regulatory and law enforcement authorities that the pursuit of "guilty individuals should always take precedence over the prosecution of entities". They may also face a greater risk of imprisonment, given that U.S. federal prosecutors can now consider the adequacy of prosecuting culpable employees when determining whether to pursue a corporation for malfeasance.

In a memorandum released by Larry D. Thompson in January 2003 (**the Thompson Memo**), the U.S. Department of Justice detailed a set of guidelines (entitled the *Principles of Federal Prosecution of Business Organizations*) for federal prosecutors to follow when determining

Levi, M., and Reuter, P., Money Laundering (2006) The University of Chicago 338 http://www.publicpolicy.umd.edu/faculty/reuter/Working%20Papers/Levi_and_Reuter.pdf at 16 October 2008

²⁰⁵ Ibid.

²⁰⁶ See Thompson, L.D., (Untitled speech delivered at the Corporate Fraud Task Force Conference, Washington D.C., 26 September 2002).

whether to indict a U.S. company for criminal misconduct. The guidelines stressed the importance of prosecuting individuals for business crimes, and stipulated that because the imposition of individual criminal liability "may provide the strongest deterrent against future corporate wrongdoing", it should be pursued "even in the face of offers of corporate guilty pleas". They essentially enabled U.S. federal prosecutors to consider the satisfactoriness of prosecuting culpable employees, when determining whether to lay criminal charges against a corporation for malfeasance. Where the prosecution of such individuals satisfies the need to provide retribution, deterrence, rehabilitation and restitution, the prosecution of the relevant corporation may be deemed to be unnecessary. ²⁰⁸

The result of this has been that several institutions accused of committing money laundering offences have sought to limit their own criminal culpability and AML/CTF legal risk by providing U.S. prosecutors with evidence against their employees. One of the more striking examples of this is provided by global accounting firm KPMG, which faced regulatory scrutiny in 2005 after it was found to have laundered funds and created fraudulent tax shelters for the purposes of assisting its wealthy clients to evade USD\$2.5 billion in taxes. In what became the largest criminal tax case ever filed in the U.S., federal prosecutors indicted eight former KPMG executives with conspiracy (an offence punishable by imprisonment), and filed a criminal Information against KPMG charging it with conspiracy and other crimes.²⁰⁹

Unlike its eight former executives, KPMG ultimately managed to avoid being prosecuted for its offences. In part, this is due to the fact that the company's indictment may have put it out of business and left only three international audit firms remaining (a highly undesirable result given the previous collapse of Arthur Andersen). However, it is also attributable to the various representations KPMG made to U.S. prosecutors in order to avoid formal indictment. The company not only agreed to pay USD\$456 million in penalties, but also to submit to an

Memorandum from Larry D. Thompson, Deputy Attorney General, to Heads of Department Components and United States Attorneys, 20 January 2003 http://www.usdoj.gov/dag/cftf/corporate_guidelines.htm at 1 August 2008.

Wray, C.A., and Hur, R.K., 'Corporate Criminal Prosecution in a Post-Enron World: The Thompson

Memo in Theory and Practice' (2006) 43(3) American Criminal Law Review 1095, 1106.

(KPMG Pays \$456 million US Fine, 8 Former Execs Charged with Conspiracy', CBC News, 29 August 2005 http://www.cbc.ca/money/story/2005/08/29/KPMG fined20050829.html > at 15 May 2008.

independent monitor and assist authorities with their investigations into the activities of the eight indicted employees. Further, in an undertaking that attracted the ire of many legal practitioners and industry participants, KPMG essentially agreed to "[throw] its former partners overboard while giving the government evidence to use against them".²¹⁰

However, it is debatable whether KPMG had much choice with respect to avoiding its own prosecution by legally abandoning its employees. According to the Honorable Lewis A. Kaplan, a U.S. District Court Judge for the Southern District of New York, the past decade has seen the U.S. move from a system in which "prosecutors prosecuted and courts and juries decided guilt or innocence" to one where prosecutors "threaten business entities with unbearable extrajudicial consequences and thus exact acquiescence in the government's demands". Such acquiescence may involve the payment of large fines, firing of culpable employees, and implementation of additional internal controls.

If Judge Kaplan's commentary is to be accepted, it may be that under the current enforcement environment in the U.S., an institution that finds one of its employees accused of criminal wrongdoing must choose between "betting the company's future that the employee will be exonerated" or doing whatever the U.S. Department of Justice demands to avoid indictment.²¹² This certainly appears to have been the case in relation to KPMG; with claims that U.S. government officials held a "proverbial gun" to the company's head by making the availability of a deferred prosecution agreement contingent on its agreement not to pay its former employees' legal fees in any related criminal proceedings.²¹⁴ Evidently, the KPMG case demonstrates that even where an institution condones or encourages the commission of a money laundering offence by one or more of its employees, those employees may find themselves abandoned by the institution in the face of subsequent criminal proceedings.

The use of deferred prosecution agreements is further discussed in **Chapter 5** of this thesis.

Gleckman, H., Borrus, A., and McNamee, M., 'Inside the KPMG Mess', *BusinessWeek*, 12 September 2005, 46.

Kaplan, L.A., Some Reflections on Corporate Criminal Responsibility (2007) The Antitrust Source 1 http://www.abanet.org/antitrust/at-source/07/10/Oct07-Kaplan10-18f.pdf at 31 December 2008.

Khoury, P.F., DOJ's "Thompson Memo" Is Unconstitutional (2006) Wiley Rein LLP http://www.wileyrein.com/publication.cfm?publication_id=12690 at 3 August 2008.

In addition to the strategies employed by federal prosecutors, an individual's risk of incurring a term of imprisonment may be influenced by their organisational position. In jurisdictions such as the U.S., the U.K. and Australia, municipal AML/CTF laws require institutions to appoint a nominated officer to oversee AML/CTF compliance and file, as appropriate, Suspicious Activity Reports (SARs).²¹⁵ This individual will generally – with the exception of deliberately non-compliant employees – face the greatest AML/CTF legal risk in relation to their institution's breaches of AML/CTF legislation.

In the U.K., responsible officers are referred to as Money Laundering Reporting Officers (MLROs). Whilst all employees can be held criminally liable for the deliberate commission of certain money laundering offences, MLROs may be held liable and imprisoned for their institution's failure to report suspicious activities and/or implement appropriate AML/CTF controls. For instance, under Section 330 of the Proceeds of Crime Act 2002 (U.K.) (POCA), a MLRO convicted of failing to file a SAR may be imprisoned for up to five years. The practical effect of this and similar provisions is that MLROs may personally assume some of the AML/CTF legal risk that would otherwise fall squarely on the shoulders of their institutions.

As with the legislative position in the U.K., a failure to properly report suspicious activities may carry a term of imprisonment in Australia. However, the full extent of the AML/CTF legal risk attached to this offence will not be known until such time as the AML/CTF Act 2006 (Cth) is fully implemented. Once the staggered implementation of the Act is complete, the risk attached to reporting failures may appear to be slightly different to that in the U.K. Whilst the U.K. test for reporting is whether an individual had "reasonable grounds to suspect" that another was involved in money laundering, the Australian test is whether a person "suspected on reasonable grounds" that another was involved in such activities. Given that this distinction will likely result in Australia relying on a somewhat subjective test

The name given to such reports may vary between different jurisdictions. For instance, Australian AML/CTF legislation has recently renamed such reports (which were previously referred to as Suspicious Transaction Reports) Suspicious Matter Reports,

Fagg, S., Laundering Causing Recruiting Woes (2006) Human Resources Magazine http://www.humanresourcesmagazine.com.au/articles/a0/0c043fa0.asp at 20 September 2006.

of knowledge, as opposed to the purely objective test adopted in the U.K.,²¹⁷ the AML/CTF legal risk attached to a reporting failure may prove to be lower in Australia than it is in the U.K. However, further exploration of this issue should take place once the transaction reporting requirements under the Act come into force, and AUSTRAC begins to actively monitor and enforce compliance with them.

Evidently, the extent of an individual's AML/CTF legal risk (and, more specifically, their risk of imprisonment) may be somewhat dependent upon their organisational position and the role they are expected to play regarding their institution's AML/CTF compliance. However, it may also be linked to their profession or industry, as the past few years have seen certain jurisdictions take a more hard-lined stance with regards to particular individuals considered to represent a greater ML/TF risk and/or have an increased AML/CTF compliance burden. This is perhaps most evident with regards to members of the legal profession; a number of whom have been sentenced to terms of imprisonment in the U.K. for deliberately facilitating, being wilfully blind to, and/or failing to report their clients' money laundering activities.

In the U.K., the *POCA* and the country's *Money Laundering Regulations* have significantly extended the obligations imposed upon professional advisers to report suspicions of money laundering and other illegal activities.²¹⁸ They have also heightened the penalties for failing to report such suspicions, with professionals facing up to 14 years imprisonment for violating legislative reporting requirements. In *R v Duff* [2002] EWCA Crim 2117 for instance, U.K. solicitor Jonathan Duff (**Mr Duff**) was expelled from the U.K. Law Society and sentenced to six months imprisonment for failing to disclose knowledge or suspicions of money laundering.

After a wealthy, long-standing client of his was gaoled for drug trafficking and possession, Mr Duff became suspicious of two transactions that he had previously conducted on their behalf. However, in accordance with legal advice he received from the U.K. Law Society

²¹⁷ Oliver, P., Reputation and Risk on the Line (2006) Lawyers Weekly

http://www.lawyersweekly.com.au/articles/50/0C045650.asp?Type=55&Category=1325 at 3 November 2006

Quick, C., 'Money Laundering – Get it Wrong, Go to Jail' (2004) 133(1325) Accountancy 46.

and another law firm, Mr Duff did not report the transactions because he believed that the U.K.'s new AML/CTF laws did not apply retrospectively to past transactions. ²¹⁹ At trial, Mr Duff pleaded guilty to two counts of failing to disclose suspicions of money laundering, and became the first U.K. solicitor to be convicted of, and imprisoned for, failing to disclose suspicions of money laundering. When refusing leave to appeal against his sentence, the Court of Appeal held that this was "a case where a solicitor received £70,000 in cash... the money had been put in part into fictitious names [so that] for six months... he was courting a risk that his suspicions were reportable". Undoubtedly, this ruling "stripped away the last vestiges of complacency over money laundering in the [legal] profession". ²²⁰ Perhaps for the first time, it made U.K. legal professionals acutely aware of the fact that their AML/CTF legal risk was not confined to the deliberate laundering of criminal funds – it also extended to genuine misunderstandings regarding the timing and scope of their legislative AML/CTF obligations.

Nevertheless, more recent cases such as *R v. Dougan* (unreported, 2006)²²¹ and *R v Griffiths and Pattison* [2006] EWCA Crim 2155,²²² demonstrate that even after the U.K. AML/CTF legislative regime has been operational for several years, some solicitors are still turning a blind eye to (or are simply ignorant of) their ongoing reporting obligations.²²³ Further, they suggest that the AML/CTF legal risk faced by legal practitioners may continue to be greater than that faced by ordinary corporate officers for some time. In accordance with the statements of Kerr LCJ of the Northern Ireland Court of Appeal in *R v. McCartan* [2004]

²¹⁹ Op cit n217.

²²³ Op cit n217.

Myint, R., 'Solicitors Beware: Money Laundering after R v Duff' (2003) 2(10) Journal of International Trust and Corporate Planning 65.

²²¹ In R v. Dougan (unreported, 2006), Mr Dougan allowed £66,000 (AUD\$167,062) in illegal tax scam earnings to pass through his client account. Although he did not initially realise that the funds were the proceeds of crime, Mr Dougan continued to act for the client after he became suspicious. When sentencing Mr Dougan to three months imprisonment, the presiding judge accepted that Mr Dougan was "a naïve victim of a sophisticated criminal" but held that solicitors had to "take the greatest care" to stop others using their respectability to launder cash.

²²² In R v. Griffiths and Pattison [2006] EWCA Crim 2155, Mr Griffiths acted on behalf of clients who were selling a property for less than one-third of its market value in an attempt to prevent the property being considered an asset in any proceeds of crime confiscation hearing. The property was being sold by drug traffickers to an estate agent for the amount of the outstanding mortgage. Mr Griffiths argued that he had relied on the explanation of the estate agent, whom he had trusted for years, for the reason behind the transaction. However, in sentencing Mr Griffiths to 15 months' imprisonment, the presiding Judge stated that Mr Griffiths had "clearly closed his eyes to the obvious".

NICA 43, "a custodial sentence will almost invariably be required" where a lawyer violates their AML/CTF reporting requirements because it is important for the courts "to make clear the importance of [their] scrupulous adherence to the requirements of... legislation".

3.4 The long-arm of the law: Extraterritorial AML/CTF legislation

Traditionally, criminal law was confined to conservative territorial terms. Bound and restricted by the principles of domestic jurisdiction or 'sovereignty', ²²⁴ a nation state was only able to exercise jurisdiction in relation to a criminal matter in circumstances where that matter arose within its own geographical boundaries. However, as recognition of the potential internationalisation of criminal activities grew, so too did the jurisdictional rules governing what nation states could legislatively provide for. The rigid common law 'territorial paradigm' started to lose favour and a number of jurisdictions started to legislatively assert authority over criminal activities occurring outside their own borders.

Whilst a state's jurisdiction may still be fundamentally tied to a particular geographic territory, it is now well established that nation states have the authority to enact extraterritorial legislation under specific international agreements (e.g. the *Vienna Convention*) and certain principles of international law.²²⁵ Whilst international law might be thought to place a number of constraints on the extraterritorial reach of nation states, some academics believe that it has actually expanded the legislative power of countries over persons and acts committed abroad.²²⁶ In the U.S. for instance, any constitutional obstacles to the extraterritorial application of domestic legislation to the perpetrators of 'universal' crimes (for instance, financiers of terrorism), may be overcome as a result of the interaction between

Under the well established principles of sovereignty, a nation state has authority to "prescribe, adjudicate, and enforce its laws within its own borders". See Colangelo, A.J., 'Constitutional Limits on Extraterritorial Jurisdiction: Terrorism and the Intersection of National and International Law' (2007) 48(1) Harvard International Law Journal 121, 127.

For instance, under the "protective principle" in international law, countries may seek to enact legislation enabling them to assert jurisdiction over conduct which occurs outside their geographic borders, but which bears a reasonable relation to a legitimate interest of their country. See, by way of example, the U.S. Model Penal Code.

See Colangelo, A.J., 'Constitutional Limits on Extraterritorial Jurisdiction: Terrorism and the Intersection of National and International Law' (2007) 48(1) Harvard International Law Journal 121.

the international legal doctrine of universal jurisdiction and congressional lawmaking authority.

Accordingly, whilst AML/CTF legal risk might arise by virtue of municipal AML/CTF legislation, it might also arise as a product of the criminal offences and penalties provided for under foreign AML/CTF laws with extraterritorial or "long-arm" jurisdiction.²²⁷ These laws essentially enable national governments to impose binding, enforceable obligations on individuals and institutions operating beyond their own geographic boundaries. Given the transboundary nature of many money laundering and terrorism financing activities, the increasing globalisation of the financial services industry, and the number of international bodies currently working to address AML/CTF issues, recent years have seen a number of jurisdictions enact extraterritorial AML/CTF laws.

In the immediate aftermath of the September 11 attacks, the U.S. government imposed a suite of extraterritorial controls upon foreign financial institutions. These controls, which have significantly changed the way that foreign institutions conduct business in the U.S. and with U.S. institutions, are enshrined in several extraterritorial legislative instruments, including Executive Order 13224 – Blocking Property and Prohibiting Transactions with Persons who Commit, or Threaten to Commit, or Support Terrorism (Executive Order 13224) and the USA PATRIOT Act. Whilst the legality of such sweeping legislation has often been questioned, the U.S. government has continually justified the extraterritorial reach of its laws by reference to the 'effects doctrine'. Under this doctrine, U.S. courts are instructed to presume that Congress intended to regulate extraterritorially whenever foreign conduct is deemed to have a 'substantial effect' within the U.S. 228

Whilst a number of nation states have enacted extraterritorial AML/CTF laws, these laws are arguably far narrower than the broad provisions and expansive scope of U.S. extraterritorial

²²⁸ Mitchell, S.L., 'The Implications of the USA Patriot Act on Foreign Banking Institutions' (Speech delivered at the National Anti-Money Laundering Training Seminar, St. Vincent and the Grenadines, 24 May 2002) 1.

²²⁷ Extraterritorial laws enable countries to exercise jurisdiction beyond their own geographic borders. They operate such that persons existing beyond the limits of the enacting state or nation are still amenable to its legislative provisions.

legislation. For instance, the U.K. has previously enacted the *Terrorism Act 2000* (U.K.) to empower U.K. courts to oversee cases concerning the planning and orchestration of terrorist acts, regardless of where in the world such acts are carried out.²²⁹ In comparison to U.S. AML/CTF legislation however, the extraterritorial implications of this Act are somewhat limited by the *Anti-Terrorism, Crime, and Security Amendments to the Terrorism Act 2000* (U.K.), which stipulates that freeze orders do not have extraterritorial effect in relation to the foreign branches of U.K. companies or financial institutions. As such, it is unlikely that other third parties acting outside U.K. territory, either directly or indirectly in support of terrorism, will be covered by the *Terrorism Act 2000* (U.K.).

3.4.1 Widening the posts: The Money Laundering Control Act

One of the first pieces of extraterritorial AML/CTF legislation to be enacted in the U.S. was the *MLCA*. Codified as *18 U.S.C.* §§ 1956 and 1957, this Act criminalises domestic and international money laundering, and carries large fines and potential prison terms for their commission. Unlike earlier, relatively unsuccessful legislative attempts to curb the movement of illegal income, the *MLCA* was not solely created to impose currency reporting requirements upon financial institutions. Rather, it was enacted to more widely undermine the use of financial institutions to convert illegally derived funds into usable and inconspicuous funds.²³⁰ Under the Act, the term "financial institution" is defined broadly; encompassing not only U.S. institutions but also foreign banks and other foreign financial institutions.²³¹

In addition to its expansive definition of "financial institution", the extraterritorial scope of the *MLCA* is cemented by provisions criminalising the international transportation, transmission or transfer of illicit proceeds to or from the U.S. It is also strengthened by expansively drafted provisions which render it a criminal offence for any institution to engage in financial transactions using money or property known to have been derived from

Alexander, K., 'Extraterritorial US Banking Regulation and International Terrorism: The Patriot Act and the International Response' (2002) 3(4) *Journal of International Banking Regulation* 307, 312.

Tucker Mann, T., 'Money Laundering' (2007) 44(2) American Criminal Law Review 769.

Under the Act, the term "financial institution" includes any financial institution as defined in 31 U.S.C. § 5312(a)(2), and any foreign bank as defined in Section 1 of the International Banking Act of 1978 (12 U.S.C. § 3101(7)).

unlawful activity. This includes transactions designed to avoid a federal or state transaction reporting requirement, and those intended to conceal or disguise the nature, location, source, ownership or control of illegally obtained funds.

However, whilst the *MLCA* extends the compliance obligations of, and the AML/CTF legal risk faced by, various U.S. and non-U.S. institutions, there are certainly limitations on the extraterritorial reach of the Act. It has been established that for the purposes of adjudicating an action or enforcing a penalty under the *MLCA*, U.S. District Courts have jurisdiction over any foreign person (including any foreign financial institution) against whom such an action is brought. That being the case, 18 U.S.C. § 1956(f) stipulates that the courts can only exercise their extraterritorial jurisdiction under the *MLCA* where one of the following conditions is met:

- a foreign person has committed an offence under the Act in relation to a financial transaction that has occurred wholly or partly in the U.S.;
- a foreign person has converted, for their own use, property in which the U.S. has an ownership interest in by virtue of the entry of an order of forfeiture by a U.S. court; or
- an offence under the Act has been committed by a foreign financial institution that maintains a correspondent or interbank account with a U.S. financial institution.

Although 18 U.S.C. § 1956(a) explicitly states that "unlawful activity" under the MLCA encompasses tax fraud and tax evasion, 232 18 U.S.C. §§ 1956(f) and 1957(d)(2) prevent the U.S. government from exercising extraterritorial jurisdiction with respect to both these crimes. Regardless of this restriction however, extraterritorial jurisdiction may still be exercised in respect of wire and mail fraud by virtue of 18 U.S.C. § 1956(c)(4)(A) and (5), and 18 U.S.C. § 1957(f)(1). Consequently, where an institution covered by the Act mails or wires funds to a foreign jurisdiction for a customer seeking to avoid the proper payment of taxes, any failure by that institution to report the transaction could constitute concealment of

²³² See 18 U.S.C. § 1956(a)(1)(A)(ii), and I.R.C. §§ 7201 and 7206.

Whilst 18 U.S.C. § 1956(f) relates to conduct concerning a transaction or series of related transactions involving "funds or monetary instruments" of a value exceeding USD\$10,000, 18 U.S.C. § 1956(a)(2) deals with funds or monetary instruments but does not include tax fraud or tax evasion. As 18 U.S.C. § 1957 does not refer to tax fraud or tax evasion, extraterritorial jurisdiction is not granted to the U.S. government with respect to these crimes.

tax fraud or tax evasion. If this were to occur, the transaction would constitute a specified unlawful activity under 18 U.S.C. § 1956(a)(1)(A)(ii), and the U.S. government could exercise its extraterritorial jurisdiction. Whilst the involvement of tax fraud or tax evasion does not grant extraterritorial jurisdiction in and of itself, in such circumstances the mail and wire fraud act as the predicate offences that give rise to the extraterritorial jurisdiction. 234

Given its extraterritorial reach, the *MLCA* carries a certain level of AML/CTF legal risk for financial institutions operating outside the U.S. Particular offences under the Act carry criminal penalties including imprisonment up to 20 years, and fines up to USD\$500,000 or twice the value of the monetary instruments or funds laundered (whichever is greater). Where an institution commits one of these criminal offences, the quantum of their penalty will depend upon a range of factors, including the purpose of their intended punishment, the nature of their offence, and their compliance history.

3.4.2 A new regulatory era: The USA PATRIOT Act

Considered "the strongest expression of extraterritorial powers over the international dollar payments system", ²³⁶ Title III of the USA PATRIOT Act is formally known as the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 (P.L. 107-56, 115 Stat. 272). Enacted in the U.S. in the immediate aftermath of September 11, the Act applies to both U.S. and non-U.S. financial institutions, and is responsible for extending the country's extraterritorial AML/CTF enforcement powers.²³⁷

The legislation, which amends certain provisions of the *Bank Secrecy Act* and the *MLCA*, was drafted on the premise that weaknesses in financial transparency are critical to the financing of terrorism. It has considerable extraterritorial implications for financial institutions (and the AML/CTF legal risk they face) because it has vastly:

Duke, J.R., 'Penalties Relating to Foreign Trusts for Failure to Report' (Speech delivered at Ashford Suites, High Point, North Carolina, 27 January 2006) 5.

²³⁵ Op cit n230, 789.

²³⁶ Op cit n228, 2.

Preston, E., 'The US Patriot Act: New Adventures in American Extraterritoriality' (2002) 10(2) Journal of Financial Crime 104.

- widened the predicate offence of money laundering to encompass policies related to the interdiction of terrorism financing;
- expanded U.S. extraterritorial jurisdiction in relation to the activities of foreign third
 parties (including banks and professional advisers) deemed to be supporting terrorists or
 terrorist groups; and
- increased U.S. supervisory control over the global activities of foreign banks that maintain a correspondent or payable through account with a U.S. institution.²³⁸

Five sections of the *USA PATRIOT Act* have notable implications for non-U.S. financial institutions. Three of these sections (*Sections 311, 312* and *313*) indirectly regulate foreign entities by imposing restrictions on their activities with domestic financial institutions.²³⁹ The remaining two sections (*Sections 317* and *319*) directly regulate the activities of institutions beyond U.S. borders. As these latter sections explicitly relate to the potential initiation of civil proceedings and civil forfeiture actions against non-U.S. institutions, they are addressed in **Chapter 4** of this thesis.

Some of the most notorious U.S. extraterritorial provisions contained in the *USA PATRIOT Act* are enshrined in *Section 311*. That section carries significant AML/CTF legal risk for foreign institutions dealing with the U.S. financial system, because it empowers the U.S. Secretary of the Treasury to invoke one or more targeted "special measures" in relation to those nations, institutions, transactions and accounts deemed to be of "primary money laundering concern". ²⁴⁰ In order of ascending severity, these special measures include:

- (i) additional recordkeeping or reporting requirements for particular transactions;
- (ii) requirements around the identification of the foreign beneficial owners of certain accounts held at a U.S. financial institution;

²³⁸ Op cit n229, 307.

As outlined in 31 U.S.C. § 5312(a) and (c), domestic financial institutions are defined broadly under U.S. law to encompass a range of varied entities. Examples of those covered by the definition include banks, trust companies, credit unions, thrift institutions, securities brokers and dealers, currency exchanges, insurance companies, pawnbrokers and travel agencies.

Fleming, T., 'OFAC and 311 Exposure Issues' (Paper presented at the 2006 ABA/ABA Money Laundering Enforcement Conference, Washington DC, 9 October 2006) 9.

- (iii) requirements around the identification of foreign bank customers who use an interbank payable-through account opened by that foreign institution at a U.S. bank;
- (iv) requirements around the identification of foreign bank customers who use an interbank correspondent account opened by that foreign institution at a U.S. bank; and
- (v) restrictions or prohibitions on the opening/holding of certain interbank correspondent or payable-through accounts.

Once a foreign institution is deemed to represent a "primary money laundering risk" under Section 311, FinCEN will issue a notice of proposed rulemaking. Depending on the steps and corrective actions (if any) subsequently taken by the relevant institution to address the U.S. government's concerns, this proposed rulemaking may be withdrawn or finalised. To illustrate, following its initial designation as a "primary money laundering concern" on 26 April 2005, Latvian institution Multibanka revised its AML/CTF policies, procedures and internal controls so significantly²⁴¹ that FinCEN withdrew its proposed rulemaking on 13 July 2006 and no special measures were ever invoked. 242 By comparison, a proposed rulemaking issued with respect to the Commercial Bank of Syria in May 2004, was finalised on 9 March 2006 after the bank allegedly continued to provide political and material support to Lebanese Hezbollah and Palestinian terrorist groups. Using the justification that the bank had repeatedly "been used by terrorists to move funds and... acted as a conduit for the laundering of proceeds generated from the illicit sale of Iraqi oil", 243 the U.S. Department of the Treasury (U.S. Treasury Department) ordered all U.S. banks to terminate any correspondent account they maintained for the institution. The effect of this on the Commercial Bank of Syria was significant, as too were the ramifications for Banco Delta Asia (addressed in **Chapter 7** of this thesis) when the U.S. Treasury Department deemed it to be of "primary money laundering concern".

Financial Crimes Enforcement Network, FinCEN Withdraws Finding on Latvia's Multibanka and Issues Final Rule against Latvia's VEF Banka (2006) http://www.fincen.gov/latvia_311_withdraw.html at 5 December 2006.

United States Government, U.S. Federal Register - Proposed Rules, Vol. 71, No. 134, 13 July 2006, 39606.

Financial Crimes Enforcement Network, Treasury Issues Final Rule against Commercial Bank of Syria U.S. Financial Institutions Must Terminate Correspondent Accounts (2006) U.D. Department of the Treasury http://www.ustreas.gov/press/releases/js4105.htm at 5 December 2006.

In addition to the expansive powers provided by *Section 311*, *Section 312* of the *USA PATRIOT Act* enables the U.S. government to indirectly regulate the activities of foreign financial institutions. It stipulates that all U.S. banks that maintain correspondent accounts for certain types of foreign banks, must identify the beneficial ownership of those banks. Further, they must determine whether such banks provide correspondent accounts to other foreign banks, and conduct enhanced due diligence on their correspondent accounts to assess their ML/TF risk.²⁴⁴

Section 313 of the Act also has extraterritorial implications for foreign institutions as it strictly prohibits U.S. institutions from directly establishing, maintaining, administering or managing correspondent accounts for foreign shell banks, or any foreign bank that conducts business with a foreign shell bank.²⁴⁵ It is not sufficient for U.S. institutions to simply ensure that they are not directly maintaining a correspondent account on behalf of a shell bank; they must also take "reasonable steps" to safeguard the indirect abuse of their correspondent accounts by foreign institutions conducting banking activities for a shell bank.

For foreign financial institutions, the AML/CTF legal risk represented by the extraterritoriality of the *USA PATRIOT Act* is particularly pronounced because the powers granted to U.S. authorities under the Act are so significant. Under its provisions, any foreign institution seeking to access the U.S. banking system must implement AML/CTF controls that conform to the high standards of due diligence and transparency²⁴⁶ required of U.S. institutions. If its controls do not meet the standards required by the U.S. government under the *USA PATRIOT Act*, a foreign institution may have its U.S. correspondent account(s) terminated and find itself barred from conducting business with U.S. institutions and accessing the U.S. banking system thereafter.

²⁴⁴ See 31 U.S.C. § 55318(i)(2)(B) (2002) and 31 U.S.C. § 5318(i)(3) (2002).

For the purposes of the Act, a "correspondent account" is defined as an account established to receive deposits from, make payments on behalf of, or handle other financial transactions related to, a foreign financial institution. A "shell bank" is a bank that does not have a physical presence (for instance, a place of business that is located at a fixed address) in any country.

246 Op cit n229, 312.

Whilst the U.S. government might contend that the far-reaching extraterritorial provisions contained in the *USA PATRIOT Act* are necessary to protect the U.S. financial system, it may be argued that there is a certain degree of 'legislative arrogance' inherent in their enactment. Embedded in the drafting of many of the Act's provisions appears to be an assumption on the part of U.S. legislators that, regardless of the additional costs that U.S. laws may impose upon foreign financial institutions, such institutions will endeavour to meet them. Presumably, this assumption is largely hinged upon the status of New York City as one of the world's most important international financial centres, and the dominance of the U.S. in the international banking system. Nevertheless, despite what it may be attributable to, the view that foreign institutions will typically fall into line with U.S. compliance standards, has largely proven to be correct.

Although some commentators have argued that the expansive extraterritoriality of the Act could cause a backlash and "threaten America's primacy in the international financial system", 247 this does not appear to have been the case. In order to ensure their continued survival and ongoing access to the U.S. banking system, vast numbers of foreign financial institutions have voluntarily assumed compliance with the Act and adopted additional AML/CTF controls in order to avoid being cut off from U.S. business. In the current commercial environment, where the U.S. is one of the largest and most influential players in international commerce, exclusion from the U.S. financial system is seemingly far too high a price to pay for falling foul of the USA PATRIOT Act.

That said, it must be noted that in some countries there has certainly been a shift or, at the very least, speculation of a shift towards an increasing use of the Euro as an alternative to U.S. dollars. The international role of the Euro has changed markedly in recent years.²⁴⁸ In the Asia-Pacific region, countries including Indonesia and Malaysia have already shifted some of their central banks' reserves from U.S. dollars to Euros. Further, China and a number of other Asian nations have increased the share of the Euro in their foreign exchange

²⁴⁷ Op cit n237.

²⁴⁸ Kuroda, H., 'The Importance of the Euro in a Rapidly Changing Environment: An Asian Perspective' (Speech delivered at the Brussels Economic Forum 2008: Economic and Monetary Union in Europe: 10 Years On, Brussels, 15 May 2008).

reserves.²⁴⁹ As a result, it may be contended that the dominance and influence of U.S. currency has waned slightly, and the scope and relevance of U.S. extraterritorial AML/CTF legislation has been reduced. As foreign nations and institutions rely more heavily upon the Euro as a means of conducting business, their exposure under – and their need to strictly comply with – U.S. AML/CTF legislation may be somewhat limited.

3.4.3 Beyond AML/CTF compliance: Economic and trade sanctions

The term "economic and trade sanctions" refers to the deliberate government withdrawal, or threat of withdrawal, of trade or financial relations. The use of sanctions has a lengthy history; traceable back to 432 B.C. when Athens officials denied certain traders from accessing the city's harbour and marketplace. However, whilst economic and trade sanctions may not be entirely new legal tools, it was not until the 1990s that their use became more commonplace on the global stage. At that time, the United Nations started to play a greater role in international affairs and the United Nations Security Council became more willing to endorse mandatory sanctions against nation states involved in civil strife, regional aggression, and/or gross violations of human rights. ²⁵¹

Economic and trade sanctions have generally been invoked to achieve the same purposes as criminal penalties; namely, deterrence, punishment and rehabilitation. More specifically however, they have been used to foster or exacerbate political or economic instability in a certain country by limiting its exports/restricting its imports, or interrupting its commercial finance (i.e. by reducing its aid and/or cutting any loans made to its government).²⁵²

Suparno, R., 'The Euro: A Viable Alternative to the U.S. Dollar', *The Jakarta Post* (Jakarta), 18 July 2005 http://www.thejakartapost.com/news/2005/07/18/euro-viable-alternative-us-dollar.html at 24 January 2009

Paulson, M., 'History of U.S. Sanctions Shows Most Haven't Worked', Seattle Post-Intelligencer, 11 May 1999 http://seattlepi.nwsource.com/irag/sanction.shtml at 30 December 2008.

Hufbauer, G.C., Schott, J.J., Elliott, K.A., and Oegg, B., Economic Sanctions Reconsidered (3rd ed, 2007) 132.

Elliott, K.A., Hufbauer, G.C., and Oegg, B., The Concise Encyclopaedia of Economics (2nd ed, undated) http://www.econlib.org/library/Enc/Sanctions.html at 30 December 2008.

In recent times, countries such as the U.S. have aggressively used economic and trade sanctions to pursue their own foreign policy and national security interests.²⁵³ Following September 11, targeted financial sanctions have been used to isolate supporters of terrorism and prevent the facilitation of suspect money flows.²⁵⁴ However, whilst a number of sanctions have been invoked in relation to terrorism, terrorism financing and money laundering activities, many sanctions programs have involved political objectives far beyond those associated with AML/CTF. Unlike AML/CTF countermeasures, economic and trade sanctions can be used to address a far broader spectrum of issues considered to threaten international order and stability.²⁵⁵ This is evidenced by the fact that sanctions have previously been used to force the apartheid government of South Africa to allow democratic elections, block the Russian transfer of sophisticated cryogenic rocket engines to India, and prevent China from continuing to export sensitive military equipment.²⁵⁶

Whilst there are many economic and trade sanctions programs currently being administered around the world, the discussion herein is limited to OFAC sanctions as they are often considered to be some of the most important and influential sanctions programs post-September 11. Using its authority under Presidential wartime and national emergency powers, ²⁵⁷ as well as under specific legislation, OFAC currently administers a number of sanctions to regulate transactions and freeze foreign assets under U.S. jurisdiction. It maintains country-based sanctions programs (which may be limited, comprehensive or regime-based in nature), as well as list-based programs targeted towards foreign narcotics traffickers, foreign terrorists, weapons proliferators, and persons undermining the sovereignty of specific nation states.

²⁵³ Op cit n229, 308.

²⁵⁴ Zarate, J.C., Financial Power and International Security: Reflections on the Evolution of the Global Anti-Money Laundering and Counter-Terrorist Financing Regime since 9/11, *UBS Money Laundering Prevention* Newsletter, Spring 2009, 15, 16.

For instance, economic and trade sanctions may be invoked in circumstances where a particular country is believed to be proliferating weapons of mass destruction, violating fundamental human rights, or trafficking in narcotics.

²⁵⁶ Op cit n250.

These powers are largely enshrined in the *Trading with the Enemy Act of 1917* (P.L. 65-91, 40 Stat. 411) and the *International Emergency Economic Powers Act* (P.L. 95-223, 91 Stat. 1626).

Depending on whether a sanctions program is country-based, regime-based or list-based, the obligations placed upon institutions may include:

- blocking the accounts, assets and other property²⁵⁸ of specified individuals and entities;
- · blocking transactions that are-
 - (i) conducted by or on behalf of a blocked individual or entity;
 - (ii) directed to, or planned to go through, a blocked entity; or
 - (iii) otherwise connected with a transaction in which a blocked individual or entity has an interest; and
- rejecting unlicensed trade and financial transactions with specified individuals and entities.²⁵⁹

A review of OFAC's sanctions programs reveals how greatly the obligations under each may vary. For instance, the list-based sanctions programs prohibit institutions from dealing with, and oblige them to freeze the property of, any person/entity appearing on a specified list. By comparison, country-based sanctions programs typically impose trade prohibitions on institutions, and require them to block any assets of a specified government. Some sanctions regulations go even further than these requirements, with the Cuban sanctions program prohibiting institutions from exporting goods to or importing goods from Cuba, travelling to Cuba without a specific licence, and dealing with any property in which Cuba or a Cuban national has an interest.²⁶⁰

In addition to the aforementioned sanctions programs, OFAC also maintains a list of Specially Designated Nationals and Blocked Persons (**SDNs list**). Created under *Executive Order 13224*, this list contains more than 3,500 "foreign adversaries" (including individuals, entities and vessels) based in more than 110 countries. Under OFAC regulations, "all U.S. persons" are strictly prohibited from engaging in any form of financial transaction with anyone listed on the SDNs list.

The definition of "assets and property" is particularly broad and includes anything of direct, indirect, present, future or contingent value (including all types of bank transactions).

present, future or contingent value (including all types of bank transactions).

Federal Financial Institutions Examination Council, Bank Secrecy Act/Anti-Money Laundering Examination Manual (2006) 136.

Office of Foreign Assets Control, Cuba: What You Need to Know about the U.S. Embargo (2004) http://www.treas.gov/offices/enforcement/ofac/programs/cuba/cuba.pdf at 19 October 2007.

For the purposes of OFAC's SDNs list, the term "all U.S. persons" is defined to include all U.S. citizens and permanent residents wherever they are located, all people and organisations within the U.S., and all U.S. incorporated entities and their foreign branches throughout the world. The expansiveness of this definition means that OFAC's sanctions programs have a far broader scope – and potentially carry a higher level of AML/CTF legal risk – than many AML/CTF laws. Unlike the Bank Secrecy Act for instance, OFAC's regulations are not only binding upon U.S. banks and their domestic branches, agencies and international banking facilities, but also upon the foreign branches of U.S. institutions (including their foreign offices and subsidiaries) and a host of other industries not typically caught by U.S. municipal AML/CTF legislation (for instance, travel agencies and publishers). ²⁶¹

Whilst some OFAC regulations are explicitly extraterritorial in nature, the vast majority are only directly applicable to U.S. persons. However, this has not prevented a significant number of foreign institutions from nevertheless observing those regulations and bestowing upon them a legal status akin to de facto international law.²⁶² Presumably, many entities have sought to comply with all of OFAC's sanctions programs in order to avoid the potential:

- extraterritorial third party liability they may incur as a result of assisting, facilitating or conducting transactions for designated terrorist organisations;²⁶³ and
- reputational and financial damage they may sustain as a result of dealing with a restricted entity and being placed on the SDNs list themselves.²⁶⁴

Since the events of September 11, the legal risk represented by non-compliance with OFAC regulations has become more pronounced as the U.S. Treasury Department has paid

A select number of OFAC sanctions regulations (including those relating to Cuba and North Korea) extend beyond the definition of "all U.S. persons", to encompass all foreign subsidiaries owned or controlled by U.S. companies.

²⁶² Given that so many foreign institutions abide by OFAC sanctions programs in order to protect their own reputations and their ability to conduct business in (and with) the U.S., OFAC sanctions have assumed a status comparable to international law. Their coverage is arguably akin to international law now, despite the fact that they are created, enforced and monitored by a single jurisdiction.

²⁶³ Op cit n229, 312.

Under various pieces of legislation, the U.S. government maintains broad powers with respect to those individuals and entities seen to be supporting terrorist activities. For instance, under Section 1(d) of Executive Order 13224, the U.S. government is empowered to block the property of foreign persons who "assist in, sponsor, or provide financial, material, or technological support for, or financial or other services to or in support of" acts of terrorism and/or those individuals/entities otherwise designated by the U.S. Secretary of the Treasury.

increased attention to institutions' compliance with economic and trade sanctions.²⁶⁵ Currently, a single violation of an OFAC sanctions program may result in one of more of the following penalties:

- criminal fines up to USD\$10 million dollars for corporations and USD\$5 million dollars for individuals;
- terms of imprisonment ranging from 10 to 30 years for wilful violations;
- civil penalties ranging from USD\$11,000 to USD\$1 million; and
- forfeiture of the funds/property involved in the violation.

Since February 2003, hundreds of institutions have been penalised for breaching U.S. federal sanctions regulations.²⁶⁶ However, perhaps the most notable penalty imposed upon an institution for OFAC sanctions violations is that incurred by Swiss banking giant UBS in May 2004. The bank received a USD\$100 million monetary penalty for engaging in USD banknote transactions with sanctioned countries, and deliberately attempting to conceal those transactions from the U.S. Federal Reserve. Given that this penalty was approximately twenty times the amount of net profit that UBS made as a result of breaching OFAC sanctions,²⁶⁷ it was seemingly intended to damage the institution's financial standing and send a clear message to other institutions that non-compliance with OFAC sanctions can carry heavy penalties. Interestingly however, it is probable that the penalty levied against the institution would have been even higher had it not cooperated with investigators and reduced its future risk by instituting corrective actions internally, disciplining responsible staff, and agreeing to withdraw from the international banknote trading business.²⁶⁸

Whilst institutions are not required to design and implement a sanctions compliance program, the *Economic Sanctions Enforcement Guidelines* published in the U.S. Federal

Office of Foreign Assets Control, OFAC Compliance Mandatory; Penalties for Non-Compliance Staggering http://216.70.94.10/legupdates/officeofforeignassetscontrol.pdf at 18 November 2006.
Op cit n180, 400.

²⁶⁷ Baxter. T.C., 'Risk Management and Regulatory Failures at Riggs Bank and UBS: Lessons Learned' (Testimony before the Subcommittee on Oversight and Investigations, Committee on Financial Services, U.S. House of Representatives, 2 June 2004).

²⁶⁸ UBS, UBS Statement on Regulatory Actions by the U.S. Federal Reserve and the Swiss Federal Banking Commission (2004)

http://www.ubs.com/1/e/media_overview/media_global/search1/search10?news1d=59058> at 24 January 2009.

Register on 8 September 2008, enable OFAC to consider a range of general factors when determining the appropriate enforcement response to an apparent violation of sanctions regulations.²⁶⁹ These factors include the history of an institution's sanctions compliance, the strength and scope of its sanctions compliance program, any voluntary disclosure of its violations, and any actions subsequently taken to secure its future compliance with OFAC sanctions programs.²⁷⁰

Whilst there is a degree of overlap between the customer screening requirements contained in U.S. AML/CTF legislation²⁷¹ and the sanctions list-checking requirements overseen by OFAC, OFAC sanctions generally extend beyond known money launderers and terrorism financiers to include known terrorists, narcotics traffickers, weapons proliferators and other designated foreign persons. Accordingly, OFAC sanctions may be considered to carry greater legal risk for financial institutions than the *Bank Secrecy Act*'s customer identification requirements because there is a broader, ongoing risk of contravention.²⁷²

3.5 Enforcement and AML/CTF legal risk

An institution's AML/CTF legal risk is not simply hinged upon the number and scope of applicable AML/CTF laws, offences and penalties in a particular jurisdiction. It is also a product of the way in which such laws, offences and penalties are interpreted, pursued and applied. Whilst the overriding enforcement environment will affect institutions' AML/CTF legal risk in relation to their potential liability at both civil and criminal law, for ease of reference the issue of enforcement is addressed in this Chapter.

Unless AML/CTF legislation is strongly enforced by regulatory authorities and the courts, it is unlikely to have any impact on the way institutions identify, mitigate and manage their

See United States Government, U.S. Federal Register, Vol. 73, No. 174, 8 September 2008, 51933-51941.
 Ibid

Under current U.S. AML/CTF laws, U.S. financial institutions are required to compare new accounts against government lists of known or suspected terrorists/terrorist organisations within a reasonable time after opening the account.

^{2&}lt;sup>†2</sup> Institutions are not only required to screen their new customers against the OFAC lists when opening an account, but also screen their existing customer base regularly to ensure that they are not unintentionally holding an account for an individual/entity that has been subsequently added to the lists. In addition, institutions are required to filter their payments for transactions to or from sanctioned individuals or entities.

ML/TF risk. Where institutions believe that non-compliance with such legislation is unlikely to carry a high degree of AML/CTF legal risk, there will be little incentive for them to spend copious amounts of money trying to fulfil their legislative obligations.

Whilst the two primary deterrents for individuals engaged in money laundering are considered to be the risk of getting caught for their crimes and the severity of their likely punishment, ²⁷³ the same can arguably be said with respect to institutions covered by domestic and/or extraterritorial AML/CTF legislation. Indeed, an institution's AML/CTF legal risk is likely to be directly proportionate to the aggressiveness with which AML/CTF compliance is enforced, and legislative breaches are punished. Even in a jurisdiction where AML/CTF laws provide for a number of offences and harsh criminal penalties, the AML/CTF legal risk faced by institutions will still be minimal unless accompanying enforcement efforts are coordinated and concerted.

In some jurisdictions, institutions may try to assess their potential AML/CTF legal risk by reference to the number of successful criminal prosecutions for breaches of domestic AML/CTF laws. This is perhaps underpinned by the fact that many regulatory bodies have traditionally used public enforcement actions and harsh criminal penalties to demonstrate that non-compliance with AML/CTF laws may be sternly punished. However, by assessing their AML/CTF legal risk solely on the basis of how many successful prosecutions have taken place in a certain jurisdiction, institutions may understate (and therefore underestimate) the level of risk they face. Whilst criminal penalties are often the most newsworthy hallmarks of a strong enforcement environment, they are not the only hallmarks. As is further discussed in **Chapter 4** of this thesis, civil enforcement actions are frequently used to address AML/CTF compliance failures and contraventions of AML/CTF legislation. In fact, many domestic regulatory bodies have demonstrated a preference for pursuing non-compliance through the use of civil actions, which enable them to appease politicians and the public by dispensing with the more arduous criminal standard of proof and notching up some 'quick wins' on the regulatory scoreboard.

Yeandle, M., Mainelli, M., Berendt, A., and Healy, B., Anti-Money Laundering Requirements: Costs Benefits and Perceptions (2005).

Thus, whilst the number of successful criminal prosecutions may be an indicator of the effectiveness of a country's AML/CTF laws, the strength and/or reliability of that indicia may be questionable if viewed in isolation. There might be a range of reasons why a country has had very few prosecutions in relation to a specific crime. For instance, at the most basic level, it may simply be that there are low levels of that crime. Quantifying AML/CTF legal risk *solely* on the basis of prosecutions may lead to inaccurate assessments of risk given that a sizeable proportion of money laundering and terrorism financing offences are never identified. As discussed in **Chapter 2** of this thesis, there are no accurate statistics with respect to the prevalence of such activities so, at best, the published statistics are simply informed estimates. Accordingly, it is difficult to analyse the appropriateness of the number of criminal prosecutions in any jurisdiction without having sound crime statistics to compare them to.

Another significant problem with basing assessments of AML/CTF legal risk wholly upon the number of prosecutions is that in many jurisdictions a significant number of enforcement proceedings never advance to that stage. Many are settled out of court via cooperative (and sometimes confidential) agreements with regulatory authorities. Thus, the number of visible prosecutions in a particular nation state may not reflect the totality of regulatory and enforcement efforts in respect of AML/CTF.

From a legal risk perspective, what is perhaps more important than the number of criminal prosecutions in a certain country, is any criticism levied against authorities there for their refusal or unexplained reluctance to initiate criminal proceedings in circumstances where they are deemed to be warranted. This may involve criticism provided by other nation states or even international bodies concerned with the effective enforcement of AML/CTF legislation. For instance, in the FATF's 2005 Mutual Evaluation Report on Australia, the FATF expressed concern about the "dearth of money laundering prosecutions and convictions" at both the federal and state levels. ²⁷⁴

²⁷⁴ Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Combating the Financing of Terrorism - Australia* (2005) Organisation for Economic Cooperation and Development 28 http://www.oecd.org/dataoecd/60/33/35528955.pdf at 3 May 2008.

In reviewing the country's apparently low levels of money laundering prosecutions, FATF officials held that Australian authorities did not appear to be treating money laundering as a separate and serious offence. Rather, they seemingly considered money laundering offences to be ancillary to predicate offences; a viewpoint only strengthened by the fact that Australian judges have generally sentenced predicate crimes and money laundering offences concurrently. The effect of this Mutual Evaluation report was that the Australian government set about drafting and enacting the *AML/CTF Act 2006* (Cth) to bolster both its AML/CTF regime, and the FATF's opinion of the seriousness with which it regarded global AML/CTF efforts. Whilst the *AML/CTF Act 2006* (Cth) is currently still being implemented across regulated sectors, 2008 saw a number of money laundering prosecutions launched against individuals alleged to have breached the money laundering provisions of the *Criminal Code Act 1995* (Cth). This is seemingly demonstrative of a desire of law enforcement officials to more actively pursue money laundering prosecutions. Indeed, during 1997 and 2005 inclusive, there were only 5 successful prosecutions for money laundering in Australia.²⁷⁵

3.5.1 The stakes are raised: Increased enforcement

Historically, the levels of visible, criminal enforcement of AML/CTF laws have tended to be "extremely modest". ²⁷⁶ Whilst there were laws in some countries relating to AML and, to a lesser extent, CTF, the offences enshrined in those laws – and the legal courses of action they gave rise to – generally focussed upon the crime of money laundering as committed by drug traffickers. Where an individual was charged with committing any criminal offence from which they derived a profit, money laundering was simply an additional charge used by prosecutors to bolster their case against the defendant and increase any penalties they ultimately received.

However, during the past decade many jurisdictions have expanded their AML/CTF laws and focussed their regulatory efforts on the broader processes of money laundering and terrorism financing. Money laundering is now widely recognised as a criminal offence in its

²⁷⁵ Op cit n274, 31.

²⁷⁶ Levi, M., Money Laundering and Its Regulation (2002) 582 ANNALS American Academy of Political and Social Science 181.

own right, and AML/CTF laws often provide for a range of related offences that do not necessarily require the active laundering of dirty funds or the financing of terrorist acts. For instance, under Australia's AML/CTF Act 2006 (Cth), individuals and institutions may be held criminally liable for a range of criminal acts, including tipping off (Section 123), giving false or misleading information to regulatory/law enforcement authorities (Section 136), and providing a designated service (i.e. a financial service covered by the Act) using a false customer name (Section 139).

Whilst most high profile AML/CTF enforcement actions have occurred in the U.S., the past few years have seen a number of other foreign regulators start to more actively enforce compliance with their domestic AML/CTF laws. This is particularly apparent in the Asia-Pacific region, where many countries have enacted AML/CTF legislation and increased their enforcement efforts in an effort to gain membership to the FATF. For example, from the time it became an FATF Observer in January 2005 until the time it was accepted as a fully-fledged member in June 2007, China took considerable steps to strengthen its AML/CTF regime. ²⁷⁷ Its government passed more stringent AML/CTF laws and during 2005 alone, the People's Bank of China fined more than 600 financial institutions a total of CNY56.29 million (AUD\$5.3 million) for breaching the country's AML regulations. ²⁷⁸

Whilst there has been an apparent increase in the enforcement efforts of Asia-Pacific nations seeking FATF membership, the past few years have also seen an amplification of the enforcement activities undertaken by some countries that are already members of the international body. Amongst these countries is Japan, where regulatory authorities have made a focussed attempt to reprimand institutions in breach of their AML/CTF obligations. Most notably, after finding in October 2004 that Citibank's internal AML/CTF controls were inadequate, the Japanese Financial Services Agency barred the institution from Japanese

People's Bank of China, China Became a Full Member of Financial Action Task Force on Anti-Money Laundering (2007) http://www.pbc.gov.cn/english//detail.asp?col=6400&ID=872 at 17 July 2007.

PBC Fines BTMU CNY1.2mn for Violation of Anti-Money Laundering', SinoCast China Business Daily News (Beijing), 5 April 2006, 1.

Government bond auctions,²⁷⁹ revoked a number of its banking licences, and ordered the closure of all accounts at its four private banking branches in Japan.

Whilst the U.S. is typically hailed as setting the benchmark for AML/CTF regulation and enforcement, the action taken by Japanese regulatory authorities against Citibank is seemingly far more aggressive and more damaging than most of the enforcement actions waged against institutions in the U.S. Rather than simply imposing a large fine or monetary penalty upon the bank, which has often been the preference of U.S. regulators, the Japanese Financial Services Agency caused Citibank considerable reputational and financial damage by forcing it to shut down a lucrative component of its business.

3.5.2 Tighter crime-fighting networks

In recent years, a number of jurisdictions have enacted legislation to facilitate greater cooperation and information sharing between the organisations responsible for overseeing AML/CTF compliance and enforcement. In fact, one of the greatest drivers behind the enactment of the *USA PATRIOT Act* was the need to create tighter crime-fighting networks and remove several legal barriers impeding the sharing of information between:

- law enforcement bodies and intelligence agencies; and
- regulatory authorities and industry groups.

Whilst U.S. federal law enforcement agencies have long been able to access data relating to institutions' compliance with the *Bank Secrecy Act*, it was not until the *USA PATRIOT Act* came into force that the country's intelligence agencies were able to access the Currency Banking and Retrieval System (**CBRS**) database. Maintained by the Internal Revenue Service, this database is used to electronically warehouse all *Bank Secrecy Act* documents, including Foreign Bank & Financial Account Reports, Currency Transaction Reports, Suspicious Activity Reports, and Reports of Cash Payments over USD\$10,000 Received in a

²⁷⁹ 'Japan Closes Citibank Branches', *BBC News*, 17 September 2004 http://news.bbc.co.uk/1/hi/business/3666828.stm at 30 April 2006.

Trade or Business.²⁸⁰ Given the type and breadth of information it stores, the ability of the wider intelligence community to access the CBRS database has facilitated a more open dialogue amongst law enforcement and intelligence agencies, and aided in the investigation and prosecution of AML/CTF compliance failures. In doing so, it has potentially also heightened the AML/CTF legal risk faced by U.S. institutions.

Compliance failures that could once have slipped under the regulatory radar or fallen between bureaucratic cracks can now be more easily identified and prosecuted by a number of regulatory authorities. Historically, the utility of FinCEN data had been hampered by the overdependence of regulators and institutions on paper reporting. However, the advent of electronic reporting and the ability of intelligence agencies to now access the CBRS database, has theoretically strengthened the ability of government bodies to identify and investigate money laundering activities and breaches of AML/CTF legislation. This contrasts with the situation in Australia, where AUSTRAC has primarily relied on electronic reporting and has for many years granted a range of intelligence and law enforcement bodies access to its intelligence (both in relation to institutions, and the reports submitted by them). ²⁸¹

In addition to the enhanced collaboration between law enforcement and intelligence agencies, the past few years have also ushered in a period of heightened cooperation between financial services regulators and industry bodies. FinCEN in particular has made a concerted effort in recent times to work with industry bodies to ensure that U.S. institutions are meeting their AML/CTF obligations. According to some commentators, this public and private sector collaboration has effectively created an additional layer of regulatory oversight²⁸² and heightened the AML/CTF legal risk faced by institutions.

²⁸⁰ Brown, K., (Written Statement before the Committee on Banking, Housing and Urban Affairs, United States Senate, 28 September 2004).

Alexander, R., and Allen, C., 'Big Price for Lax Anti-Laundering' (2004) 169(204) American Banker 11.

Following the enactment of Australia's AML/CTF Act 2006 (Cth), AUSTRAC entered into Memorandums of Understanding (which enable partner agencies to access AUSTRAC information) with organisations including the Australian Commission for Law Enforcement Integrity and the Australian Secret Intelligence Service. During 2007-2008, the greatest users of AUSTRAC information included the Australian Taxation Office, Australian Federal Police, Australian Customs Service, and Australian Crime Commission. See Australian Transaction Reports and Analysis Centre, AUSTRAC Annual Report 2007-08 (AUSTRAC, Sydney, 2008) 51-59.

Arguably however, in several jurisdictions the increased dialogue between regulatory agencies and industry bodies has in fact diminished the AML/CTF legal risk faced by institutions. Indeed, it may have fostered a more cooperative approach to enforcement, where regulators are more inclined to work with industry participants to achieve AML/CTF compliance, rather than immediately launching enforcement actions against those in breach of their requirements. As stated in the U.K. FSA's Enforcement Handbook, the "open and cooperative relationship between firms and their supervisors, will, in some cases where a contravention has taken place, lead the [U.K. FSA] to decide against taking formal disciplinary action". ²⁸³

As previously discussed in **Chapter 1** of this thesis, regulatory authorities and industry participants operating in risk-based regimes may have different understandings regarding the way in which ML/TF risks should be assessed and prioritised. Clearly, better communication and cooperation between the public and private sector may ensure that there are common understandings of ML/TF risk, and help to alleviate some of the AML/CTF legal risk otherwise faced by institutions. Indeed, as Australia continues to implement its AML/CTF legislation, most major financial institutions and industry bodies (including the Australian Bankers' Association, Investment and Financial Services Association, and Australian Financial Markets Association), are seeking to limit their potential regulatory exposure (and/or the exposure of their members) by engaging in an open, ongoing dialogue with AUSTRAC.

As previously noted, this dialogue may limit the AML/CTF legal risk of Australian institutions by impacting the ability of regulatory authorities (in this case, AUSTRAC) to regulate and enforce compliance with AML/CTF legislation. Were the discussions between regulatory officials and regulated institutions (and/or the industry bodies representing them) to provide regulated institutions with an excessive ability to influence AML/CTF policy and

United Kingdom Financial Services Authority, Enforcement Handbook 4 http://fsahandbook.info/FSA/extra/4755.pdf at 12 July 2008.

its implementation, "regulatory capture" may occur.²⁸⁴ In such a case, the independence of regulatory officials may be compromised²⁸⁵ and the commercial interests of institutions may be prioritised above the public interest attached to the effective regulation of AML/CTF compliance. Regulated institutions may be able to push the boundaries of AML/CTF regulation (primarily by diluting their requirements – if not at the policy level, then certainly with respect to the compliance/enforcement approach of regulatory officials) and, by extension, limit their exposure to instances of non-compliance and/or undesirable regulatory actions in respect of non-compliance.²⁸⁶

3.5.3 The politics of enforcement

In some jurisdictions, the regulation and enforcement of AML/CTF legislation is largely attributable to the political environment and the attention being paid to AML/CTF issues by government officials. At times, the level of AML/CTF enforcement in a particular country has appeared to be directly proportionate to the level of support or criticism received by the presiding national government. As a general rule, the more acutely aware a government is of the importance of combating money laundering and terrorism financing, the greater is the pressure placed upon regulatory officials to instigate enforcement actions, and the higher is the degree of AML/CTF legal risk faced by institutions.

Throughout the 1980s and early 1990s, U.S. prosecutors displayed a great willingness to prosecute corporations for their wrongdoing. However, they seemingly broke with tradition in 1991, following the promulgation of the *U.S. Sentencing Guidelines*. Rather than seeking to criminally pursue most cases of corporate malfeasance, U.S. prosecutors agreed to forgo the criminal prosecution of several large companies for securities fraud violations, in

According to public choice theorists, regulatory capture occurs when individuals/corporations with a key interest in the outcome of policy or regulatory decisions are able to focus their resources and "capture" the influence of regulatory officials in order to secure desirable policy outcomes.

²⁸⁵ Jopson, B., 'Is the Gamekeeper Tied Down by the Big Four?', Financial Times (London), 14 September 2006. 8

²⁸⁶ It should be noted however that in certain jurisdictions, the fruition of regulatory capture may be hampered by the nature of the regulator and the review mechanisms/functions of international AML/CTF bodies. For instance, in Australia, regulatory capture may be impeded by the fact that AUSTRAC is an independent regulatory agency and, together with Australian AML/CTF laws and frameworks, it is subject to peer review by international organisations such as the FATF.

exchange for their payment of financial penalties, execution of certain remedial actions, and ongoing cooperation with regulatory and law enforcement authorities.²⁸⁷

However, the U.S. regulatory and enforcement environment again changed during the early 2000s after a number of significant corporate frauds highlighted the public policy need for corporations to be held accountable for their malfeasance. The government once again displayed a willingness to criminally prosecute companies such as Enron, WorldCom and Arthur Andersen for their wrongdoing. However, the severe consequences attached to the indictment of such organisations soon caused U.S. government officials, regulatory authorities and prosecutors to reconsider their approach to AML/CTF enforcement.

In March 2002, following its failure to cooperate with U.S. prosecutorial and regulatory officials, international accounting firm Arthur Andersen was indicted for its role in the Enron scandal. By the time the company was convicted several months later, it had collapsed and "an unmitigated disaster" was set in motion;²⁸⁹ a disaster that was only made worse by the legal proceedings that had been waged against it. The collateral damage caused – or in some cases, compounded – by Arthur Andersen's indictment was undeniable. The long-standing company went bankrupt, tens of thousands of employees were retrenched, shareholders lost their investments, and the 'Big 5' accounting firms essentially became the 'Big 4.'²⁹⁰ Indeed, the corporation's prosecution only made its demise that much more notable.

There are a number of complexities inherent in prosecuting certain types of legal persons. Indeed, the indictment or criminal prosecution of public companies is particularly problematic because any conviction is likely to punish innocent employees, shareholders and corporate constituents. Given that the defining characteristic of publicly traded companies is

²⁹⁰ Op cit n208, 1097.

²⁸⁷ Spivack, P., and Raman, S., 'Regulating the 'New Regulators': Current Trends in Deferred Prosecution Agreements' (2008) 45(2) American Criminal Law Review 159, 160.

See Memorandum from Larry D. Thompson, Op cit n207, Part I(B).
 See Ainslie, E.K., Indicting Corporations Revisited: Lessons of the Arthur Andersen Prosecution (2004)
 American College of Trial Lawyers

<http://www.actl.com/AM/Template.cfm?Section=All_Publications&Template=/CM/ContentDisplay.cfm&ContentFileID=51> at 4 August 2008.

their separation of ownership and control, the shareholders who essentially *own* the corporation do not *control* the actions of those working for it.²⁹¹ However, by imposing criminal penalties upon a corporation for the actions of its employees (rather than, for instance, punishing the employees themselves), it is arguably the shareholders who are punished. This is further discussed in the Riggs Bank case study contained in **Chapter 6** of this thesis.

Since the closure of Arthur Andersen, there has once again been a fundamental shift in the AML/CTF regulation of large U.S. corporations. Whilst some commentators claim that U.S. regulatory and law enforcement authorities have continued to "shoot first and ask questions later" 292 when pursuing corporate crime, this does not appear to be the case with respect to money laundering offences and criminal AML/CTF compliance failures. On the contrary, it appears that U.S. federal prosecutors have generally sought to find ways of tightly regulating AML/CTF compliance without unnecessarily prosecuting financial institutions. They have placed increased reliance on deferred and non-prosecution agreements and today, will generally only lay criminal charges against a U.S. corporation in the rarest and most extreme circumstances. 293 As further discussed in **Chapter 7** of this thesis, the case of foreign financial institutions appears to be somewhat different, with regulatory officials and prosecutors seemingly more willing to take formal legal action against these entities in circumstances where their prosecution will have little impact on U.S. interests.

According to former U.S. Attorney-General Alberto R. Gonzales, whilst U.S. government authorities are not afraid to target corporate misbehavior, prosecutors certainly need to consider any potential "collateral consequences" when determining whether to prosecute an institution.²⁹⁴ These comments certainly suggest a degree of reluctance to pursue criminal proceedings in circumstances where other less intrusive, less disruptive and less damaging enforcement options are available. However, whilst this less aggressive and perhaps more strategic approach to AML/CTF enforcement of AML/CTF may be preferable from the

²⁹¹ Op cit n170.

Isaac, W.M., 'Harsh Approach to Regulation is Backfiring' (2005) 170(191) American Banker 1.

²⁹³ Op cit n208, 1098.

Hamilton, W., 'KPMG Avoids Potential Collapse', Los Angeles Times (Los Angeles), 30 August 2005 http://articles.latimes.com/2005/aug/30/business/fi-kpmg30 at 21 January 2009.

standpoint of most financial institutions, it has not been without criticism. As detailed in **Chapter 6** of this thesis, cases such as Riggs Bank have at times raised questions about whether the enforcement of AML/CTF legislation is occasionally still too lax.

3.6 Conclusion

Just as money laundering and terrorism financing can seamlessly transcend geographic boundaries, so too can the AML/CTF legal risk faced by many institutions. Over the past few years, a number of countries have enacted municipal and extraterritorial legislation. Such legislation has expanded the AML/CTF obligations placed upon financial institutions, attached criminal liability to a number of AML/CTF offences, and created an additional layer of regulatory oversight with respect to institutions' AML/CTF compliance. Theoretically, it has heightened institutions' AML/CTF legal risk.

An institution's AML/CTF legal risk will always be somewhat proportionate to the scope of applicable AML/CTF laws, and the severity of the possible criminal penalties attached to non-compliance with such laws. An institution subject to an elaborate array of national and extraterritorial AML/CTF laws will likely face far greater risk than a comparable entity operating in a jurisdiction with relatively skeletal AML/CTF legislation. That said, even in those jurisdictions where municipal AML/CTF legislation creates a copious number of AML/CTF obligations and offences, the AML/CTF legal risk faced by covered institutions will still fundamentally hinge upon the aggressiveness with which AML/CTF compliance is enforced.

Where regulatory, law enforcement and prosecutorial authorities take an uncompromising stance with respect to the enforcement of AML/CTF compliance, institutions will generally face a higher level of AML/CTF legal risk. As a general rule, the more attention government officials pay to money laundering offences and AML/CTF compliance failures, the greater is the tenacity with which local regulators will pursue AML/CTF compliance, and the willingness with which local prosecutors will launch criminal enforcement proceedings against those institutions in breach of their AML/CTF requirements. This is not to simplify

the factors that may sculpt a jurisdiction's enforcement environment with respect to AML/CTF. Of course, the aggressiveness of enforcement efforts in a particular nation state may of course be heavily impacted by additional factors, including whether the relevant jurisdiction is a member of international bodies such as the FATF.

Clearly, an institution's exposure to criminal culpability for an AML/CTF compliance failure is not only attributable to the number of relevant offences and penalties in a particular jurisdiction, but to the overriding enforcement environment there. That said, even in the U.S. (which is often held to have the most aggressive AML/CTF enforcement regime in the world), there have been documented instances where prosecutors and regulatory authorities have been reluctant to wage formal criminal proceedings against a non-compliant institution. As the evolving enforcement environment in the U.S. has shown, the consequences of imposing harsh criminal penalties upon an institution may in fact limit the AML/CTF legal risk faced by entities operating there.

Following the collapse and prosecution of corporations such as Enron and Arthur Andersen, U.S. authorities have seemingly taken the view that criminal enforcement actions might not be the most effective way of addressing instances of corporate crime and legislative non-compliance. The collateral damage that can accompany a company's indictment appears to have dissuaded U.S. regulatory officials and federal prosecutors from pursuing criminal enforcement actions in a number of cases. In the past few years there have undoubtedly been many instances where potential criminal proceedings against an institution have been set aside in favour of prosecuting culpable employees, pursuing a civil action and/or securing institutional change via one of the cooperative agreements outlined in **Chapter 5** of this thesis.

Thus, whilst an institution's AML/CTF legal risk is likely to be far higher in the U.S. than other jurisdictions, it seems that the overall risk that institutions face there is overstated – least of all by regulatory authorities and institutions themselves. Whilst AML/CTF legislation provides authorities with an arsenal of enforcement tools, it appears that formal enforcement actions and criminal penalties are now only invoked in the rarest of

circumstances. This will potentially be the case where an institution has committed significant, ongoing breaches of its AML/CTF obligations, and/or has otherwise been recalcitrant or unresponsive to regulatory efforts to rectify its behaviour/control failures.

Statistics contained in the *U.S.S.C. 2008 Sourcebook* indicate just how few institutions are criminally prosecuted in the U.S. for money laundering offences and/or criminal breaches of AML/CTF legislation. They suggest that many non-compliant institutions manage to avoid even the imposition of a criminal fine for their compliance failures. Although this may largely be due to the reluctance of U.S. authorities to instigate criminal enforcement actions against institutions, it may also be attributable to the heightened cooperation between regulatory bodies and the financial services industry.

Increased dialogue between the public and private sectors in relation to AML/CTF compliance may have effectively limited institutions' AML/CTF legal risk in recent times. By fostering an environment that focuses on prevention, communication and collaboration, many U.S. regulatory authorities are now working more cooperatively with institutions to correct their compliance deficiencies before any criminal enforcement action is even considered. As reflected in U.S. sentencing statistics and the relatively small number of corporate prosecutions for breaches of AML/CTF legislation, this heightened communication between the public and private sectors has seemingly diminished the need for (or at least, discouraged) regulatory authorities from taking decisive enforcement action against financial institutions.

Greater cooperation between regulatory authorities and the 'regulated' sectors is likely to have played some role in lowering the apparent risk of institutions being criminally pursued for their AML/CTF non-compliance. From the perspective of institutions, the increased dialogue may have enabled them to build better relationships with regulatory authorities and gain a better understanding of how such authorities will assess their ML/TF risks and the effectiveness of their risk controls. From the standpoint of regulatory authorities however, the enhanced cooperation with financial institutions might have given them a greater ability

to identify and address any 'compliance gaps' earlier without the need for criminal enforcement proceedings.

Chapter 4

Looking at AML/CTF Legal Risk through the Lens of Civil Law

"We don't give our criminals much punishment, but we sure give 'em plenty of publicity" – Will Rogers

4.1 Introduction to civil liability and AML/CTF legal risk

Criminal penalties are simply one aspect of an effective regulatory framework. In accordance with the 'strategic regulation theory', successful corporate regulation requires the availability of a number of approaches and outcomes; both civil and criminal, as well as individual and corporate.²⁹⁵ Whilst criminal sanctions may form the apex of any regulatory pyramid,²⁹⁶ there should be layers of other enforcement tools and regulatory options supporting them.

This Chapter seeks to address an institution's potential AML/CTF legal risk under civil law. As previously noted in **Chapter 1** of this thesis, the term "civil" is used throughout this Chapter in an inclusionary fashion to encompass every legal course of action, type of legal proceeding or penalty that is not strictly "criminal" in nature. Unless expressly stated, the definition of civil law used throughout this thesis necessarily includes those areas of the law that might otherwise technically fall under the umbrella of equity.

Whilst many governments have enacted municipal laws attaching criminal liability to certain breaches of AML/CTF requirements, AML/CTF compliance failures have typically been addressed through the use of civil, rather than criminal, proceedings. Since the enactment of the USA PATRIOT Act and similar pieces of AML/CTF legislation, a number of institutions have incurred sizeable civil penalties for failing to fulfil their AML/CTF obligations. Whilst there has seemingly been enough evidence in at least some of these cases to successfully prosecute the relevant institution, the preference of many regulatory

²⁹⁵ Clough, J., and Mulhern, C., The Prosecution of Corporations (2002) 239.

²⁹⁶ Fisse, B., and Braithwaite, J., Corporations, Crime and Accountability (1993) 140-142.

authorities has been to address corporate AML/CTF compliance failures at civil law. As previously discussed in **Chapter 3** of this thesis, this is partly attributable to their desire to avoid the commercial consequences (as well as the potential delays and uncertainty)²⁹⁷ associated with the criminal prosecution of corporate entities.

In recent years, institutions operating in particular jurisdictions have seemingly faced heightened levels of AML/CTF legal risk in relation to their civil law obligations. This is not only due to the enforcement preferences of regulatory authorities, but also the disconnect that has at times arisen with respect to institutions' obligations at criminal and civil law. Whilst civil and criminal law are capable of operating concurrently, some institutions have identified a potential conflict between their rights and responsibilities under statute, contract law, and equitable constructive trust principles. This has been particularly apparent in the U.K., where several entities have complied with their AML/CTF obligations at criminal law, only to find themselves exposed to liability at civil law.

Given the various AML/CTF obligations commonly imposed upon financial institutions, and the types of civil penalties that can accompany a contravention of those obligations, consideration of an institution's AML/CTF legal risk at civil law falls into several parts. This Chapter seeks to:

- address the types of civil actions and civil penalties that contraventions of municipal and/or extraterritorial AML/CTF legislation may attract;
- detail the principles of constructive trusts and outline the circumstances that may see an
 institution face liability as a constructive trustee in relation to certain money laundering
 activities;
- highlight the way in which an institution's AML/CTF legal risk may be increased by any
 misalignment between their obligations at civil and criminal law; and
- examine the ways that an institution may best seek to balance its various AML/CTF obligations, and mitigate and manage its risk at civil law.

Bugg, D., 'Compliance through Prosecution (or Haunted by Kable)' (Speech delivered at the Australasian Law Teachers' Association Conference, Canberra, 3 July 2000).

As with **Chapter 3** of this thesis, the U.S. and the U.K. are the focal points of discussion around civil AML/CTF legal risk. In both these jurisdictions, there has been a number of significant civil actions involving – and a number of notable civil penalties given to – individuals/institutions in breach of local AML/CTF laws. Further, with respect to the U.K. experience, there has been a number of interesting case law developments in relation to the potential conflict between institutions' obligations under statute, contract law, and in equity.

Whilst Australia is yet to see any institution face civil proceedings for contravening the country's *AML/CTF Act 2006* (Cth), the U.S. and the U.K. provide interesting case studies for analysing the levels of risk faced by institutions operating under risk-based AML/CTF regimes. As noted previously however, differences between countries' enforcement and legal environments mean that not all of the analysis contained in this Chapter will be entirely relevant to determining the civil AML/CTF legal risk faced by institutions operating outside the U.S. and the U.K. For instance, whilst the U.S. and Australian enforcement experiences may be similar insofar as the courts in both countries may impose civil penalties upon noncompliant individuals/institutions, the U.S. civil penalty regime is broader than the Australian regime because it also gives regulators broad authority to impose such penalties directly. Thus, there is seemingly greater executive power and leverage in the U.S., and this must necessarily be taken into account when determining the likely enforcement environment, and civil AML/CTF legal risk faced by institutions, in Australia.

4.2 Civil liability & its associated penalties

In contrast to criminal penalties, which typically seek to punish illegal conduct, civil penalties aim to right a legal wrong, enforce an agreement, settle a dispute or rectify a compliance failure. With the exception of one or two specific penalties (including civil forfeiture, which seeks to both recoup improperly gotten gains and punish a wrongdoer), civil penalties are primarily concerned with compensation and fairness, rather than deterrence or retribution. Thus, it is perhaps unsurprising that where an institution has inadvertently or unintentionally engaged in an AML/CTF compliance failure, civil penalties have often been

invoked to secure institutional change and ensure that similar control failures do not arise again in the future.

In order to succeed with a case at civil law and justify the imposition of any civil penalty, a claimant must prove the alleged conduct alleged on the "balance of probabilities". As this is considerably less onerous than the "beyond reasonable doubt" standard of proof required in criminal proceedings, an institution that successfully avoids criminal prosecution in relation to its AML/CTF compliance failures may nevertheless face civil enforcement proceedings. In contrast to criminal offences and enforcement actions, civil proceedings do not generally require regulatory authorities to establish any fault element (e.g. knowledge or recklessness) on the part of a respondent institution.

Where an institution has fallen foul of its AML/CTF legislative requirements, its resulting legal risk and exposure to civil penalties will rest upon a number of factors. These include the specific requirements it has contravened, the jurisdiction(s) within which such contraventions took place, the apparent enforcement environment, and the number and type of matters that the relevant regulatory authority/court can consider when determining the most appropriate civil penalties. Under municipal laws, the matters to be taken into account for the purposes of imposing a civil penalty may be discretionary or prescriptive. For instance, when determining the appropriate quantum of a civil monetary penalty for a contravention of AML/CTF legislative requirements, Section 175(3) of the AML/CTF Act 2006 (Cth) stipulates that Australian courts must consider all relevant criteria, including:

- the nature and extent of the relevant AML/CTF contravention;
- the nature and extent of any loss suffered as a result of the AML/CTF contravention;
- the circumstances surrounding the AML/CTF contravention; and
- whether the relevant institution has previously engaged in similar conduct.

Depending on the jurisdiction(s) within which an institution has contravened its AML/CTF obligations, any civil penalties imposed upon it may be supplemented by formal orders requiring that certain corrective actions be taken. The purpose of such orders is generally to ensure that an institution's AML/CTF controls and AML/CTF program are robust enough

to meet legislative compliance and prevent similar legislative contraventions from arising in future. In the U.S., these types of formal orders have accompanied most of the significant civil monetary penalties imposed upon non-compliant institutions in the past few years.

4.2.1 Civil monetary penalties

As demonstrated by a number of recent enforcement actions, civil monetary penalties have often been used to address contraventions of AML/CTF legislation. This is certainly in accordance with the way that many municipal AML/CTF laws have been framed. Indeed, certain pieces of AML/CTF legislation have been drafted in way that explicitly endorses the use of civil penalties in preference to criminal penalties such as fines and imprisonment. When Australia's Anti-Money Laundering and Counter-Terrorism Financing Bill 2005 (Cth) was initially drafted, it primarily sought to address AML/CTF compliance failures through the use of criminal penalties. However, prior to its enactment as the AML/CTF Act 2006 (Cth), the focus of the Bill shifted significantly. Many references to criminal offences and criminal liability were removed and replaced with civil penalty provisions. Whilst the Act still provides criminal penalties for breaches of specific prescriptive requirements, the Australian Government seemingly believed that a civil penalty regime was more appropriate to address contraventions of the Act's risk-based requirements.

In the U.S., contraventions of certain AML/CTF requirements carry civil monetary penalties ranging from USD\$3,000 to 1 per cent of their assets or USD\$1 million (whichever is greater). Pursuant to an interagency policy statement adopted by U.S. federal banking agencies, the size of any civil monetary penalty imposed upon an institution will generally depend upon the duration of its AML/CTF compliance failure(s), any refusal to cooperate with regulatory authorities, and the presence (or otherwise) of a compliance program. As stated in the U.S. Treasury Department's "Interagency Policy Regarding the

²⁹⁸ Civil penalty provisions now apply to a range of offences under the Act, including the failure to conduct customer due diligence before providing a service designated by the Act, failure to report suspicious matters, failure to adopt a risk-based AML/CTF program, and failure to retain relevant AML/CTF records.

²⁹⁹ Allens Arthur Robinson, Civil Penalty Provisions in Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (2006) http://www.aar.com.au/pubs/fmres/foamldec06.htm at 24 August 2007.

Assessment of Civil Money Penalties by the Federal Financial Institutions Regulatory Agencies", the quantum of such a penalty may also be determined by reference to the following five factors:

- the size of the institution's financial resources;
- any apparent good faith of the part of the institution;
- the gravity of the legislative contravention(s);
- any history of similar contraventions; and
- any other factors that justice may require.³⁰⁰

Many commentators and banking professionals have held that more serious contraventions of AML/CTF legislation may lead to the imposition of monetary penalties that are so steep, they are financially crippling for an institution. However, whilst this may be true in a theoretical or academic sense, there does not appear to be any documented cases of an institution being forced to close as a direct result of the civil monetary penalties imposed upon it for non-compliance with AML/CTF or economic and trade sanctions legislation. Even though institutions such as UBS³⁰² and ABN Amro³⁰³ have incurred civil monetary penalties totalling USD\$100 million and USD\$80 million (respectively), the size and financial resources maintained by both these institutions makes it highly unlikely that such penalties caused any kind of financial strain upon them. Evidently, some global banking institutions are so profitable that the amount of funds they launder or use to facilitate transactions in breach of AML/CTF legislation, may pale in comparison to the possible monetary penalties their non-compliance might attract.

Office of the Comptroller of the Currency, *Interagency Statement of Civil Monetary Penalties* (1998) OCC 98-32 http://www.occ.treas.gov/ftp/bulletin/98-32.txt at 23 August 2008.

See De Koker, L., 'Some Thoughts on the Impact of Customer Due Diligence Measures on Financial Exclusion' (2006) 13(1) *Journal of Financial Crime* 26.

³⁰² On 10 May 2004, the U.S. Federal Reserve Board of Governors assessed a civil monetary penalty of USD\$100 million against UBS for repeatedly conducting U.S. banknote transactions for, and illegally transferring funds to, countries the subject of U.S. sanctions regulations. See Mojuyé, B., 'What Banks Need to Know about the Patriot Act' (2007) 124(3) Banking Law Journal 258.

On 19 December 2005, FinCEN, OFAC and a number of state banking regulators concurrently assessed a civil monetary penalty of USD\$80 million against ABN Amro for failing to identify, analyse and report suspicious activities, and facilitating transactions in violation of OFAC sanctions regulations. See Byrne, J.J., and Kelsey, M.D., 'AML Enforcement Actions: What Can We Learn?' (2006) 27(3) ABA Bank Compliance 11.

The imposition of a USD\$80 million or USD\$100 million civil monetary penalty upon a smaller or community-based institution would clearly have the potential to significantly impact its ability to continue operating. Indeed, many such institutions would be financially drained if they were ever to incur the quantum of civil monetary penalties imposed upon international banking giants such as UBS and ABN Amro. However, unless the most brazen contraventions of AML/CTF legislation were committed over a period of time, it is highly unlikely that a smaller institution would ever incur penalties in the same vicinity as these institutions. As previously noted, the size of an institution's financial resources may be taken into account for the purposes of determining an appropriate penalty. Were a small community bank to generate annual profits of USD\$2 million, it is improbable that a court would seek to address its AML/CTF compliance failures through a civil monetary penalty totalling far more than that amount. As previously stated, the fundamental purpose of civil penalties is not to punish a wrongdoer but rather, to encourage future compliance and compensate any readily identifiable 'victims'. 304

Just as criminal fines can be imposed upon individuals and institutions alike, so too can civil monetary penalties. Although such penalties appear to be overwhelmingly imposed upon corporate entities, in recent years some regulators have demonstrated a willingness to also impose them upon individuals. For instance, in November 2005 the U.K. FSA imposed its first civil monetary penalty upon an individual following September 11 and the subsequent London bombings. That individual, the Managing Director of Investment Services U.K. (Ltd), was ordered to pay £30,000 (AUD\$72,000) in relation to his company's contraventions of municipal AML/CTF regulations. Whilst this penalty may seem relatively small when compared with those imposed upon a number of other institutions, its imposition is significant because it marked a potential increase in the AML/CTF legal risk faced by organisations' senior management teams.

³⁰⁴ It should be noted however that unlike other types of financial crime (e.g. fraud), there is usually a lack of identifiable victims with money laundering activities.

McNeil, C., Laundering Lessons from the UK (2006) Risk Management Magazine http://www.riskmanagementmagazine.com.au/articles/1D/0C047E1D.asp?Type=125&Category=1241 at 29 July 2007.

4.2.2 Orders and agreements

In addition to civil monetary penalties, an institution in contravention of its AML/CTF legislative obligations may be subject to binding orders issued by regulatory authorities or the courts. Typically used to secure an institution's ongoing AML/CTF compliance, these Orders are individually stylised to an institution's compliance failures. For example, in 2004 the Office of the Comptroller of the Currency (OCC) ordered the New York National Bank to prevent its Chief Operating Officer from overseeing the organisation's Bank Secrecy Act and AML/CTF functions, and ensure that its new Compliance Officer reported directly to the Board audit committee. 306 Whilst these requirements may appear unusually narrow, they were specifically designed to remedy the bank's previous legislative contraventions, which had arisen largely because of failures on the part of the institution's Chief Operating Officer, and a lack of transparency around the oversight of the bank's AML/CTF compliance.

By virtue of § 8 of the Federal Deposit Insurance Act of 1950 (P.L. 81-797, 64 Stat. 873), U.S. federal banking regulators have a palette of administrative powers at their disposal to address violations of the AML/CTF requirements contained in the Bank Secrecy Act. These powers include the ability to issue orders that:

- require an institution to cease and desist unlawful, unsafe or unsound practices;
- require an institution to undertake specified affirmative actions;
- remove or prohibit affiliate parties from participating in the affairs of an institution; and
- terminate the insurance of an institution that violates any applicable law.³⁰⁷

This last power is arguably one of the most powerful sanctions available to banking regulators, and it may partly explain their apparent reluctance to initiate formal enforcement proceedings against institutions that have fallen foul of their AML/CTF obligations. Were an institution to lose its deposit insurance as a result of its indictment for a money laundering or terrorism financing offence and/or a contravention of AML/CTF legislation, this could create an extensive run on its deposits and, in severe cases, lead to its closure.

³⁰⁶ Op cit n164. ³⁰⁷ Op cit n190, 59.

Whilst many U.S. banking regulators have the power to unilaterally impose a cease and desist order upon an organisation, they will frequently seek an institution's consent to any order requiring it to discontinue certain activities or undertake specific remedial actions. Rather than overtly penalising an institution for its AML/CTF compliance failures, these consensual orders are intended to redress an organisations' lax internal controls and the environment that gave rise to its compliance issues. Non-compliant institutions that fully cooperate with the relevant regulatory authorities and agree to the imposition of a cease and desist order, may therefore be able to minimise their AML/CTF legal risk. This is in comparison to non-compliant institutions that actively resist or obstruct the imposition of such an order, which may place themselves at greater risk of facing more severe penalties.

4.2.3 Civil forfeiture

In addition to civil monetary penalties, institutions that contravene their AML/CTF legislative obligations by facilitating (actively or otherwise) money laundering activities, may face a civil forfeiture action initiated by government authorities. In contrast to criminal forfeiture (or asset confiscation), civil forfeiture enables governments to recover the proceeds of crime even in the absence of criminal charges or a criminal conviction. Thus, it may be used effectively in circumstances where a criminal trial is likely to be lengthy, expensive and/or unsuccessful due to a defendant's vigorous denial of all (or at least the most serious) criminal charges against them.³⁰⁸

Although the objectives of criminal and civil forfeiture are fundamentally the same (i.e. to recover the proceeds of crime and ensure that those who illegally obtained such funds are denied the opportunity to use them), the procedures attached to each are often very different. Whilst criminal forfeiture involves waging an action against a person (*in personam*) as part of a criminal case, civil forfeiture involves bringing an action specifically against certain property (*in rem*). As a result, civil forfeiture may prove to be successful in circumstances where a criminal forfeiture action would otherwise have been

³⁰⁸ Cassella, S.D., 'The Case for Civil Forfeiture: Why In Rem Proceedings are an Essential Tool for Recovering the Proceeds of Crime' (Paper presented at the 25th Cambridge International Symposium on Economic Crime, Cambridge, 7 September 2007) 7.

defeated (for instance, in circumstances where the relevant defendant is deceased, unidentifiable, or unable to be extradited from a foreign jurisdiction).

In civil forfeiture cases, the relevant government is the plaintiff, the property is the defendant, and any persons objecting to the forfeiture and claiming an interest in the property are claimants.³⁰⁹ If the court overseeing a civil forfeiture action determines on the balance of probabilities or the preponderance of the evidence that the disputed property represents the proceeds of unlawful activity, it may order its forfeiture to the state.³¹⁰ In the U.S. for example, funds sufficiently involved with money laundering activities may be forfeited to the U.S. federal government pursuant to 18 U.S.C § 981. Given that the test of "involvement" is relatively broad, even legitimate funds can be the subject of a civil forfeiture action if they have been used to facilitate the money laundering process and/or make it easier.³¹¹ Thus, an institution that enables a wealthy customer to launder a small amount of dirty funds through their bank accounts, may find that the entire contents of those accounts are forfeited if the large balances contained therein aided the concealment of the laundered funds.

In many jurisdictions, any institution or individual against whom a civil forfeiture order is made will have a formal right to contest that order and convince the court that the forfeited property should be returned to them. For instance, any person claiming an interest in funds seized by the U.S. federal government in a civil forfeiture action can file a claim asserting their interest in those funds. As stipulated by 18 U.S.C. § 983(a)(3), the government must file a complaint for forfeiture within 90 days of receiving that claim, or return the funds to the claimant. If it files a complaint and alleges that the relevant funds were

³⁰⁹ Op cit n308, 3.

Simser, J., 'The Significance of Money Laundering: The Example of the Philippines' (2006) 9(3) Journal of Money Laundering Control 293, 297.

³⁵¹ See United States v. \$557,933.89, More or Less, in United States Funds, 287 F.3D 66 (2d Cir. 2002). See also United States v. All Monies (\$477,048.62) In Account No. 90-3617-3, 754 F. Supp. 1467, 1473 (D Haw. 1991), and United States v. Baker, 227 F.3d 955, 970 n. 4 (7th Cir. 2000) and United States v. McGauley, 279 F.3d 62, 76 n. 14 (1st Cir. 2002).

³¹² See 18 U.S.C \S 983(a)(2).

involved in or used to facilitate a criminal offence, it must establish that there was "a substantial connection" between those funds and the alleged offence. 313

In the past few years, the U.S. Department of Justice has used civil forfeiture to confiscate the proceeds of crime in many money laundering cases. During 2006, it recovered USD\$1.2 billion in forfeited assets; USD\$804 million (or 67 per cent) of which was seized via contested or uncontested civil forfeiture claims. 314 This statistic clearly highlights the practicality of, and potential success rates attached to, the use of civil forfeiture actions rather than criminal asset confiscation. However, given that hundreds of billions of dollars is believed to be laundered each year, it also demonstrates the minimal level of AML/CTF legal risk that institutions may practically face at civil law with respect to any funds sufficiently connected to money laundering activities.

In addition to the U.S., there are civil forfeiture regimes in a number of other jurisdictions including Australia, South Africa, the Republic of Ireland, the Philippines and the U.K. 315 As opposed to fines and civil monetary penalties, which might only directly impact the institutions upon which they are imposed, it is interesting to note that the civil forfeiture laws in these countries may have an indirect deterrent effect on money launderers. Indeed, the underlying purpose of money laundering is to obscure and protect the proceeds of crime, and civil forfeiture is capable of removing such funds from the individuals seeking to legitimise them.

4.2.4 Shareholder derivative suits

Whilst an institution's AML/CTF legal risk will largely be determined by available civil penalties and the propensity of regulatory authorities/the courts to invoke them, it may also rest upon the types of civil lawsuits available to other interested parties. These lawsuits may arise outside the confines of applicable AML/CTF laws, and vary amongst different jurisdictions. In the U.S. for instance, institutions that fail to meet their AML/CTF

³¹³ See 18 U.S.C § 983(c).

Op cit n308, 5.
Op cit n308, 2.

compliance obligations may find themselves facing one or more shareholder derivative suits.³¹⁶

The last few years have seen a marked increase in the number of shareholder derivative suits waged against the directors of institutions in breach of U.S. municipal laws.³¹⁷ These suits are filed by shareholders (on behalf of their corporation) in circumstances where organisational officers or directors have violated one or more of the fiduciary duties they owe to the corporation.³¹⁸ They are separate and distinct from 'direct shareholder actions', which necessarily hinge upon the infringement of individual shareholder rights.³¹⁹ Whilst these types of lawsuits relatively unique to the U.S., they historically emerged in equity as a means for shareholders to enforce a corporate right or remedy a legal wrong in circumstances where the relevant directors failed to do so.³²⁰

With respect to contraventions of AML/CTF legislation, the directors of U.S. institutions such as Riggs Bank and the Bank of New York have previously faced shareholder derivative suits alleging that their institutions' AML/CTF compliance failures were attributable to their personal "systematic wrongdoing", 321 "reckless mismanagement" 322 and breaches of fiduciary duties. Given the media coverage and regulatory attention devoted to the AML/CTF failings of both institutions, they are perhaps representative of many AML/CTF-related actions. Indeed, shareholder derivative suits have typically been initiated against the directors of institutions that have:

These suits provide a device to deal with an essential problem of enforcement in company law. The challenge of AML is underlined by problems of enforcement in corporate and securities regulation where financial institutions use the corporate form as their principal structure to conduct business.

Robinson, T.L., 'A New Interpretation of the Contemporaneous Ownership Requirement in Shareholder Derivative Suits: In re Bank of New York Derivative Litigation and the Elimination of the Continuing Wrong Doctrine' (2005) 1 Brigham Young University Law Review 229.

³¹⁸ Jones Day, Shareholder Derivative Actions - Overview

http://www.jonesday.com/shareholder derivative actions/ at 24 June 2007.

Li, X., A Comparative Study of Shareholders' Derivative Actions: England, the United States, Germany and China (Ph.D., Kluwer Law International, 2007) 3.

³²⁰ See 19 A. Jur. 2D Corporations § 2250 (2003).

³²¹ 'Bank of New York Wins the Dismissal of Shareholder Suit', *The Wall Street Journal* (New York) 29 November 2001, B14.

^{&#}x27;Some Shareholders Sue Bank of New York', *The New York Times* (New York), 25 September 1999 http://query.nytimes.com/gst/fullpage.html?res=9E06E4D7133FF936A1575AC0A96F958260 at 3 November 2007.

- incurred significant civil monetary penalties and/or criminal fines for their noncompliance with AML/CTF legislation; and
- experienced one or a combination of the following:
 - (i) negative findings arising from regulatory reviews of, or investigations into, their AML/CTF compliance failures;
 - (ii) criminal charges being laid against one or more employees/officers in relation to their contraventions of AML/CTF laws; and/or
- (iii) reputational loss stemming from their poor AML/CTF compliance record. Thus, an institution's AML/CTF legal risk is not strictly limited to the imposition of civil penalties. It may also extend to civil lawsuits waged in the aftermath of any formal enforcement proceedings.

Although most shareholder derivative suits have generally been filed after the initiation of formal enforcement proceedings and the imposition of related penalties, one of the greatest impediments to the success of these claims has been, perhaps surprisingly, a lack of evidence. Further, this situation is unlikely to change in the near future due to the decision of the Delaware Supreme Court in *Stone v. Ritter*, 911 A.2d 362 (Del. 2006) (**Stone v. Ritter**). This case involved a shareholder derivative suit which alleged that 15 current and former directors of AmSouth Bancorp breached their fiduciary duty of good faith and, in doing so, gave rise to repeated violations of federal AML/CTF regulations and over USD\$50 million in fines, civil monetary penalties and legal costs. The lawsuit arose shortly after FinCEN released a damning investigatory report in relation to AmSouth Bancorp's compliance failures and inadequate AML/CTF controls. The fact that the case was heard and decided in Delaware is significant from a precedent perspective, given that most U.S. multinational financial institutions are registered in that state and will therefore be subject to its company laws.

A lack of evidence has not been the only impediment to the success of shareholder derivative suits. Whilst such analysis is beyond the scope of this thesis, it might be argued that these lawsuits are particularly difficult for claimants because the standards of common law duties imposed on directors vis a vis the company and shareholders, are not apposite (and/or not otherwise easily adaptable) to the duties owed to the State under AML/CTF legislation.

David, P., 'Ruling in AmSouth Case Offers Boards a Reprieve' (2006) 171(46) American Banker 2.

The shareholder derivative suit in Stone v. Ritter was ultimately dismissed because the claimant shareholders failed to demonstrate that AmSouth Bancorp's directors consciously ignored "red flags" 325 that their institution's AML/CTF compliance mechanisms and reporting structures were inadequate.³²⁶ According to the court, it was not sufficient for the shareholders to base their action entirely on the findings of the previously released FinCEN report and/or the penalties paid by the institution in relation to its AML/CTF compliance failures. 327 To be successful, the claimants needed to do more than just "equate a bad outcome with bad faith". They had to allege "particularised facts that created reason to doubt whether the directors had acted in good faith in exercising their oversight responsibilities". 328

In accordance with the court's ruling in Stone v. Ritter, an AML/CTF-related shareholder derivative suit based upon an alleged breach of the duty of good faith, will not be successful unless there is proof that the relevant directors knew that they were not discharging their fiduciary obligations. This standard of proof may be highly problematic for shareholders as the obligation to act in good faith does not establish an independent fiduciary duty that assumes the same importance as the duties of care and loyalty. Whilst breaches of the latter fiduciary duties may create liability directly, a failure to act in good faith can only establish liability *indirectly*. ³²⁹ Accordingly, an alleged breach of the fiduciary duty of good faith is "possibly the most difficult theory in corporation law upon which a plaintiff might hope to win judgment" 330

As the ruling in Stone v. Ritter clearly highlights the difficulties inherent in proving an alleged breach of good faith, it has the potential to diminish directors' AML/CTF legal risk

³²⁵ Stone v Ritter upheld the notion that a director's duty to act is most easily triggered when there are "red flags" indicating that something is wrong with the way their entity is being operated. See MorrisJames, Supreme Court Interprets the "Duty" to Act in Good Faith (2006) Delaware Business Litigation Report http://www.delawarebusinesslitigation.com/archives/case-summaries-supreme-court-interprets-the-duty-to- act-in-good-faith.html > at 19 November 2007.

American Bar Association, Director Oversight Duties after Caremark (2001)

http://www.abanet.org/buslaw/committees/CL996000pub/newsletter/200703/ at 24 November 2007. Op cit n324.

³²⁸ Ibid.

³²⁹ Op cit n326.

³³⁰ Ibid.

by deterring other shareholders from initiating similar suits. Undoubtedly, the case demonstrates that shareholders must have specific facts to support their claims. Even the most scathing regulatory review will not guarantee a successful outcome for claimant shareholders because a court "isn't going to allow people to simply throw an allegation by FinCEN on the court to create a case". ³³¹ Gathering the evidence required for shareholder derivative suits may prove difficult for many claimants, who may be so removed from their institution's day-to-day operations that they are unable to identify any evidence of wrongdoing beyond that already noted in regulatory reviews and/or formal enforcement proceedings.

4.2.5 International civil lawsuits

A civil lawsuit waged against the Bank of New York in May 2007 demonstrates that an institution's non-compliance with municipal AML/CTF legislation may give rise to previously unforeseen litigation in a foreign jurisdiction. Initiated by the Russian government in the Moscow Arbitration Court, the lawsuit marks the first time that a civil case involving the U.S. Racketeer Influenced and Corrupt Organizations Act of 1970 (18 U.S.C. § 1961, et seq.) (RICO Act) has been filed in a foreign court. Although the Act was originally enacted to address organised crime, it contains a number of civil provisions. These provisions are frequently used in cases involving large corporations because they entitle a plaintiff to recover up to three times as much as their actual damages.

Apart from the interesting jurisdictional issues it raises, the case against the Bank of New York is like no other AML/CTF-related action ever launched against an institution. Indeed, it appears to prove that money laundering activities and AML/CTF compliance failures – even if they arose over a decade ago – may resurface to cause an institution significant legal, reputational and financial risk.

³³¹ Op cit n324.

In these proceedings, the Russian government is seeking 579.096 billion roubles (USD\$22.5 billion)³³² in damages from the Bank of New York for its role in a 1990s money laundering scheme that enabled approximately USD\$7 billion to be siphoned out of Russia and placed into offshore accounts.³³³ It alleges that from 1996 to 1999 inclusive, the Bank of New York created a "system through which conditions were made for companies and Russian banks to not make the proper payments, thus inflicting a loss against the Russian Federation".³³⁴ According to the claimant, the result of this was that the Russian Federal Customs Service was deprived of billions of dollars in tax revenue at a time when Russian government was suffering such financial hardship that it was forced to default on USD\$40 billion in domestic debt and seek emergency loans from the International Monetary Fund.

In evidentiary terms, the Russian government's action is hinged upon materials previously created/used by U.S. authorities to mount an enforcement action against the Bank of New York, and prosecute one of its staff members.³³⁵ More specifically, it is largely based upon:

- a non-prosecution agreement entered into by the Bank of New York, in which the
 institution acknowledges certain misconduct and agreed to pay USD\$38 million to
 settle charges relating to "very serious violations" of federal AML/CTF regulations;³³⁶
- an accompanying press release published by the U.S. Department of Justice on 8 November 2005.

Both these documents are critical to the Russian government's civil litigation because they go towards establishing whether the Bank of New York ever admitted criminal liability for

Cullison, A., 'Russia Sues Bank of New York Over 1990s Scandal', *The Wall Street Journal* (New York), 18 May 2007, A.3.

Butrin, D. et al, 'The Case of the Long Gone Cash', Kommersant (Moscow), 18 May 2007 http://commersant.com/p766368/r 1/money laundering/> at 28 January 2008.

³³⁴ Ustinova, T., and Stempel, J., 'Russia Sues Bank of New York for \$22.5 Billion', Reuters, 17 May 2007 http://www.reuters.com/article/businessNews/idUSL175611720070517?pageNumber=2&sp=true at 20 September 2007. See also Medetsky, A., and Elder, M., 'Bank of New York Sued by Russian Customs for \$22Bln for Money Laundering', *The Moscow Times* (Moscow), 18 May 2007, 2.

in February 2000, former bank employee Lucy Edwards and her husband, Peter Berlin, were convicted of conspiracy and opening an unlicensed branch of a foreign bank. Whilst neither of these crimes can provide a basis for a claim under the RICO Act, it is claimed that one of the objectives of the conspiracy was to launder money in order to promote a "wire-fraud scheme" (an activity that may give rise to a cause of action under the RICO Act)

³³⁶ Gardner, H., and Levitov, M., 'Russia Sues Bank of New York for \$22.5 Billion', *Bloomberg*, 17 May 2007 < http://www.bloomberg.com/apps/news?pid=20601087&sid=aiVrh6bgUcwk&refer=home at 19 September 2007.

its involvement in money laundering activities. Such an admission of guilt is particularly important to the Russian government's case for a number of reasons. Not only is it pivotal to the government's claims that the statute of limitations clock has been reset, but it is also required to surmount the jurisdictional hurdle posed by the fact that Russian commercial courts are not supposed to become involved in the interpretation of criminal laws (whether they are local or foreign laws).³³⁷

Although the Bank of New York entered into a non-prosecution agreement to avoid being criminally prosecuted for its actions, it is contentious whether that agreement actually contains admissions of criminal wrongdoing. According to the bank, the agreement contains no more than a few acknowledgments of its incompetence. However, regardless of whether the Moscow Arbitration Court finds that the non-prosecution agreement does in fact contain admissions of intentional misconduct, fierce argument is still likely to surround the accompanying press release published in November 2005 by the U.S. Department of Justice. Although the press release explicitly states that the Bank of New York "admitted its criminal conduct", the Bank of New York claims that this statement does not refer to its acceptance of liability relating to its alleged money laundering offences. Rather, it concerns a number of fraudulent loan applications processed by one of its branches.³³⁸

In August 2008, the U.S. Attorney's offices for both the Eastern and Southern Districts of New York belatedly amended the press release that had accompanied the Bank of New York's non-prosecution agreement in 2005. The revised document clarifies that the bank never admitted criminal liability in relation to its alleged money laundering activities; it only assumed responsibility in respect of the fraudulent loan applications. Despite the amendments made to the press release however, the Russian government continues to argue that because the institution accepted "responsibility" for the matters contained in its nonprosecution agreement (i.e. a document stemming from a criminal investigation into the

³³⁷ Parloff, R., 'Bank of New York's \$22.5 Billion Headache', Fortune, 24 September 2008 http://money.cnn.com/2008/09/23/news/companies/parloff bank new york.fortune/index.htm> at 14 January 2008.

January 2008.

January 2008.

institution's activities), it unambiguously admitted criminal responsibility for its money laundering activities.

According to some business analysts, the ongoing lawsuit poses no real risk to the Bank of New York Mellon beyond minimal share price turbulence.³³⁹ Nevertheless, it remains unclear what the longer-term impacts of the case might be if the court ultimately finds in favour of the Russian government. Even if damages are awarded, it is uncertain whether any order of the Russian court could be enforced in the absence of a ruling by an international or U.S. court. The enforceability of such an order would be questionable, especially in light of the fact that Russia's legal system is generally perceived to be inexperienced with respect to complex financial cases, and "fraught with Soviet-era practices and allegations of corruption and political influence".³⁴⁰

Nevertheless, although any judgment of the Moscow Arbitration Court is unlikely to be enforceable in the U.S., the Bank of New York Mellon may still suffer reputational and financial ramifications as a result of the case. The institution currently conducts business in more than 100 countries and the judgment is likely to be enforceable in at least a few of them. Furthermore, after conducting business in Russia – a country that is currently the world's sixth-largest economy and the second-largest producer of oil – for more than 80 years, the bank would certainly suffer a degree of financial damage if it was required to cease operating there. ³⁴¹ Beyond the implications that the case may have for the Bank of New York Mellon, it may set a precedent for the international application of civil *RICO Act* provisions to money laundering activities undertaken by global financial institutions.

4.3 Civil liability and extraterritorial AML/CTF laws

As is the case with criminal liability, civil liability for AML/CTF compliance failures may be applied in extraterritorial laws and pursued across national borders. This is most apparent

³³⁹ Following the Bank of New York's alleged breaches of AML/CTF legislation, the institution and Mellon Financial Corp. agreed to merge in a USD\$16.5 billion deal that has seen the newly formed 'Bank of New York Mellon' become the world's largest custody bank and one of its largest asset managers.

³⁴⁰ Op cit n333.

³⁴¹ Op cit n337.

from U.S. AML/CTF legislation such as the *USA PATRIOT Act*, which contains a number of important extraterritorial provisions that relate to the initiation of civil actions against non-U.S. persons.

In contrast to Sections 311, 312 and 313 of the USA PATRIOT Act, which were discussed in **Chapter 3** of this thesis, Sections 317 and 319 regulate foreign financial institutions through the use of civil sanctions. Firstly, Section 317 creates a civil cause of action against "foreign persons" (including foreign financial institutions) with respect to contraventions of 18 U.S.C. § 1956 and 18 U.S.C. § 1957. It authorises U.S. courts to:

- exercise jurisdiction over a civil action instituted by the U.S. government against a
 foreign person for the purposes of enforcing a forfeiture judgment based upon a violation
 of 18 U.S.C. §1956; and
- seize any assets involved in such an action, and appoint a federal receiver to take custody
 of all assets needed to satisfy any civil judgment, forfeiture order or criminal sentence
 made under 18 U.S.C. § 1956 or 18 U.S.C. § 1957.³⁴²

Clearly, the civil cause of action enshrined in *Section 317* may provide a suitable alternative to criminal proceedings where the relevant offender is a foreign corporation, and a successful prosecution is less important³⁴³ (or perhaps far more difficult to attain) than a finding of civil liability and the imposition of a civil monetary penalty. Whilst it potentially lowers the likelihood of foreign institutions being indicted for their contraventions of U.S. AML/CTF laws, the Section may nevertheless heighten their AML/CTF legal risk in relation to incurring civil liability for their compliance failures.

In addition to Section 317, Section 319 outlines civil sanctions that may be imposed upon a foreign entity. Labelled "the most troubling aspect" of the USA PATRIOT Act,³⁴⁴ this Section embodies perhaps the most extreme application of U.S. extraterritoriality under AML/CTF legislation. Codified as 18 U.S.C. § 981(k)(1), Section 319 provides for the civil

³⁴² Op cit n237, 107.

United States Department of Justice, Field Guidance on New Authorities (Redacted) Enacted in the 2001 Anti-Terrorism Legislation (2001) < http://usacm.acm.org/usacm/DOJ_Terrorism_Law.htm at 1 November 2007.

³⁴⁴ Op cit n342.

forfeiture of funds contained in a foreign financial institution's U.S. correspondent or interbank account. It states that where funds derived from criminal activity are deposited into an account in a foreign bank, and that bank maintains a correspondent account in the U.S., the funds "shall be deemed to have been deposited into the correspondent account" in the U.S. Accordingly, it gives the U.S. government jurisdiction to seize or restrain funds in the foreign bank's U.S. correspondent account "up to the value of the funds deposited".

Section 319 was enacted to prevent foreign depositors (including money launderers and supporters of terrorism) from committing criminal offences in the U.S. and using foreign accounts to place their proceeds of crime beyond the reach of U.S. law enforcement authorities. Whilst such individuals could historically obscure the ownership and source of their funds by hiding behind a foreign bank's use of the 'innocent owner' defence, 345 Section 319 prevents foreign depositors from exploiting certain nuances of forfeiture law. Given that foreign institutions can no longer directly contest a civil forfeiture action by using the 'innocent owner' defence otherwise available to them under 18 U.S.C. § 983(d), 346 foreign depositors wanting to contest a forfeiture action in the U.S. federal courts are now required to mount an action on their own behalf.

Many of the hallmarks of Section 319 were recently challenged by a foreign financial institution in United States v. Union Bank for Savings and Investment (Jordan), 487 F.3d 8 (1st Cir. 2007). Considered to be "the first real test of Section 981(k)", 347 this case concerned two individuals in Canada who obtained approximately USD\$7 million via a telemarketing fraud scheme; more than USD\$2.8 million of which was traceable to an account held by a money exchanger at the Union Bank for Savings and Investment (Union Bank) in the West Bank of Israel. During 2002 and 2003, the U.S. government successfully mounted a civil

Cassella, S.D., Recovering the Proceeds of Crime from the Correspondent Account of a Foreign Bank (2005).6 http://works.bepress.com/cgi/viewcontent.cgi?article=1015&context=stefan_cassella at 22 May 2008.

³⁴⁶ See Section 981(k)(3) and (4). The 'innocent owner' defence can ordinarily be used by an institution to defeat a forfeiture action in circumstances where (i) it was unaware that the relevant funds were derived from unlawful activities; and (ii) upon learning of the conduct giving rise to the forfeiture, it did all that could reasonably be expected to terminate the use of such funds.

forfeiture action under *Section 981(k)* and seized USD\$2.8 million from Union Bank's U.S. correspondent account at the Bank of New York.³⁴⁸

Although any claim for the return of the funds should have been filed by the money exchanger, it was Union Bank that sought to contest the application of Section 981(k) and the forfeiture of the funds. Whilst the bank acknowledged that it may have held funds that represented the proceeds of crime, it contested the civil forfeiture of those funds on a number of constitutional and other grounds. Fundamentally, Union Bank argued that:

- the funds seized from its U.S. correspondent account were not directly traceable to the fraud proceeds allegedly deposited in the account at its West Bank operations;
- as the owner of the funds in its correspondent account, it had legal standing to contest the forfeiture by virtue of the 'innocent owner' defence; and
- the forfeiture of the funds in its correspondent account violated the Eighth Amendment of the U.S. Constitution because it represented "excessive punishment". 349

Each of Union Bank's arguments failed and it was unsuccessful in its claim to have the USD\$2.8 million in forfeited funds returned. Firstly, the court held that the U.S. government was under no obligation to trace the forfeited funds to the Canadian fraud scheme because Section 981(k) "allows for the forfeiture of funds in an interbank account without proof that the funds are directly traceable to forfeitable funds that were originally deposited with the foreign bank". Secondly, on the issue of the institution's ability to assert a claim using the 'innocent owner' defence, the court confirmed that such a defence was not available to Union Bank because only the foreign account holder (as opposed to the foreign bank) had standing to contest the forfeiture of funds seized from a correspondent account under Section 981(k). Finally, with respect to the Eighth Amendment constitutional challenge, the court held that the forfeiture could never amount to "cruel and unusual punishment" or the imposition of an

³⁴⁸ Hogan & Hartson, The Long Arm (and Tight Grip) of Deposit Forfeiture Under the USA PATRIOT Act (2007) http://www.hoganandhartson.com/files/Publication/dd5bbfdc-e2a2-466e-a9e3-f3609bb82b63/Presentation/PublicationAttachment/b608bc68-2e17-4fd8-ab7b-ffab2baca6ca/FinSvcRegUpdate.pdf at 22 May 2008.

³⁴⁹ Op cit n345, 12-15.

See United States v. Funds on Deposit in Account No. 890-0057173 maintained at the Bank of New York by the Union Bank for Savings and Investments Jordan, No. 02-472-B, (D.N.H. Jan. 6, 2005).

"excessive fine" because forfeiture merely restores the status quo ante and therefore can never be punitive or construed as a punishment in a strict constitutional sense.

Evidently, the Union Bank case illustrates the potential civil law ramifications and AML/CTF legal risk that an institution may face under Section 319 of the USA PATRIOT Act. That Section effectively "exports the risk of forfeiture" to foreign financial institutions and gives the U.S. government considerable leverage over their activities. It places them in a particularly vulnerable legal position and leaves them open to incurring strict liability for the criminal acts of their customers. Even where a foreign financial institution has implemented an effective AML/CTF program and a host of other internal controls, it may still face the risk of accepting tainted funds and having those funds seized via a virtually incontestable civil forfeiture order granted by the U.S. courts. Thus, such an institution may always have a degree of exposure to the civil law consequences and extraterritorial reach of Section 319.

4.4 When you can't even trust your own bank – financial institutions and constructive trusts

The primary aim of risk-based AML/CTF legislation is to thwart opportunities for money laundering and terrorism financing by ensuring that institutions implement appropriate AML/CTF controls tailored to their ML/TF risk. Although such legislation has typically been concerned with identifying, reporting and confiscating the proceeds of crime, rather than recompensing the victims of crime, identifiable victims of fraud and money laundering may nevertheless seek to recover their losses in certain jurisdictions. In countries such as the U.K., individuals may file a civil claim against an institution involved in the laundering of their funds. The such as the laundering of their funds. Pursuing such a claim is likely to be particularly

³⁵¹ Op cit n342, 108.

Whilst a large proportion of laundered funds will not have been derived from readily identifiable victims (this may be the case if the suspect funds are the product of drug trafficking, for instance), funds derived from crimes such as fraud, false accounting and forgery, may lend themselves to the identification of obvious victims who have suffered financial loss.

Wessing, T., Money Laundering: Changes to the UK's Money Laundering Regime (2005) http://www.taylorwessing.com/website/generator/taylorwessing/content/publications/items/UK/MondeyLaundering_TWUK_english.de,property=file.pdf at 20 October 2006.

attractive where a victim of fraud/money laundering is seeking a 'deep pocket' from which to recover their lost funds, and the wrongdoer cannot be located or is unable to recompense them.³⁵⁴

Legally recognised in jurisdictions such as Australia and the U.K., a trust is a relationship in respect of property "under which one person, known as a trustee, is obliged to deal with the property vested in him or her for the benefit of another person, known as a beneficiary". 355 Whilst there tends to be "no clear and all-embracing definition" of a constructive trust, such a trust will arise by operation of law where an individual or institution that has not been appointed as a trustee, nevertheless invokes the liabilities of trusteeship by conducting themselves as trustees in relation to certain property. As opposed to other types of civil actions that might be brought against an institution in relation to money laundering activities, constructive trust claims will generally concern customers who are the perpetrators – rather than the victims – of crime. 357

As constructive trusts arise subsequent to a breach of trust or fiduciary duty (often due to fraud),³⁵⁸ they are not particularly relevant in the context of terrorism financing. As previously discussed, the funds involved in such activity may be 'clean' before they are received by, and even after they are processed by, a financial institution. However, despite the inapplicability of constructive trust principles to funds that are 'clean' and legitimate, a number of constructive trust cases concerning fraud and money laundering have arisen in the U.K. in recent years. Whilst there are no civil causes of action in the U.K. that directly equate to the criminal offences of theft and/or the handling of stolen property, it is well

Law Society of England and Wales, Guide Online

http://www.lawsociety.org.uk/professional/conduct/guideonline/view=page.law?POLICYID=225074 at 12 November 2006.

Tagoe, L., 'An Analysis of Banks' Liability for the Deposits of Proceeds of Criminal Activities in the U.K.' (2003) 4(4) Journal of International Banking Regulation 352, 354.

See the comments of Edmund-Davies LJ in Carl Zeiss Stiftung v Herbert Smith & Co [1969] 2 Ch 276, at pp. 300.

357 Brindle M 'The Liabilities of Financial Intermediation and the Country of the Country

Brindle, M., 'The Liabilities of Financial Intermediaries and their Advisers for Handling the Proceeds of Crime' (2002) 9(3) *Journal of Financial Crime* 227.

Binnington, A., Constructive Trusts And All Crimes Money Laundering Legislation: Is There a Problem? (1998) Jersey Legal Information Board

http://www.jerseylegalinfo.je/publications/jerseylawreview/Oct98/constructive_trusts.aspx at 10 October 2006.

settled that a banker or financial institution may be held liable as a constructive trustee in respect of their dealings with the proceeds of crime paid into an account.³⁵⁹

Due to the existence of supporting U.K. case law, and the fact that the AML/CTF experience in the U.K. has often been cited in debates about how AML/CTF issues should and will be addressed in other jurisdictions (such as Australia), the analysis of constructive trusts contained in this Chapter primarily focuses on U.K. legal authorities.

4.4.1 The twin branches of constructive trust liability

As articulated in U.K. authorities such as *Barnes v. Addy* (1874) L R 9 Ch App 244, liability as a constructive trustee may arise in circumstances where there has been:

- "knowing assistance" (i.e. evidence of a person knowingly assisting in a fraudulent and dishonest design on the part of a trustee); or
- "knowing receipt" (i.e. evidence of a person receiving and becoming chargeable with trust property). 360

The specific elements required to succeed with a claim under each of these heads of liability, are outlined on the following page in **Table 2**.

³⁵⁹ Cases such as *Foley v. Hill* [1848] 2 HL Cas 28 established early on that a banker who is not expressly declared as a trustee may nevertheless be treated as a constructive trustee on account of their dealing(s) with trust affairs.

³⁶⁰ Whilst a constructive trust can also arise in circumstances where there have been inconsistent dealings with trust funds, only cases of 'knowing assistance' and 'knowing receipt' are relevant with respect to instances of money laundering.

Table 2 - Elements of 'knowing assistance' and 'knowing receipt' claims

Knowing Assistance	vs. Knowing Receipt
(i) Existence of a trust or other fiduciary relationship	(i) Existence of a trust or other fiduciary relationship
(ii) The trust or fiduciary duty was breached by someone other than the Respondent	(ii) The Plaintiff's assets were disposed of in breach of the relevant trust or fiduciary duty
(iii) The Respondent assisted in the relevant breach of trust/fiduciary duty and in doing so, acted dishonestly	(iii) The Respondent beneficially received (and became chargeable with) assets traceable as those of the claimant
(iv) The Respondent's actions resulted in loss for the claimant.	(iv) The Respondent had knowledge ³⁶¹ that the assets they received were traceable to a breach of fiduciary duty which made it unconscionable to retain them.
Example - See the statements of Hoffman L.J. in <i>El Ajou v Dollar Land Holdings plc</i> [1994] 2 All ER 685	Example- See the statements of Lord Selborne in Barnes v Addy (1874) L R 9 Ch App 244

4.4.2 Knowing assistance

As outlined in *Royal Brunei Airlines v. Tan* [1995] 2 AC 378 (PC), liability for 'knowing assistance' will arise where a primary wrongdoer acts in breach of a trust or fiduciary duty, and another – acting dishonestly – assists them to do this. Accordingly, an institution can incur liability as a constructive trustee where it receives certain trust funds and, despite having information that they may be derived from breach of a trust or fiduciary duty, subsequently pays the funds away at another's request. For instance, if an institution knowingly facilitates a transaction on behalf of a customer using funds that the customer attained by defrauding their employer, the employer can launch a civil action for 'knowing assistance' against the institution. Indeed, it will be open to them to argue that the institution should be held liable as a constructive trustee because it knowingly assisted a breach of fiduciary duty by paying away the funds in the manner directed by the fraudulent employee/customer.

³⁶¹ For the purpose of this test, the concept of 'knowledge' extends beyond actual knowledge to include (a) 'Nelsonian knowledge', which involves the deliberate shutting of the eyes to what would otherwise be obvious, and (b) knowledge in circumstances where an honest and reasonable man would have been suspicious.

Dishonesty is the touchstone of liability in 'knowing assistance' cases. As stated by Lord Selborne in *Barnes v. Addy* (1874) L R 9 Ch App 244, an institution will only be held liable for 'knowing assistance' where it has assisted "with knowledge in a dishonest and fraudulent design on the part of the [relevant] trustees". With respect to constructive trust cases, U.K. case law suggests that the necessary standard of knowledge is particularly broad and may be satisfied by the following:

- actual knowledge;
- wilfully shutting one's eyes to the obvious;
- wilfully and recklessly failing to make such inquiries as an honest and reasonable man would make;
- knowledge of circumstances that would indicate the facts to an honest and reasonable man; or
- knowledge of circumstances that would put an honest and reasonable man on inquiry.³⁶³

With respect to the aforementioned categories of knowledge, Australian case law has demonstrated that not all five categories will be sufficient for the purposes of substantiating the requisite 'knowledge' requirements needed to succeed with a 'knowing assistance' claim in Australia. Whilst the High Court of Australia held in *Farah Constructions v. Say-Dee Pty Ltd* [2007] 230 CLR 89 that the first four categories of cognisance would meet the relevant knowledge requirement, it stated that the fifth category (i.e. knowledge of circumstances that would put an honest and reasonable man on inquiry) would not suffice under Australian law. Thus, whilst the knowledge requirements for 'knowing assistance' claims are substantially similar in the U.K. and Australia, institutions operating in the U.K. may face a slightly higher level of legal risk than their Australian counterparts because their acceptable standard of knowledge is broader than that allowed for in Australia.

Given that knowledge is pivotal to the success of any 'knowing assistance' claim, an institution facing such a claim could attempt to minimise its risk by disputing claims that it

³⁶² Op cit n355, 375.

³⁶³ See the comments of Gibson J in Baden v. Societe Generale [1993] 1 WLR 509, at 575-576.

had the necessary standard of knowledge to attract liability as a constructive trustee. Even if it clearly paid away funds related to a breach of trust or fiduciary duty, an institution could still avoid liability by establishing that it only had vague suspicions (rather than actual or constructive knowledge) regarding the source of the funds. As enunciated in *The Bank v. A Ltd* [2000] All ER 864, institutions cannot be held liable as a constructive trustee "merely because they entertain suspicions as to the provenance of money deposited with them". 364

Additionally, an institution facing a 'knowing assistance' claim may try to limit its legal exposure by contending that in light of *subjective* considerations (such as its previous experience with the customer involved) its conduct was not *objectively* dishonest by the ordinary standards of honest and reasonable people. However, substantiating this claim may prove particularly difficult for some institutions, given that the increased global attention paid to AML/CTF issues during the past decade has ushered in an expectation of tighter KYC controls and customer/account screening. In the aftermath of September 11, the enactment of extensive risk-based AML/CTF legislation and the imposition of various AML/CTF obligations upon institutions means that "honest and reasonable" bankers are now arguably expected to act with a far greater level of diligence than ever before.

4.4.3 Knowing receipt

In comparison to 'knowing assistance', the cause of action for 'knowing receipt' is restitutionary and only available where a Respondent has received or applied funds in breach of a trust or fiduciary duty for their own use and benefit. The most significant and perhaps the most strictly applied requirement of 'knowing receipt' cases is the beneficial receipt of tainted funds. An institution that receives funds into a customer's account will not generally be treated as the recipient of those funds. This is fundamentally because it will be

International Ltd [2006] 1 All ER 333.

This statement accords with the finding in *The Governor and Company of the Bank of Scotland v. A Limited* [2000] All ER 864 that a bank's suspicions about its customer were not sufficient to give rise to constructive trust liability – even though a report to the relevant investigatory agency was made.

365 See the test for dishonesty outlined by the U.K. Privy Council in *Barlow Clowes v. Eurotrust*

³⁶⁶ It is important to note that in cases of knowing receipt, a bank will only be liable for the amount that it has received. This contrasts with cases of knowing assistance, where an institution is potentially liable for the whole of the amount lost as a result of a fraud or other illicit activity.

³⁶⁷ Op cit n357, 230.

receiving those funds as an agent of its customer, and bound to account to its customer for any interest earned on them.

Importantly however, there are still circumstances where an institution will be deemed to have beneficially received customer funds. Under U.K. case law, an institution that receives funds into a customer's account and subsequently uses them to discharge/reduce the customer's overdraft or mortgage, will be deemed to have received those funds beneficially. As such, where an institution receives funds in this way, it may be held liable for 'knowing receipt' if it applied the funds for its own benefit and did so knowing that they were being misapplied in breach of a trust or fiduciary duty. ³⁶⁹

Given the limited circumstances in which an entity will be deemed to have received funds for their own use and benefit, an institution's AML/CTF legal risk is far greater with respect to 'knowing assistance' claims than 'knowing receipt' claims. This is clear when considering that 'knowing assistance' claims involve both the receipt and paying away of funds; a type of transactional behaviour that is integral to the placement and layering stages of money laundering. Nevertheless, a 'knowing receipt' claim may still be successfully waged against an institution in circumstances where it received tainted funds and, knowing that they were paid in breach of a trust or fiduciary duty, applied them for its own benefit.³⁷⁰

Although 'knowing receipt' claims do not require evidence of dishonesty, proof of knowledge is pivotal to their success.³⁷¹ Thus, as with 'knowing assistance' cases, an institution may seek to limit its AML/CTF legal risk and deflect its culpability in a 'knowing receipt' case by arguing that it did not have the necessary degree of knowledge to attract liability as a constructive trustee. However, given that an institution does not need to have actual knowledge of the fact that the funds they beneficially received were traceable to a breach of fiduciary duty, substantiating such a claim could be problematic. In the context of

Herbert-Smith, *The Effect of the Risk Based Approach on Civil Liability* (2006) <http://www.herbertsmith.com/NR/rdonlyres/F9AC5EB7-8A64-43C2-AA40-650B320155F4/2275/TheeffectofriskbasedapproachJune2806.html at 2 November 2006.

See Polly Peck International v. Nadir [1992] 4 All ER 769.

³⁷⁰ See *Houghton v. Fayers* [2000] 1 BCLC 511 at 516.

³⁷¹ See Re Montagu's Settlement Trusts [1987] Ch 264.

'knowing receipt' claims for instance, an institution may be "disentitled to rely on lack of actual knowledge" and affixed with constructive knowledge where it has failed to collect and verify additional KYC information in circumstances where it could have been expected to do so. 373

4.5 The potential tension between an institution's AML/CTF obligations at criminal and civil law

The extent of an institution's potential liability under constructive trust principles is not solely determined by its exposure to 'knowing assistance' and 'knowing receipt' claims. Indeed, its AML/CTF legal risk in relation to such principles may be heightened in circumstances where there is an apparent tension between its:

- obligations to third parties under equitable constructive trust principles;
- contractual requirements to follow customers' instructions;
- statutory obligations in relation to 'tipping off'; and
- statutory requirements to report suspicious transactions and/or activities.

In jurisdictions such as the U.K., the interplay between the abovementioned obligations has occasionally created significant challenges for institutions trying to achieve AML/CTF compliance and balance their competing responsibilities. In recent years, a number of U.K. authorities have dealt with the apparent tension between institutions' various AML/CTF obligations and exposures. Whilst some commentators have held that these cases have provided guidance that is unclear and unsatisfactory at best, this Chapter draws on such authorities in order to highlight the way in which institutions may face heightened AML/CTF legal risk as a result of their competing obligations. Further, it seeks to analyse the steps that institutions should take in order to best meet their compliance obligations and minimise their potential liability.

³⁷² See statements of Buckley LJ in *Belmont Finance Corporation Ltd v. Williams Furniture Ltd* [1979] Ch 250, at 267.

³⁷³ Op cit n355, 360.

4.5.1 Institutions' various contractual and legislative obligations

Contractual obligations to customers

As financial institutions typically hold money for their customers on the basis of a contractual banker/customer relationship, ³⁷⁴ they are generally bound to follow their customers' instructions within the boundaries of the law. Accordingly, any institution that deals with a customer's funds in a manner inconsistent with an express or implied term of their contract with that customer, may face a civil lawsuit for breach of contract.

Civil liability might not only attach to an institution where it has failed to honour a customer's instructions, but also where it has blindly complied with such instructions. To demonstrate, if a bank held an account on behalf of a company and that account authorised each company director to sign cheques/give payment instructions in relation to the account, the bank could be held liable for breaching its contract with the company if it enabled one of the directors to fraudulently misapply funds from the account. In accordance with the decision in Lipkin Gorman v. Karpnale [1989] 4 All ER 409, the company could argue that under an implied term of its contract, the bank was prevented from honouring payment or transactional instructions from a director in circumstances where an honest and reasonable person would have considered there to be a serious or real possibility that the director was acting fraudulently. In order to successfully establish a breach of contract, the company would not need to prove any fraud or dishonesty on the part of the bank. It would simply need to demonstrate that the institution was negligent in carrying out financial activities on its behalf.375

If the aforementioned scenario were to materialise, the bank could be held liable to account for the funds misapplied by the fraudulent director, and ordered to pay damages to the company. Evidently, this would be a highly undesirable outcome for an institution given its potential reputational impacts, and the fact that the misappropriation of funds might have been prevented through the use of enhanced due diligence and transaction monitoring. By properly identifying the nature of company's business and understanding what constituted

³⁷⁴ Op cit n357, 227. ³⁷⁵ lbid.

'normal' transactional behaviour on its account(s), the institution could possibly have identified that the director's payment instructions were atypical for the company.

Statutory obligations to report suspicious activities and freeze accounts

Financial institutions may become suspicious of certain customers or accounts for a number of reasons. They may doubt the legitimacy of a customer's alleged identity, the validity of their transactions, and/or the legality of their activities. The reporting of such suspicions generally plays an integral role in most AML/CTF regimes. Given its ability to provide crucial intelligence on financial dealings related to criminal conduct, such reporting can provide regulatory and law enforcement authorities with the lynchpin they need to not only trigger an investigation into money laundering, but also the predicate offences underlying it. Accordingly, in many jurisdictions the threshold for suspicious activity reporting is generally quite low for institutions – covering both *objective* money laundering/terrorism financing 'red flags', and *subjective* suspicions held by employees and AML/CTF staff.

It should be noted however that the requisite legislative standard for reporting may vary amongst jurisdictions, with some AML/CTF regimes requiring only objective or subjective suspicions to be reported. Often, the distinction between an institution's obligation to report objective or subjective suspicions may be solely attributable to the legislative drafting of a few select words. For instance, whilst institutions operating in the U.K. are required to report those instances where they have "reasonable grounds to know or suspect" money laundering, institutions operating in Australia are required by Section 41 of the AML/CTF Act 2006 (Cth) to report those instances where they "suspect [money laundering] on reasonable grounds". Whilst their drafting is similar, the reporting obligations under U.K. and Australian AML/CTF laws are in fact very different. Whilst institutions operating in Australia are required to report subjective assessments of suspicion, institutions operating in the U.K. have a broader reporting requirement as they are bound to report objective

assessments of suspicion (i.e. those circumstances where they ought to have had reasonable cause to suspect, or where an objective test of suspicion arises).³⁷⁶

Whether based upon objective or subjective suspicions, it is clear that suspicious activity reporting requirements typically carry a higher degree of AML/CTF legal risk than many other AML/CTF obligations. Due to its ability to deter illegal behaviour, and support the identification, investigation and prosecution of criminal activities, 377 suspicious activity reporting has generally been one of the most strictly enforced aspects of risk-based AML/CTF regimes. In a significant number of jurisdictions, failure to report a suspicion of money laundering or terrorism financing is regarded as a standalone criminal offence, capable of attracting hefty penalties. In recent years, many of the largest, formal enforcement actions have involved breaches of suspicious activity reporting regulations.

In certain jurisdictions, municipal AML/CTF legislation requires institutions to freeze a suspect account and/or block the provision of further banking services to a suspect customer immediately upon filing a SAR with the relevant Financial Intelligence Unit (FIU). For instance, in Switzerland, local AML/CTF laws compel institutions to freeze (for a minimum of five days) funds suspected of being connected with money laundering or a predicate offence.³⁷⁸ Whilst these freezing requirements may sound drastic when compared to the approaches taken in other countries, institutions operating in Switzerland do not generally report their suspicions or file a report until they have conducted an extensive internal investigation into the suspect customer/funds/transactional behaviour.³⁷⁹

Evidently, Swiss legislative obligations in relation to the reporting of suspicious activity and the freezing of suspect funds are vastly different to those enacted in the majority of AML/CTF regimes. The reporting requirements enshrined in the country's AML/CTF laws

³⁷⁷ Romaniuk, P., Haber, J., and Murray, G., 'Suspicious Activity Reporting: Regulatory Change and the Role of Accountants' (2007) *The CPA Journal* 70.

Bosworth-Davies, R., How Do I Know When I am Suspicious? (2004) SAS http://www.sas.com/news/feature/fsi/dec04aml.html at 1 June 2008.

³⁷⁸ Financial Action Task Force, Third Mutual Evaluation Report on Anti-Money Laundering and Combating the Financing of Terrorism – Summary: Switzerland (2005) 4 http://www.fatf-gafi.org/dataoecd/60/30/35529139.pdf> at 19 November 2007.

are so narrowly drafted that institutions only report 'actionable intelligence', i.e. those customers/transactions that warrant further investigation by regulatory and law enforcement authorities. This is in contrast to the position in most other jurisdictions, where institutions are simply required to file a report upon the initial formation of a suspicion, and the relevant FIU must necessarily sift through masses of reports in order to identify a handful requiring further investigation. Under the majority of AML/CTF regimes, an institution will not be automatically required to freeze fund or suspend the provision of financial services upon reporting a suspicion. In fact, in many countries (including the U.K., the U.S. and Australia), freezing a suspect account immediately upon the submission of a report is likely to inflame an institution's AML/CTF legal risk by giving rise to a 'tipping off' offence.

Statutory obligations in relation to 'tipping off'

In many AML/CTF regimes, including those in Australia, Singapore, the U.K. and the Cayman Islands, suspicious activity reporting requirements are accompanied by legislative provisions criminalising the act of 'tipping off'. Whilst its legal construction often differs slightly between jurisdictions, tipping off will generally occur where a person who knows or suspects that a suspicion has been reported, makes a disclosure that might give the relevant suspect customer(s) an opportunity to take evasive action and/or destroy evidence relating to their criminal activities. 380 In countries such as Australia, the offence of tipping off is broadly drafted to involve the communication of information that "could reasonably be expected to infer" that a suspicion had been reported to AUSTRAC.³⁸¹ Under U.K. AML/CTF legislation however, the offence has been constructed more narrowly to include the communication of information that may prejudice any subsequent money laundering/terrorism financing investigation and/or criminal prosecution.

Statutory tipping off provisions generally give regulatory and law enforcement authorities significant control over how money laundering and terrorism financing cases are handled.

See Section 123(2) of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth).

³⁸⁰ HM Treasury, The UK's Anti-Money Laundering Legislation and the Data Protection Act 1998: Guidance Notes for the Financial Sector (2002) 3 http://www.hm- treasury.gov.uk/mediastore/otherfiles/money_laundering.pdf> at 22 November 2007.

381 See Section 122(2) of the distriction of the section (2002) of the distriction of the distriction of the section (2002) of the distriction of the districti

They provide such authorities with a formal avenue of redress in respect of those who have committed a tipping off offence through direct, verbal communication, as well as those who have inadvertently alerted a customer to their suspicions via unspoken acts and omissions. Accordingly, the offence of tipping off enables formal enforcement proceedings to be launched against any institution/individual whose immediate closure of an account or unexplained refusal to process certain transactions alerts a customer to the fact that they have aroused suspicion.

The AML/CTF legal risk represented by legislative tipping off provisions is arguably greater with respect to an institution's existing (as opposed to new or prospective) customers. To illustrate, if a prospective customer behaves in a way that gives rise to suspicion, an institution may simply refuse to "on-board" them – perhaps with an explanation that they failed to meet internal customer acceptance standards. However, in circumstances where an existing customer arouses suspicion, it may be far more difficult for an institution to conceal their suspicion. Apart from the close ties they may have established with their Relationship Manager and other internal bank staff, existing and long-standing customers are likely to be acutely aware of the time frames within which they usually have certain transactions processed. Thus, any deviation from their institution's typical processing patterns and/or any sudden unavailability of their funds, may effectively tip them off as to the existence of the institution's suspicion.

In addition to the nature and length of its relationship with a suspect customer, an institution's risk of committing a tipping off offence will also be linked to the jurisdictions in which it operates. For instance, given that institutions operating in Switzerland are required to freeze any funds that the subject of a reported suspicion, their risk of committing a tipping off is significantly reduced. Due to the construction of Swiss AML/CTF laws, such institutions cannot be held liable for tipping off a customer simply because they have frozen that customer's funds in accordance with their other statutory obligations. The legislation essentially removes some of the discretion around tipping off and the freezing of accounts that occasionally sees entities in other jurisdictions facing formal enforcement actions.

4.5.2 Competing contractual and legislative obligations

In accordance with FATF Recommendation 14, national governments are encouraged to enact laws that protect financial institutions from incurring criminal or civil liability as a result of breaching any legislative or contractual restriction on the disclosure of information, in the course of reporting a suspicion in good faith. In conducting their Mutual Evaluation reviews, organisations such as the FATF and the APGML have previously criticised a number of countries for failing to implement measures protecting institutions from incurring liability as a consequence of their AML/CTF compliance and proper reporting of suspicious activities.³⁸²

Certain countries have long recognised the importance of enabling financial institutions to file reports with their FIU free of the fear of reprisals. In the U.S. for instance, Congress enacted the Annunzio-Wylie Anti-Money Laundering Act of 1992 (12 U.S.C. §§ 1786, 1821) to amend the Bank Secrecy Act. That Act not only compels institutions to report all suspicious transactions, but also protects them from facing civil liability from private plaintiffs (including disgruntled customers) as a result of doing so. As stated in Jose Daniel Ruiz Coronado v. Bank Atlantic Bancorp Inc., 222 F.3d 1315 (11th Cir. 2000), U.S.C. § 5318(g)(3) enshrines 'safe harbour' provisions that provide "an affirmative defense to claims against a financial institution for disclosing an individual's financial records or account-related activity". They effectively give institutions immunity in relation to three different types of disclosures:

- a disclosure of any possible violation of law or regulation;
- a disclosure pursuant to δ 5318(g) itself; or
- a disclosure pursuant to any other authority.

However, even in countries that have given financial institutions a level of immunity and have tried, as far as possible, to align their various legislative requirements, the AML/CTF-related obligations placed upon institutions have occasionally appeared to be at slight odds

For instance, see Asia-Pacific Group on Money Laundering, Summaries of Mutual Evaluation Reports Adopted in 2002 - 2003 (2003) 9

http://www.apgml.org/documents/docs/8/Summary%20ME%20Reports%202002-03.pdf at 28 January 2008.

with one another. In recent years, this has been particularly apparent in the U.K., where institutions have occasionally identified a misalignment, and sought judicial guidance to balance (or at least prioritise), their obligations under AML/CTF legislation, contract law, and constructive trust principles.

In countries with strong tipping off provisions, an institution that reports a suspicion will often be instructed to continue conducting business as usual with the relevant suspect customer.³⁸³ This course of action is often desirable for law enforcement officials as it enables them to continue monitoring the customer's activities and potentially identify other parties/criminal activities they are connected to.³⁸⁴ Simply closing or suspending a suspect customer's accounts may tip them off and prompt them to alter their transactional behaviour, thereby destroying any future opportunities for law enforcement to monitor their activities.

By following the instructions of regulatory and/or law enforcement authorities in relation to a suspect customer/account, an institution will typically avoid criminal liability in relation to any consequent tipping off offence or facilitation of money laundering/terrorism financing activities. However, in some jurisdictions, an institution that follows the directions of law enforcement may still be exposed to civil liability in the form of:

- a contractual claim initiated by a suspect customer, alleging a breach of mandate (i.e. in relation to the institution's freezing of their funds or its refusal to conduct business on their behalf); and/or
- an equitable constructive trust claim (most typically, 'knowing assistance' claims) initiated by a related third party.

As illustrated on the following page in **Table 3**, an obvious tension may exist between an institution's legislative obligations, contractual obligations to customers, and constructive trust obligations to third parties. Following the reporting of a suspicion, an institution may – unless operating in a country such as Switzerland, where there are legislatively prescribed outcomes – need to choose from a number of different courses of action. Each with their own

³⁸³ Op cit n305.

Gallo, P.A., *The Writing on the Bank of Scotland's Wall* (2002) Pacific Risk Ltd 6 http://www.asiamaze.com/asiamaze%20-%20BoS%20ABC%20Case.pdf at 20 November 2007.

potential benefits and drawbacks, in certain circumstances these courses of action may protect an institution under one branch of the law, only to leave it exposed to liability under another.

Table 3 - Courses of action available to an institution that has reported a suspicion

Course of Action	Positive Results	Negative Results
Report the suspicion and, in accordance with the instructions of law enforcement/regulatory officials, continue to conduct transactions on behalf of the suspect customer	 Minimal risk of committing a tipping off offence as the customer's transactions are processed as usual Likely avoidance of criminal liability in relation to any consequent facilitation of ML/TF activities Protection from any 'breach of contract' claim waged by the suspect customer. 	 Exposure to equitable constructive trust claims initiated by wronged third parties Filed report may constitute prima facie evidence that the institution had reasonable grounds to suspect that it was handling the relevant funds as a constructive trustee.³⁸⁵
Report the suspicion and, in the absence of regulatory instructions, seek court Directions	 Limited exposure to criminal liability as a result of its subsequent dealings with the relevant funds Greater ability to substantiate in any subsequent enforcement action, that it took all reasonable steps in the circumstances. 	 Seeking formal Directions may prove to be expensive If Directions cannot be sought and provided immediately, the institution's legal position will remain uncertain Avoidance of tipping off may be difficult where Directions are still being sought but the suspect customer wants their funds paid immediately into another account or geared towards another transaction.
Report the suspicion and, in the absence of regulatory instructions, freeze the suspect customer's funds	Protection from equitable constructive trust claims initiated by wronged third parties.	 Probable commission of a criminal tipping off offence in many jurisdictions Exposure to a civil, contractual claim waged by the suspect customer, alleging a breach of mandate.
Report the suspicion and, in the absence of regulatory instructions, continue to conduct transactions on behalf of the suspect customer	 Minimal risk of committing a tipping off offence as the customer's transactions are processed as usual Protection from any 'breach of contract' claim waged by 	 Exposure to criminal liability in relation to the active facilitation of ML/TF activities Exposure to equitable constructive trust claims initiated by wronged third

³⁸⁵ If a constructive trust claim was launched against an institution, any related Suspicious Activity Report filed by that institution would likely be listed for production in an 'Anton Piller' Order.

Course of Action	Positive Results	Negative Results
	the suspect customer.	parties • Filed report may constitute prima facie evidence that the institution had reasonable grounds to suspect that it was handling the relevant funds as a constructive trustee.

To understand the operational implications of the possible misalignment between an institution's obligations, it is useful to consider the position of a financial institution that receives funds into an account in suspicious circumstances, and is instructed by the relevant account owner (customer) to immediately pay them on to a third party. After properly reporting its suspicions, the institution may be instructed by regulatory or law enforcement officials to avoid tipping off the customer by proceeding with the requested transaction. By following those instructions and paying away the funds in the manner directed by the customer, the institution may avoid criminal liability for a reporting failure, tipping off offence and/or a substantive money laundering offence. However, if it were subsequently revealed that the suspect funds were in fact the proceeds of a fraud perpetrated by their customer, the institution may nevertheless face liability in any constructive trust proceedings launched by the defrauded parties. Such parties may attempt to use the institution's initial transaction report as prima facie evidence that it:

- knew or suspected that it was dealing with the proceeds of crime; and
- had the necessary knowledge to be held liable as a constructive trustee in respect of those funds.

4.5.3 Resolving competing obligations

In recent years, the U.K. courts have been asked to clarify the AML/CTF obligations placed upon institutions and provide guidance on the most appropriate course of action should an institution find itself in a precarious legal position with respect to a suspect customer or transaction. The resulting legal authorities, a number of which are discussed on the following pages, have attempted to address institutions' obligations in a way that does

³⁸⁶ Op cit n368.

not require them to compromise compliance with one branch of the law, in order to diminish their AML/CTF legal risk and liability under another.

The Bank of Scotland case

One of the most significant U.K. authorities to address institutions' competing obligations, is *Bank of Scotland v. A Ltd & Ors* [2001] 3 All ER 58. This case concerned *Sections 93A* to *D* of the *Criminal Justice Act 1988* (U.K.)³⁸⁷ and involved a company – identified only as 'A Ltd' – that opened an account with the Bank of Scotland in September 1999. Shortly after the company became a customer of the bank, its transactional activity aroused suspicion.³⁸⁸ Upon properly reporting its suspicions under U.K. AML/CTF legislation, the Bank of Scotland learned that A Ltd was being investigated for an alleged fraud.³⁸⁹ This placed the institution in an invidious legal position as it required it to swiftly determine whether to:

- enable A Ltd to access the suspect funds in its account and, in doing so, perhaps incur liability as a constructive trustee in respect of any subsequently identified third parties; or
- prevent A Ltd from accessing the suspect funds in its account and, in doing so, perhaps face-
 - (i) a civil action initiated by A Ltd for breach of its contractual mandate;³⁹⁰ and/or
 - (ii) criminal prosecution in relation to the commission of a tipping off offence.³⁹¹

In an attempt to resolve its precarious legal position, the Bank of Scotland sought formal Directions from a Judge in chambers. At the same time however, two victims of A Ltd's alleged fraud (an individual identified as 'B' and a company identified as 'C Ltd') came forward. In an apparent attempt to protect the bank from engaging in money laundering activities, committing a tipping off offence or facing a constructive trust claim, the Judge granted an injunction freezing A Ltd's accounts, and made an Order directing that A Ltd, B

These provisions concerned the offences of money laundering and tipping off.

Carey Olsen, Latest Developments in Anti-Money Laundering Provisions (2006) 2 http://www.careyolsen.com/downloads/co100453.pdf at 13 December 2007.

³⁸⁹ Op cit n384, 3.

³⁹⁰ Op cit n388.

³⁹¹ Op cit n384, 4.

and C Ltd not be informed of, or shown any evidence substantiating, the injunction's existence.

The effect of this was that when A Ltd subsequently brought an action against the Bank of Scotland to have its funds released, the bank – constrained by the previous court Order – was forced to make private submissions to a Judge sitting in the Court of Appeal.³⁹² Rather than clearing up the Bank of Scotland's unenvious legal predicament, the Judge declared that he would order the release of A Ltd's funds unless the bank lodged an application objecting to this course of action. This significantly heightened the Bank of Scotland's legal risk as it left the institution exposed to potentially competing court Orders, and essentially put A Ltd on notice that it was the subject of a continuing investigation. Arguably, it placed the institution in a more delicate legal position than it would have been had it simply elected to risk incurring liability in relation to either a breach of a constructive trust or a tipping off offence.

Despite learning of the previous Order's existence and acknowledging the inability of law enforcement and prosecutorial authorities to disclose confidential information, the U.K. Court of Appeal ordered the Bank of Scotland to release A Ltd's funds and pay all relevant legal costs. In setting a precedent deemed by some commentators to be "worrying and unsatisfactory", 393 the court held that its judicial power to grant interim advisory declarations could not be regarded as a substitute for financial institutions making decisions within their own realms of commercial responsibility (for instance, deciding whether to contest proceedings brought by a customer for breach of mandate). 394

The Court of Appeal noted that whilst a Judge could grant interim declaratory relief in similar cases to protect a bank from criminal proceedings, such relief would not automatically protect the institution from civil actions waged by disgruntled customers or third parties. Thus, any relief granted by a court could only be partial in its application. It would protect an institution from the possible imposition of criminal fines and other

³⁹² Op cit n384, 5.
³⁹³ Op cit n384, 3.
³⁹⁴ Op cit n388, 3.

penalties, but leave it exposed to civil monetary penalties and compensatory judgments made in favour of suspect customers and related third parties. Despite its resulting level of AML/CTF legal risk however, the Bank of Scotland managed to emerge relatively unscathed after its court hearing. British authorities never criminally prosecuted A Ltd, and neither B nor C Ltd ever initiated a constructive trust against the institution. Had any of these events arisen, the legal ramifications for the bank may have been considerably worse.

Authorities after the Bank of Scotland case

Whilst the Bank of Scotland case concerned an institution's application for Directions on how to handle suspect funds, a subsequent authority known as *Amalgamated Metal Trading Limited v. City of London Police Financial Investigation Unit & Others* [2003] 1 WLR 2711 (**Amalgamated Metal Trading case**) concerned an institution's application for a Declaration that suspect funds were not the proceeds of crime. In this case, the court held that in order to make such a Declaration (and protect an institution from incurring liability in relation to its dealings with certain suspect funds) it required positive evidence that the funds were derived from legitimate sources.

Understandably, this ruling has been relatively unhelpful to most institutions. Given that the required evidentiary standard is relatively difficult to meet (if it were not, it is uncertain why any institution would make such an application at all), seeking a Declaration may prove to be both time consuming and resource-intensive for an institution. In accordance with obiter dicta in the Bank of Scotland case, any institution operating in the U.K. must take a commercial view regarding whether or not to apply for such a Declaration in the first place.

Following on from the Amalgamated Metal Trading case, the next major U.K. authority to address institutions' various AML/CTF-related obligations was *Hosni Tayeb v. HSBC Bank plc* [2004] EWCH 1529. In this case, Mr Tayeb opened an account with HSBC to receive the proceeds of a sale transaction. After these funds were subsequently transferred to his account electronically via the Clearing House Automated Payment System (**CHAPS**), a bank employee became suspicious of the transaction and decided to freeze Mr Tayeb's account

without notice and return the funds to the transferor's account. Mr Tayeb decided to sue HSBC after he experienced difficulty recovering the funds.

At trial, Colman J noted that in addition to the potential criminal liability institutions may sustain for breaching AML/CTF laws, those handling suspect customer funds must balance two competing civil interests; namely, their contractual obligations to customers and their obligations to third parties under equitable constructive trust principles.³⁹⁵ To guide them in weighing up these interests, His Honour held that where an institution has doubts as to the legitimacy of certain customer funds, it should take the following actions:

- where it has a genuine suspicion that a customer is <u>about to pay over</u> money derived from criminal activity-
 - (i) make a report in advance to the U.K.'s FIU, the National Criminal Intelligence Service (NCIS); or
 - (ii) in the case of a CHAPS payment, delay the authentication of the relevant funds whilst a report is made to the NCIS.³⁹⁶
- where it has a genuine suspicion that a customer has <u>just paid over</u> money derived from criminal activity, and such money has already been credited-
 - (i) apply to the NCIS and wait for directions; or
 - (ii) in situations where it is anticipated that the relevant customer will imminently request that the suspect funds be transferred out of their account, temporarily freeze their account.

In providing such guidance, Colman J articulated that "although [a] bank may be placed in a difficult commercial position vis-à-vis its customer by reason of the need to avoid criminal liability including tipping off on the one hand and liability as a constructive trustee on the other, there now exists procedures which it is entitled to deploy in order to protect its position in both respects..." ³⁹⁷ His Honour held that whilst statutory obligations such as tipping off are of real concern to an institution, the Bank of Scotland case provides a process

Perrin, S., 'The Pitfalls of Flagging up Suspect Bank Transactions' (2004) Financial Director 42 http://images.vnunet.com/v6_static/oracle/pdf/fd/dec_laundering_fdbrief.pdf at 16 August 2007.

³⁹⁷ See Hosni Tayeb v. HSBC Bank plc [2004] EWCH 1529, para 77.

for determining how to resolve the question of what information can be disclosed to avoid or defend proceedings brought by a customer for breach of mandate.

Reconciling conflicting and competing interests

As evidenced by the previously discussed authorities, U.K. courts now consider the position regarding institutions' various AML/CTF-related obligations (and potential liabilities) to be settled. Whilst the cases have not disputed that there has at times been a misalignment between institutions' obligations under legislation, contract law and constructive trust principles, they have generally taken the view that the U.K. Parliament intends for there to be a "precise and workable balance of conflicting interests" under municipal AML/CTF laws. 398

Though some institutions may still be uncertain regarding how best to balance their obligations and resulting risk exposure, a number of commentators have held that their primary objective should always be the avoidance of criminal liability under AML/CTF laws. Given the penalties, reputational damage and commercial consequences that may accompany a criminal conviction under AML/CTF legislation, institutions that have some suspicion regarding the legitimacy of a customer's funds, should – first and foremost – satisfy their reporting obligations and seek further regulatory and/or legal guidance.

Whilst regulatory advice and/or court Directions will not necessarily protect an institution from potential lawsuits initiated by customers and third parties, they may assist it to defeat any subsequent civil actions waged against it. Although there is a school of thought that seeking the court's guidance will heighten an institution's AML/CTF legal risk by exposing evidence that may later be used to affix it with liability as a constructive trustee, there is a strong contrary view that doing so might minimise its exposure to such liability. Indeed, by properly reporting its suspicions and seeking Directions before paying away certain suspect

³⁹⁹ Op cit n388, 12.

³⁹⁸ See the decision of the U.K. Court of Appeal in K Ltd v. National Westminster Bank plc [2006] EWCA Civ 1039.

funds, an institution may be considered to have worn "a badge of honesty" ⁴⁰⁰ in its dealings with the funds. As previously discussed, this may prove to be particularly important in any 'knowing assistance' case, where the presence of dishonesty will be crucial to the success of a claim. ⁴⁰¹

It is highly unlikely that any institution acting in accordance with judicial Directions will subsequently be held liable as a constructive trustee. In *Bank of Scotland v. A Limited* [2001] 1 WLR 751, the court held that it would be "almost inconceivable" that any institution that proactively sought and followed the court's guidance would subsequently be held to have acted dishonestly. Further, in *Hosni Tayeb v. HSBC Bank plc* [2004] 4 All ER 1024, the court ruled that it would be "wholly unrealistic" for any institution that complied with judicial guidance and did not pay away the relevant funds, to subsequently incur liability as a constructive trustee. 403

Thus, whilst every case will turn upon its own facts, U.K. case law suggests that any institution that has a suspicion regarding certain customer funds and is concerned about its various legal obligations, should:

- report its suspicion to the relevant FIU;
- where tipping off is an immediate concern (perhaps due to customer instructions to pay out or transfer the suspect funds), seek advice from the relevant regulator;⁴⁰⁴
- where regulatory or law enforcement officials have directed that the suspect transactions should proceed but there is still concern about exposure to civil liability, apply to the court for formal Directions;⁴⁰⁵ and

⁴⁰⁰ Op cit n354.

⁴⁰¹ See Royal Brunei Airlines v. Tan [1995] 3 All ER 97.

⁴⁰² Op cit n400.

⁴⁰³ It should be noted that when Colman J was making this point in *Hosni Tayeb v. HSBC Bank plc* [2004] 4 All ER 1024, His Honour was envisaging a situation where the Respondent protected the third party's position by not paying the relevant funds away. Thus, a court's view of an institution's potential liability as a constructive trustee may differ from this where (a) 'tipping off' concerns are involved, and (b) the institution has paid funds away and is facing civil action from an aggrieved third party.

It should be noted that in jurisdictions such as Australia, the role of the regulator and FIU may be carried out by the same government body.

Case law from the United Kingdom suggests that an institution may avoid liability as a constructive trustee and deflect any claims of dishonesty where it (i) properly reported its suspicions; (ii) was unable to apply to the Court for directions because doing so may have 'tipped off' the suspect customer; and/or (iii)

 strictly follow any Orders made by a court in relation to the handling of the suspect funds and the disclosures (if any) that may be made to that customer and/or any associated third parties.

Whilst the steps outlined above might still leave an institution exposed to the initiation of civil lawsuits by a suspect customer and/or third parties, in most cases they should protect it from incurring criminal liability under applicable AML/CTF legislation. Further, they should mitigate the likelihood that an institution will be found to have acted "dishonestly" for the purposes of any 'knowing assistance' claim.

4.6 Conclusion

Whilst many institutions may focus their AML/CTF compliance efforts upon the avoidance of criminal liability under applicable legislation, it is clear that they should not ignore their possible liability at civil law. Institutions that disregard or deliberately overlook their civil law obligations when undertaking their risk evaluation and treatment activities, may (depending on the jurisdiction(s) within which they operate) heighten their AML/CTF legal risk and their exposure to civil 'breach of contract' claims and equitable constructive trust claims. Further, and perhaps more importantly, they may increase their vulnerability to lengthy and intrusive regulatory reviews that are not only resource-intensive, but potentially damaging to their reputation and bottom line.

As previously discussed in **Chapter 3** of this thesis, many AML/CTF regulators currently appear to be abandoning criminal AML/CTF enforcement actions in preference to civil courses of action. Given their ability to reprimand an institution without the collateral damage attached to criminal prosecutions, civil enforcement actions may secure a positive result and the imposition of penalties against a non-compliant institution, far more efficiently than any criminal lawsuit. The number of civil monetary penalties imposed upon institutions in recent years for AML/CTF compliance failures, appears to far outweigh the number of comparable criminal fines imposed during the same period. Evidently, where the primary

complied with Directions to pay the suspect funds away in circumstances where the destination of the funds was known to law enforcement.

purpose of a particular enforcement action is to 'name and shame' a non-compliant institution and rectify its internal control failures, this can just as easily (if not more easily) be achieved via a civil suit than a criminal prosecution.

Undoubtedly, an institution's AML/CTF legal risk at civil law will be heightened where it operates in a jurisdiction characterised by:

- a regulatory propensity to launch civil enforcement actions against institutions in breach of their AML/CTF compliance obligations; and/or
- some uncertainty about the interaction and coexistence of their various AML/CTF-related obligations under statute, in contract law and under constructive trust principles.

As evidenced by the situation in the U.K. during the past few years, institutions operating in certain countries may find themselves in a precarious legal position if there is a lack of clarity surrounding the interplay between their legislative requirements, contractual obligations to customers, and potential liability as a constructive trustee. Any uncertainty around their obligations and, more specifically, which obligations should take priority in terms of their compliance efforts, may create a situation where some institutions feel compelled to trade off compliance with their civil obligations in order to avoid committing criminal AML/CTF offences (or vice versa). As demonstrated by the string of U.K. authorities discussed in this Chapter, in certain circumstances an institution's compliance with one set of legal obligations may heighten its AML/CTF legal risk with respect to another.

Whilst this Chapter has primarily focused upon the efforts of the U.K. courts to address the apparent misalignment between various AML/CTF obligations, it is hoped that other jurisdictions with comparable legal systems and AML/CTF laws will take a similar approach to the U.K. Requiring institutions to comply with their AML/CTF legislative obligations, only to leave them exposed to lawsuits under contract law or equity, is surely counterproductive to creating a robust AML/CTF reporting regime and engendering the support of financial institutions in the fight against financial crime. Evidently, the only individuals to benefit from any legal uncertainty surrounding institutions' obligations and levels of AML/CTF legal risk, would be the money launderers and terrorism financiers trying to exploit the financial system for their own purposes.

Chapter 5

Managing and Mitigating AML/CTF Legal Risk

"Even a correct decision is wrong when taken too late" - Lee lacocca

5.1 Introduction

As previously discussed, an institution in breach of its prescriptive or risk-based AML/CTF requirements may face AML/CTF legal risk, financial risk and reputational risk. Depending on the nature, length and severity of its legislative breaches, and the jurisdiction(s) within which they occurred, an institution's risk may translate into a range of formal and/or informal enforcement actions. Typically, the former will create the greatest risk exposure for an institution. Unlike more private, informal enforcement actions such as Memorandums of Understanding, formal enforcement actions (including criminal prosecutions) often have a greater propensity to attract media coverage and invoke public opinion. Accordingly, they generally represent a higher level of reputational risk than those enforcement tools that enable an institution's identity and compliance failures to remain shrouded in secrecy.

Once an institution's breaches of municipal or extraterritorial AML/CTF legislation have come to the attention of regulatory officials, the risk management strategies that it can employ may be limited. Clearly, it is too late for the adoption of an avoidance strategy as the risk has materialised and compliance failures have already occurred. However, that is not to say that an institution that has fallen foul of its legislative obligations, has no risk management strategies available to it at all. Indeed, it might still be capable of mitigating its ongoing risk and even influencing the regulatory outcomes of its behaviour, by taking certain corrective actions in the aftermath of its compliance failure(s). Even after unequivocally engaging in contraventions of AML/CTF legislation, an institution's fate will not always be predetermined. Given that many AML/CTF regulators have typically dedicated significant

⁴⁰⁶ United States Department of the Treasury, BSA/AML – Getting it Right: OTS Formal and Informal Enforcement Actions (2006) http://www.ots.treas.gov/docs/4/480250.pdf> at 6 January 2008.

resources to the prevention and early resolution of AML/CTF compliance failures, 407 institutions may be able to avoid protracted and expensive enforcement proceedings by proactively identifying, reporting and addressing its legislative contraventions.

As **Chapter 4** of this thesis has already discussed a number of ways in which an institution might seek to manage its AML/CTF legal risk at civil law, this Chapter focuses largely on the risk management strategies that may be employed to limit an institution's risk of incurring criminal liability for a money laundering or terrorism financing offence and/or an AML/CTF compliance failure. That being the case, there is undoubtedly a degree of overlap between the risk management techniques an institution may use to address its potential liability at both civil and criminal law. Whether it is facing civil or criminal enforcement action, an institution may minimise its AML/CTF legal risk by taking certain steps to convince regulatory and law enforcement authorities of the seriousness with which it regards AML/CTF compliance. Thus, whilst this Chapter is primarily concerned with the way in which an institution might seek to avoid or limit its criminal liability, it also highlights several ways that an institution may seek to limit its potential liability at civil law.

As Australia is still in the process of implementing the *AML/CTF Act 2006* (Cth), it is not yet possible to provide any detailed analysis of the risk management techniques and strategies that Australian institutions may rely upon when found to be in breach of their legislative requirements. To date, no institutions have faced formal enforcement proceedings as a result of their non-compliance with the Act's provisions. Accordingly, the commentary contained herein with respect to the management of AML/CTF compliance failures and AML/CTF legal risk, tends to focus on the experiences of institutions and regulatory authorities in the U.S. and the U.K. Essentially, this Chapter:

- explores the ways in which an institution might seek to manage and mitigate its
 AML/CTF legal risk following a breach of its AML/CTF legislative obligations;
- outlines the various regulatory outcomes that may arise where an institution is prepared to voluntarily report its legislative breaches and take appropriate correction actions; and

⁴⁰⁷ Schmidt Bies, S., 'Bank Secrecy Act Enforcement' (Testimony before the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, 3 June 2004).

 assesses the mitigating factors that might influence the number, type and quantum of penalties imposed upon an institution for breaches of AML/CTF legislation.

5.2 Methods of managing AML/CTF legal risk

Some commentators have reasoned that institutions cannot viably use transfer, reduction (mitigation) or acceptance risk management strategies to manage their legal risk, because such strategies inherently recognise that the law may be infringed. Similarly, several commentators have held that whilst a number of traditional risk management techniques have become engrained in the fabric of institutional decision-making, many cannot be applied to the concept of legal risk because they inadvertently promote breaking the law where doing so is more financially profitable than compliance. The oft-cited example of these types of risk management techniques is the cost-benefit approach which, when used in isolation from other decision-making tools, may encourage an institution to flout its AML/CTF legislative obligations if the total expected benefits of non-compliance outweigh the potential penalties (and other costs) it may attract. According to some commentators, crimes committed by corporations as a result of "a studied calculation of likely costs and benefits" of engaging in criminal behaviour are "especially reprehensible".

However, assertions that legal risk can only be viably managed through the use of an avoidance strategy appear to be incorrect or, at the very least, limited in their application to prescriptive AML/CTF legislative requirements. Even when enacted in risk-based regimes, such requirements will apply to institutions equally, irrespective of their individual ML/TF risk profiles. Typical examples of prescriptive requirements include reporting significant (or 'threshold') transactions over a stated monetary value, conducting minimum customer due diligence, and retaining specific records relating to customers' transactions. Given that institutions have no real legal discretion regarding the extent of their compliance with such obligations, prescriptive requirements appear to give rise to a clear 'dichotomy of

Trzaskowski, J., Legal Risk Management – Some Reflections (2005) Legal Risk Management http://www.legalriskmanagement.com/PUBLICATIONS/2005_LRM.pdf at 28 March 2006.

op cit n211, 2.

compliance', insofar as institutions that are not strictly compliant with them, will necessarily be non-compliant with them. Unlike the situation that might arise in relation to risk-based requirements, there will not be 'degrees of compliance' with prescriptive obligations.

However, whilst prescriptive legislative requirements may be quite amenable to claims that institutions can only prudently address their legal risk through an avoidance risk management strategy, it appears that risk-based requirements may give rise to a broader palette of possible risk management strategies. By their very nature, risk-based legislative requirements implicitly empower institutions to adopt the level of risk they desire, commensurate to their level of ML/TF risk and their appetite (or otherwise) for such risk.

As opposed to the 'dichotomy of compliance' that may exist with respect to prescriptive legislative requirements, risk-based requirements seemingly lend themselves to a broader spectrum of compliance tools and techniques. Despite setting certain baseline standards, they enable institutions to determine the extent to which they mitigate their ML/TF risk. In some cases, they even enable institutions to dispense with the minimum standards, providing that they can justify any such deviation on the basis of their risk profile. For instance, whilst Chapter 4 of Australia's Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) (Cth) outlines the minimum identification procedures for low and medium risk customers, some institutions have – in a limited number of cases – seemingly attempted to use their ML/TF risk profile and overarching risk-based approach to justify a dispensation from these requirements, and implement less onerous due diligence standards. By comparison, more risk averse institutions have sought to manage and mitigate their ongoing ML/TF risk (and AML/CTF legal risk) by implementing internal KYC processes that are far more stringent than the minimum requirements contained in AML/CTF legislation.

It should be noted however that any deviation from minimum legislative standards – whether or not it is perceived by an institution to be justified – may attract heightened levels of regulatory scrutiny and legal risk. This is especially apparent where most other institutions/industry segments have adopted the minimum standards.

Thus, claims that an institution's legal risk can *only* be addressed through the adoption of an avoidance risk management strategy, are not entirely correct when contextualised in terms of risk-based approaches to AML/CTF. Whilst such approaches necessarily entail a number of prescriptive requirements, to which an avoidance strategy will ideally be applied, they also contain a number of risk-based requirements which enable institutions to determine the degree to which they mitigate their risk. As such, risk-based regimes may give rise to a range of avoidance and mitigation strategies, all tailored to different legislative obligations and the ML/TF risk profiles of the institutions addressing them.

Whilst avoidance and mitigation strategies may provide an effective means of addressing AML/CTF legal risk, the management of such risk does not easily lend itself to the use of transfer strategies. Whilst it is well established that institutions may use risk transfer strategies to limit their reputational and financial risk, they will generally be unable to do the same in relation to their AML/CTF legal risk. Operationally outsourcing or transferring some of its compliance activities to a third party⁴¹² will generally not relieve an institution from its legal obligation to ensure that the AML/CTF requirements underpinning such activities are met. The overriding legal responsibility for compliance with AML/CTF legislation (and therefore, the AML/CTF legal risk attached to non-compliance) will remain with the institution and, unlike the practical execution of certain compliance activities, cannot be transferred to another entity.

Thus, whilst an avoidance risk management strategy should safeguard an institution against committing any inadvertent contraventions of AML/CTF legislation, the adoption of a risk transfer or mitigation strategy might always leave an institution exposed to a degree of AML/CTF legal risk. This is especially evident in risk-based AML/CTF regimes, where regulatory authorities may have difficulty determining an institution's ML/TF risk profile, understanding its risk-based approach, or assessing its level of compliance with legislative requirements. As opposed to the use of an avoidance strategy in relation to prescriptive AML/CTF requirements, reliance on a mitigation or transfer strategy in relation to risk-based

In accordance with FATF Recommendation 9, many countries now permit institutions to rely upon intermediaries and other third parties (such as brokers and financial planners) to carry out customer due diligence, screen customers' identities, and create/retain records on their behalf.

requirements will potentially hamper the ability of regulatory authorities to measure an institution's level of AML/CTF compliance. Evidently, the way in which an institution seeks to address its risk-based requirements is likely to be hinged upon its own perceptions of ML/TF risk.

Even in instances where an institution has fallen short of its risk-based requirements, it may still avoid a formal enforcement action if it can demonstrate that it made reasonable and genuine attempts to fulfil its obligations. In both the U.K. and the U.S., a number of institutions have effectively limited their AML/CTF legal risk by showing regulatory authorities that despite their AML/CTF compliance failures, they had assessed their ML/TF risk and made a concerted effort to implement controls commensurate to that risk. 413

Though it will not always be easy for an institution to demonstrate that it had effective, risk-based controls in place at the time of an AML/CTF legislative breach, many institutions operating in more heavily regulated AML/CTF regimes are now spending copious resources on the implementation of their AML/CTF compliance programs. According to a survey of more than 60 financial services executives conducted in 2006 by global accounting firm KPMG, more than 50 per cent of respondents planned to hire more AML/CTF compliance staff and approximately 75 per cent of respondents planned to spend more money on their AML/CTF programs during the 2007 calendar year. 414

Whilst limited in its scope and respondent base, the findings of the KPMG survey appear to correlate with the increased AML/CTF legal risk seemingly faced by institutions operating in the U.S. and other more heavily regulated AML/CTF regimes. Many institutions are now emphasising the importance of AML/CTF compliance, and seeking to mitigate their potential AML/CTF legal exposure by adopting an avoidance and/or mitigation risk management strategy. There is seemingly an upwards trend in the time and money that institutions are now spending to design and implement their AML/CTF controls, and safeguard themselves against money laundering and terrorism financing activities. Whilst this may partially be

⁴¹³ 'FSA Says Demonstrating Controls Can Help Avoid Enforcement', Compliance Reporter, 4 July 2005, 1. Newman, R., 'Firms Tackle Money Laundering', Knight Ridder Tribune Business News, 5 October 2006,

done in an attempt to prevent their exploitation at the hands of money launderers and terrorism financiers, the underlying motivation for the implementation of such controls is likely to be legislative compliance and the mitigation of AML/CTF legal risk.

5.3 Minimising the fallout from a compliance failure

Whilst an institution may seek to fulfil its statutory requirements and minimise its AML/CTF legal risk by employing an avoidance or mitigation strategy, it might still fall foul of its legislative obligations if such a strategy is not properly executed. However, even in circumstances where the adoption of a formal risk management strategy has failed to prevent the commission of a money laundering/terrorism financing offence and/or an AML/CTF compliance failure, an institution can still take certain steps to mitigate and minimise the resulting damage. Depending on the severity of its legislative breaches and the jurisdiction(s) within which they occurred, an institution might be capable of minimising its ongoing AML/CTF legal risk, influencing the type of enforcement action(s) (if any) taken against it, and/or reducing the quantum of any penalty ultimately imposed upon it.

5.3.1 Self-reporting to regulatory authorities

Where an institution has identified a potential breach of its AML/CTF requirements, it may attempt to minimise its AML/CTF legal risk (both at criminal and civil law) by proactively disclosing that breach to regulatory authorities. Depending upon the type of legislative breach at hand, regulatory officials may decide that no formal enforcement action is required because – in the spirit of meta monitoring – the institution is adequately monitoring its own AML/CTF compliance and independently taking steps to rectify its control failures. Even in circumstances where officials determine that formal enforcement action is necessary because the breach is significant or long-standing, self-reporting might enable an institution to receive a reduction in the penalties subsequently imposed upon it. Indeed, sentence reductions for self-reporting have been around for some time. They have often been taken into account by courts willing to acknowledge the time and resource benefits that voluntary admissions of

wrongdoing may have not only for regulatory and prosecutorial authorities, but for the legal system more generally.

That said, it should be noted that the ability of an institution to self-report an AML/CTF compliance failure may be dependent upon the type of compliance failure at hand. Whilst there does not appear to be any academic research on this point, it is presumably far easier for an institution to detect and identify breaches of prescriptive AML/CTF requirements, than risk-based requirements. As noted, prescriptive requirements give rise to a 'dichotomy of compliance' that provides institutions (and, it follows, regulatory authorities) with an unambiguous and objective benchmark against which they can judge their compliance or, as the case may be, non-compliance. By comparison, risk-based AML/CTF legislative requirements are not generally so amenable to such simple assessments of compliance. Considering the degree to which institutional risk-based approaches may vary, and the spectrum of potential compliance options to which these requirements may give rise, an institution's level of compliance or non-compliance will likely be more difficult to identify and, as appropriate, proactively report to regulatory officials.

Given that compliance with risk-based obligations will hinge upon an institution's individual ML/TF risk profile, an institution's perception of its own ML/TF risk will generally dictate how it seeks to achieve AML/CTF compliance. Thus, in cases where an institution's ML/TF risk assessment methodology⁴¹⁵ is inherently flawed or deliberately geared towards particular outcomes, it is unlikely that the entity will be capable of identifying any instances where its AML/CTF program falls short of risk-based legislative requirements. In essence, the institution will be assessing the adequacy and suitability of its AML/CTF measures on the basis of an inaccurate ML/TF risk profile. Whilst it may genuinely believe that its AML/CTF program and controls are commensurate to its ML/TF risk, a risk assessment and compliance review conducted by an independent third party/regulatory authority may determine that the institution's measures are vastly inadequate.

An institution's "ML/TF risk assessment methodology" refers to the way in which an institution seeks to assess its levels of ML/TF risk and, by extension, construct its risk-based approach. Whilst many institutions may hinge their risk assessment methodology upon the "three bases" of ML/TF risk, the precise risk factors used by each institution, as well as the relative importance assigned to each of them, will typically vary from institution to institution.

Nevertheless, where a potential breach of AML/CTF legislation has been identified, an institution might minimise its AML/CTF legal risk by voluntarily and swiftly reporting that breach to regulatory authorities. Regulators in some jurisdictions have seemingly been more lenient in their treatment of self-reporting institutions, as opposed to those that have deliberately sought to ignore and/or conceal their legislative breaches. A number have been prepared to significantly decrease a monetary penalty (or even forego formal enforcement action altogether) when an institution has reacted immediately to its legislative breaches and taken corrective action to rectify them.

In the U.S., the ability of institutions to limit their AML/CTF legal risk (as well as their financial and reputational risk) by proactively self-reporting their legislative breaches, is formalised in the McNulty Memo. That Memo, which in December 2006 superseded and replaced the Thompson Memo discussed in **Chapter 3** of this thesis, states that by voluntarily disclosing their misconduct, institutions may be granted concessions with respect to the severity of any enforcement action taken against them. Further, in relation to criminal AML/CTF legislative breaches, the *U.S. Sentencing Guidelines* also stipulate that a defendant institution may have its offence level reduced where it has:

- promptly self-reported its offences/compliance failures;
- cooperated with investigative and regulatory authorities during any resulting investigation;⁴¹⁷ and
- accepted responsibility for its acts (for instance, by entering a guilty plea prior to the commencement of any criminal trial).⁴¹⁸

That said, simply self-reporting its AML/CTF compliance failures will not be sufficient to limit an institution's AML/CTF legal risk in circumstances where the disclosure was forced⁴¹⁹ and/or only made to regulatory authorities a significant time after the failures arose.

Memorandum from Paul J. McNulty, Deputy Attorney General, to Heads of Department Components and United States Attorneys, 12 December 2006. http://www.usdoj.gov/dag/speeches/2006/mcnulty_memo.pdf at 1 March 2009.

⁴¹⁷ See Hyewon, H., and Wagner, N., 'Corporate Criminal Liability' (2007) 44(2) American Criminal Law Review 337.

⁴¹⁸ United States Sentencing Commission, Federal Sentencing Guideline Manual (2006) § 8C2.5(g)(1) http://www.ussc.gov/2006guid/tabcon06 1.htm> at 10 October 2007.

Self-reporting may clearly assist an institution to demonstrate that its legislative breaches are not attributable to any failure to monitor and manage its ongoing AML/CTF compliance. In order to properly self-report however, an institution will need to accept responsibility for its AML/CTF compliance failures, and implement corrective actions to ensure that such failures do not reoccur. Even where self-reporting does not enable an institution to avoid a formal enforcement action, it may nevertheless limit its reputational damage and qualify the institution for more commercially desirable enforcement outcomes, such as a deferred or non-prosecution agreement.

Whilst it may have a number of benefits however, self-reporting should be regarded as a calculated risk. 420 Before proactively disclosing any instance of legislative non-compliance to regulatory officials, an institution should weigh up both the potential costs and benefits attached to such a course of action. Whilst voluntary disclosure may pave the way for a deferred or non-prosecution agreement, it may alternatively give rise to criminal proceedings – hinged upon the very admissions made by the institution in the course of its self-reporting.

Even where an institution successfully avoids criminal prosecution by self-reporting its legislative breaches, it may nevertheless still be exposed to civil law proceedings. Given the ability for criminal and civil proceedings to be conducted in parallel, and the enhanced information sharing evident between regulatory and law enforcement bodies post-September 11, voluntarily disclosing misconduct to certain authorities may result in others also coming into possession of the same information. Thus, unless an institution is prepared to contemporaneously report its legislative breaches to all concerned regulatory and law enforcement authorities, it should carefully assess the impact that self-reporting may have upon its level of AML/CTF legal risk. Voluntary disclosure without any prior consideration of the possible consequences may leave an institution exposed to an even greater level of risk than it would have faced had it simply failed or refused to disclose its non-compliance.

Self-reporting may appear to be forced and entirely self-serving in cases where it takes place immediately after an independent/regulatory review is announced, and/or occurs in a situation where the discovery of the institution's AML/CTF compliance failures appears inevitable.

420 Op cit n208, 1144.

5.3.2 Deferred and non-prosecution agreements

The difficulties inherent in waging complex prosecutions against large, well-resourced corporations have been widely documented. Apart from the high level of evidentiary material required for such actions to be successful, 222 corporate prosecutions may prove to be unjustifiably resource-intensive for typically under-resourced regulatory authorities. This is particularly so in circumstances where a corporate defendant is financially profitable enough to engage a throng of legal professionals and draw proceedings out over many years using various avenues of appeal. Due to these reasons, and the fact that indictment can amount to "a virtual death sentence for business entities", 223 prosecutors and AML/CTF regulators will not always be eager to launch criminal enforcement actions against non-compliant institutions. Accordingly, institutions alleged to have committed a money laundering offence and/or a criminal breach of AML/CTF legislation may seek to limit their ongoing AML/CTF legal risk by entering into a deferred or non-prosecution agreement.

Although these types of agreements are functionally very similar, there is one striking point of difference between them. Whilst non-prosecution agreements arise in the absence of any formal indictment, deferred prosecution agreements arise only after criminal charges have been filed against an entity. Alexamer Nevertheless, the practical operation of these agreements is ostensibly the same; both can enable an institution to avoid a potentially protracted and expensive criminal trial by acknowledging its wrongdoing, undertaking prompt remedial action, implementing a compliance program, making restitutionary payments and, as necessary, submitting to a federal monitor. If, at the end of the relevant deferred or non-prosecution period, the terms of such agreements are not strictly met, the U.S. government

For instance, see New South Wales Law Reform Commission, Sentencing: Corporate Offenders (Report No 102, NSWLRC, Sydney, 2003).

⁴²² In many jurisdictions, prosecutors must fully disclose evidentiary material, provide particulars of all charges and, perhaps most importantly, prove such charges beyond reasonable doubt. This may be particularly challenging with respect to certain money laundering offences, which may involve a number of accounts, several layers of transactions, complex financial products, fictitious customer identities, and international transfers.

⁴²³ Op cit n208, 1097.

⁴²⁴ Illovsky, E., Corporate Deferred Prosecution Agreements: The Brewing Debate (2006) 21(2) Criminal Justice 36.

⁴²⁵ Altenbaumer-Price, K., Pros and Cons of Deferred Prosecution Agreements [2006] Executive Legal Adviser 1.

may resuscitate (or, in the case of a non-prosecution agreement, file) the criminal charges relating to an institution's misconduct.

Perhaps demonstrative of the fact that many commentators have inflated views of institutions' levels of AML/CTF legal risk, there appears to be a sharp increase in the use of deferred and non-prosecution agreements in the U.S. This may be largely attributable to a fundamental shift in U.S. enforcement policy following a spate of corporate fraud scandals in the early 2000s. After seeing first-hand the potential consequences attached to the indictment of large corporations such as Enron and Arthur Andersen, the U.S. Department of Justice has seemingly shifted its role from one of indictment and prosecution, to one of "widespread structural reform." As opposed to simply prosecuting institutions for their alleged wrongdoing, government officials now appear to be more interested in identifying, and requiring the rectification of, the internal control failures that enabled such wrongdoing to occur in the first place.

Whilst the *U.S. Sentencing Guidelines* have for some years allowed an institution's culpability score to be reduced for the purposes of sentencing where it has reported its offences and fully cooperated with any subsequent investigation, it was not until the release of the Thompson Memo in 2003 that the U.S. Department of Justice formally recognised the use of deferred and non-prosecution agreements. At that time, the Department acknowledged that U.S. prosecutors could reward an entity's regulatory and investigatory cooperation by granting it prosecutorial immunity or amnesty. Interestingly, since the publication of the Thompson Memo, no criminal charges have been filed against a major U.S. corporation in the absence of a deferred or non-prosecution agreement.

In appropriate circumstances, U.S. officials are clearly willing to forego an institution's criminal indictment in return for its agreement to enter into a deferred or non-prosecution agreement. Between 2002 and 2005 inclusive, U.S. prosecutors executed more than twice as

Op cit n287, 167.

⁴²⁶ Op cit n287, 161.

⁴²⁷ See Memorandum from Larry D. Thompson, Op cit n207.

many of these agreements than they did during the preceding decade. Further, whilst an estimated 13 deferred and non-prosecution agreements were executed during 2006, an additional 37 were publicly announced during 2007. Of these 37 agreements, four (i.e. approximately nine per cent) related to money laundering offences and/or criminal breaches of U.S. AML/CTF legislation. Electronic Clearing House Inc., United Bank of Africa and Union Bank of California all entered into agreements to avoid being criminally prosecuted for their various money laundering offences, whilst American Express Bank International agreed to the execution of such an agreement to avoid criminal proceedings in relation to its criminal breaches of the Bank Secrecy Act.

Although each of these four institutions have since managed to avoid the time and cost typically associated with protracted legal proceedings, the terms of their individual agreements highlight just how burdensome compliance with a deferred or non-prosecution agreement can be. ⁴³⁴ Given that the terms of an agreement will be individually stylised to an institution and its specific AML/CTF compliance failures, they may necessarily require an institution to implement measures that exceed usual industry standards. That said, as the alternative to any deferred or non-prosecution agreement will be criminal prosecution, many entities may consider themselves lucky to escape formal enforcement proceedings by implementing systems and controls that – in operational terms – constitute best practice.

It is not uncommon for the conditions of a deferred or non-prosecution agreement to be sweeping in their scope. For instance, the terms of the deferred prosecution agreement executed in the matter of *United States of America v. American Express Bank International*

⁴²⁹ Corporate Crime Reporter, Crime without Conviction: The Rise of Deferred and Non Prosecution Agreements (CCR, New York, 2005).

⁴³⁰ Op cit n287, 191-193.

See *United States of America v Electronic Clearing House Inc.*, Non-Prosecution Agreement, United States Attorney, Southern District of New York, 26 March 2007.

⁴³² United States Department of Justice, U.S. Announces Agreement with United Bank of Africa (Press Release, 6 July 2007).

⁴³³ United States Department of Justice, Union Bank of California enters into Deferred Prosecution Agreement and Forfeits \$21.6 million to Resolve Bank Secrecy Act Violations (Press Release, 17 September 2007).

That said, it should be noted that none of the four institutions' agreements required them to engage a federal monitor to secure their future legislative compliance. Had they done so, the ongoing financial burden of compliance with their deferred and non prosecution agreements would likely have been far more significant.

on 3 August 2007, required the institution to formally acknowledge its wrongdoing, pay USD\$55 million in civil forfeiture, and implement an effective AML/CTF program in compliance with the *Bank Secrecy Act*.⁴³⁵ This program necessarily entailed the creation of additional policies and procedures, enhancement of transaction monitoring capabilities, deployment of further AML/CTF employee training, and engagement of AML compliance experts to comprehensively review and overhaul the institution's AML/CTF program.⁴³⁶

In addition to instigating these structural and remedial reforms, American Express Bank International's deferred prosecution agreement also required it to stand silent in the face of any public criticism or negative media coverage surrounding its criminal acts/omissions; even where such criticism was factually incorrect. According to *Clause 3* of the agreement, "any such contradictory public statement by [the bank], its attorneys, board of directors, agents, officers or employees" would constitute a breach of the agreement and render the institution subject to prosecution. Such clauses are not altogether uncommon in deferred prosecution agreements, 437 with many other institutions also finding that their agreements prohibited them from countering the reputational damage they might have incurred as a result of their criminal offences and legislative breaches.

Thus, whilst deferred and non-prosecution agreements may spare an institution from incurring the reputational damage they would otherwise have faced during the course of a lengthy, highly publicised and/or otherwise unfavourable enforcement action, they will not entirely safeguard an institution against incurring reputational risk. In fact, it may be contended that such agreements actually enflame an institution's reputational risk by requiring it to take responsibility for its money laundering offences or AML/CTF compliance failures. This risk may be particularly pronounced in those cases where the U.S. Department of Justice has publicly announced the execution of the agreement or required the relevant company to prominently display the agreement on its website.

⁴³⁵ United States Department of Justice, American Express Bank International enters into Deferred Prosecution Agreement and Forfeits \$55 million to Resolve Bank Secrecy Act Violations (Press Release, 6 August 2007).

⁴³⁶ See *United States of America v. American Express Bank International*, Deferred Prosecution Agreement, United States District Court in the Southern District of Florida, 3 August 2007.

⁴³⁷ Op cit n424, 37.

Nevertheless, in circumstances where an institution has committed blatant breaches of AML/CTF legislation and is likely to be found guilty in any ensuing criminal action, the execution of a deferred or non-prosecution agreement may limit its longer term AML/CTF legal risk and reputational risk. Whilst taking responsibility for its criminal offences, agreeing to pay a monetary penalty and implementing sweeping internal reforms may not at first glance be appealing to an institution, entering into such an agreement may enable it to avoid prosecution, limit its reputational damage, protect its shareholder value and preserve the jobs of its employees. Given the collapse of several companies following their indictment for financial crimes in the early 2000s, the terms of a deferred or non-prosecution agreement would have to be particularly burdensome for an institution to consider forgoing the risk management benefits it may provide.

5.3.3 Reliance on criminal defences

Where a deferred or non-prosecution agreement has not been forthcoming or complied with, an institution may still seek to mitigate its legal exposure by mounting one or more defences in any ensuing criminal action. Typically, the number and type of defences that an institution (or one of its employees) can rely upon, will hinge upon the construction of municipal AML/CTF laws and the legislative drafting of the relevant offence(s). For instance, the *MLCA* stipulates that it is a criminal offence to knowingly engage in (or attempt to engage in) transactions involving property derived from "specified unlawful activity" with a value greater than USD\$10,000. As this offence extends to both actual and attempted dealings with property gained through unlawful means, institutions and individuals are relatively limited in the defences they can use to deflect criminal liability. They cannot simply seek to defend themselves on the basis that they never completed the transaction in question, and/or that they did not know that the funds involved were derived from a specific crime. Even if such arguments were substantiated in court, they would

⁴³⁸ Op cit n425.

⁴³⁹ Under 18 U.S.C. § 1957 a defendant need only know that the funds in question were derived from some type of criminal activity. It is not required that they know the particular crime from which funds were derived. See Razzano, F.C., 'American Money Laundering Statutes: The Case for a Worldwide System of Banking Compliance Programs' (1994) 3(277) Journal of International Law & Practice 288.

not diminish an institution's liability because they would not defeat any of the key elements of the offence.

In addition to the particular drafting of certain legislative provisions, the defences available to an institution will generally rest upon the interpretation of those provisions by the courts. Through case law and precedent, courts may restrict or expand the pool of defences from which a defendant may seek to limit their AML/CTF legal risk. For instance, returning to 18 U.S.C. § 1957(a), whilst the drafting of this offence indicates that knowledge is one of its key elements, in recent years the U.S. courts have significantly weakened the type and extent of knowledge necessary for the commission of this offence. In cases such as *United States v. Flores*, 454 F.3d 149, 155-156 (3d Cir. 2006) and *United States v. Epstein*, 426 F.3d 431, 440 (1st Cir. 2005), the courts have held that 'wilful blindness' will be sufficient to satisfy the knowledge requirements of the offence. As a result, the evidentiary burden placed upon U.S. prosecutors in such cases has decreased, whilst the AML/CTF legal risk faced by potential defendants has increased.

The expansive judicial interpretations given to certain elements of 18 U.S.C. § 1957(a) have limited the types of defences available to institutions in any related legal proceedings. As such, many of the defences used by institutions to deflect liability and defeat criminal charges relating to breaches of the MLCA, have been largely technical in nature. For instance, as seen in United States v. Jackson, 983 F.2d 757, 764-65 (7th Cir. 1993), a number of defendants have challenged the necessary knowledge requirements on the basis that they are unconstitutionally vague. However, the courts have uniformly rejected this argument on the basis that Congress included sufficient guidelines for defendants to understand what conduct the legislation prohibits.

In addition to arguments of unconstitutional vagueness, a number of institutions have also tried to minimise their AML/CTF legal risk by attacking the overall construction of 18 U.S.C. § 1957(a). As evidenced by United States v. Edgmon, 952 F.2d 1206 (10th Gr. 1991), some defendants have argued, albeit unsuccessfully, that the longstanding principles of

⁴⁴⁰ Op cit n230, 776.

'double jeopardy' should prevent them from being tried for both money laundering and the required "specified unlawful activity". 441 Others have challenged the MLCA in its entirety; claiming that Congress cannot legally regulate a certain type of criminal activity unless it falls within its powers under the constitutional Commerce Clause. 442 However, the Courts have rejected such arguments on the basis that the use of federally insured banks to transport money across state borders creates a sufficient nexus with interstate commerce to fall within the Congressional powers enshrined in the U.S. Commerce Clause. 443

Clearly, the aforementioned defences have all been relatively academic and legalistic in nature. Many institutions prosecuted for committing an offence under 18 U.S.C. § 1957 have contested the legislation's formulation and drafting, rather than the substantive elements constituting the alleged offence. As opposed to rebutting the necessary mens rea of the alleged offence and showcasing their efforts to achieve legislative compliance, a number of defendants have sought to minimise their AML/CTF legal risk by relying on highly technical defences. That said, whilst these types of defences have often been used in relation to the MLCA, they are not relevant and/or arguable with respect to all money laundering and terrorism financing offences and/or criminal AML/CTF compliance failures.

The availability (or otherwise) of highly technical defences will rest upon the relevant AML/CTF legislation, the drafting of the relevant offence(s), and the judicial interpretation of the elements of that offence. With respect to certain offences, particularly those that carry strict liability, an institution may be left with few avenues through which to defend the charges against it. It may have little choice but to accept the prosecution's claims and accept the legal, financial and reputational ramifications stemming from its AML/CTF compliance failures.

⁴⁴¹ In *United States v. Edgmon*, 952 F.2d 1206 (10th Gr. 1991), the defendant contended that their conviction for both conversion and money laundering constituted multiple punishments for the same offence because conversion was a necessary element of the money laundering charge. However, the Tenth Circuit rejected that claim and held that Congress "intended the money laundering statute to be a separate crime distinct from the underlying offence that generated the money to be laundered".

⁴⁴² See United States v. Owens, 159 F.3d 221 (6th Cir. 1998).

⁴⁴³ Op cit n440, 788.

However, with respect to breaches of other AML/CTF legislative requirements – particularly those relating to risk-based requirements – an institution may be able to deflect its potential liability in any subsequent enforcement proceedings on the basis of several arguments. Given that compliance with risk-based requirements fundamentally hinges upon a shared regulatory and institutional perception of an entity's ML/TF risk profile, any alleged breach of those requirements may be attributed to a number of factors. An institution may seek to defend itself by contending that its ML/TF risk assessment is accurate and regulatory officials simply have an inflated view of its risk levels. Further, it may argue that at the time of the alleged AML/CTF compliance failures, it had appropriate risk-based systems and controls in place to manage and mitigate the risk that its products/services may be exploited for the purposes of money laundering and terrorism financing. Given that each institution will have its own ML/TF risk assessment methodology and individually stylised risk profile, any institution accused of non-compliance with risk-based requirements will presumably have some latitude to convince a court or regulatory authority why it should not attract legal liability and hefty penalties.

5.3.4 Mitigating factors affecting criminal penalties

Where an institution is found by a court to have committed a money laundering/terrorism financing offence and/or breached its AML/CTF legislative requirements, it may nevertheless reduce its AML/CTF legal risk by highlighting circumstances that justify a lesser penalty. Just as defendant institutions may increase their legal culpability through certain acts and omissions, in many jurisdictions they may also decrease their AML/CTF legal risk, as well as their potential reputational and financial damage, by taking certain steps following the identification of their non-compliance. Often, the ways in which an institution may limit the quantum of any penalties imposed upon it, will be enshrined in legislation.

In the U.S., an institution likely to be convicted of criminal breaches of AML/CTF legislation should familiarise itself with the country's *Organizational Sentencing Guidelines* (as contained in *Chapter 8* of the *U.S. Sentencing Guidelines*). These Guidelines stipulate

that an institution can minimise the likelihood of criminal prosecution⁴⁴⁴ and/or the quantum of any fine ultimately imposed upon it,⁴⁴⁵ by accepting responsibility for its conduct. In practical terms, this means self-reporting its criminal legislative breaches and being forthright about its commission of an offence.⁴⁴⁶

The Organizational Sentencing Guidelines also indicate that an institution may seek a reduced offence level (for the purposes of sentencing) where it can demonstrate that at the time of its AML/CTF offence, it had an effective "compliance and ethics program" in place to prevent and detect any violations of U.S. AML/CTF regulations. ⁴⁴⁷ They recognise that even the most diligent institution may not prevent every violation of U.S. law and accordingly, a compliance and ethics program may still be a mitigating factor in sentencing – even in circumstances where it failed to prevent the commission of the relevant offence(s). ⁴⁴⁸

However, as outlined in § 8B2.1 of the Guidelines, an institution seeking to limit its AML/CTF legal risk through evidence of a compliance and ethics program, must do more than simply show that it had designed such a program at the time of the relevant offence(s). It must also prove that it had implemented and enforced that program; perhaps by providing evidence of the internal controls intended to exercise due diligence, meet its AML/CTF compliance obligations, and promote a culture of ethical conduct. An institution's ability to avoid criminal prosecution and/or minimise its resulting AML/CTF legal risk will undoubtedly be greater where it can demonstrate top-down oversight of its compliance activities, the provision of appropriate AML/CTF training to employees, and a process

Whilst the adoption of an effective compliance and ethics program will not guarantee an institution immunity from prosecution, its existence may influence a prosecutor's decision whether or not to prosecute. See United States Sentencing Commission, Federal Sentencing Guideline Manual (2006) § 8B2.1 http://www.ussc.gov/2006guid/tabcon06_1.htm at 10 October 2007.

As discussed in Section 5.3.1 of this Chapter, self-reporting an AML/CTF offence may serve as a deterrent to prosecution or, in circumstances where the relevant offence is perhaps more severe, a mitigating factor that lessens an institution's offence level for the purposes of sentencing. See Tucker Mann, T., Op cit n443, 792.

⁴⁴⁷ Importantly, if high-level personnel have been involved in the relevant AML/CTF offences, there is a rebuttable presumption that the institution did not have an effective compliance program in place at the time of the relevant offence(s). See United States Sentencing Commission, Op cit n418, § 8C2.5(f)(3)(B).

⁴⁴⁸ Op cit n418, § 8B2.1(a).

through which those employees with operational responsibility for AML/CTF controls can report to senior management on their effectiveness.

Interestingly, whilst the drafting of the *Organizational Sentencing Guidelines* suggests that defendant institutions may limit their AML/CTF legal risk through the implementation of a compliance and ethics program, it appears that in practice few institutions actually receive full credit for their programs. Of the 108 institutions fined for money laundering and other corporate crimes under the *U.S. Sentencing Guidelines* during 2006, not a single one earned a reduction in its culpability score for having an effective compliance program in place.

According to the *'Culpability Factors'* table contained in the U.S. Sentencing Commission's *Sourcebook of Federal Sentencing Statistics (2006)*, the U.S. courts did not consider any of the 108 institutions to have an effective compliance and ethics program in place at the time their criminal conduct occurred.⁴⁴⁹ Evidently, whilst U.S. laws make provision for sentence reductions in cases where an effective compliance program had been implemented, sentencing statistics indicate that qualifying for those reductions may prove to be particularly difficult for defendant institutions.

5.4 Conclusion

Clearly, the most reputationally prudent way for an institution to manage its AML/CTF legal risk is to simply adopt an avoidance strategy and comply with all relevant AML/CTF laws and regulations. However, whether this is also the most cost efficient way for an institution to address its risk is perhaps debatable. Whilst a number of commentators and banking professionals have claimed that non-compliance with AML/CTF laws can lead to significantly steep (if not, financially crippling) monetary penalties, the analysis contained in **Chapter 3** of this thesis contends that the penalties actually imposed upon institutions for AML/CTF compliance failures often appear to be minimal and relatively infrequent. Thus, the adoption of an avoidance strategy may not always be the most cost effective risk management avenue for an institution.

⁴⁴⁹ United States Sentencing Commission, *Sourcebook of Federal Sentencing Statistics* (2006) Table 54 http://www.ussc.gov/ANNRPT/2006/SBTOC06.htm at 10 October 2007.

Whilst it is difficult to accurately pinpoint the costs associated with the design and implementation of risk-based controls, it appears to be well accepted that full legislative compliance with AML/CTF laws will be very costly for some institutions⁴⁵⁰ (especially those operating in more developed AML/CTF regimes and subject to a greater number of compliance obligations). Further, as evidenced by the industry surveys periodically conducted by international accounting firm KPMG, it appears that in many jurisdictions the cost of AML/CTF compliance has risen substantially over the past few years.

Thus, whilst some institutions may take the view that the potential ramifications associated with an AML/CTF compliance failure make a compelling case in favour of an avoidance risk management strategy, others may believe that the costs associated with achieving AML/CTF compliance are considerably more than the penalties likely to be imposed upon them for non-compliance. This is particularly so given the apparent reluctance of many regulatory authorities to pursue formal enforcement proceedings, and the number of retroactive risk management strategies available to a non-compliant institution following an AML/CTF compliance failure.

Putting the issue of cost to one side, because it clearly requires further research and analysis beyond this thesis, there seems little doubt that the implementation of appropriate risk-based systems and controls may enable an institution to avoid the time and expense associated with defending a lengthy formal enforcement action, paying a significant fine or civil monetary penalty, and/or rebuilding a tarnished corporate reputation. In most jurisdictions, regulatory authorities recognise that even the most carefully implemented AML/CTF systems and controls may be exploited by money launderers and terrorism financiers. Accordingly, even where an institution's risk management strategy has failed and an AML/CTF compliance failure has arisen, evidence of its efforts to meet legislative compliance may nevertheless limit its overall level of AML/CTF legal risk. Such evidence may rebut claims that it did not genuinely attempt to comply with AML/CTF legislation and even, in some cases, enable it to avoid formal enforcement proceedings altogether. Further, in circumstances where an

⁴⁵⁰ Mainelli, M., 'Anti-Anti Money Laundering, Feed-Back or Fed-Up' (2005) 6(4) *Journal of Risk Finance* 386.

institution has been successfully prosecuted for its AML/CTF offences, such evidence may minimise the quantum of any penalties ultimately imposed upon it.

Undoubtedly, there will be some instances where evidence of previously implemented AML/CTF systems and controls will not be, in and of itself, sufficient to significantly reduce an institution's AML/CTF legal risk. In such cases, it may be that the institution needs to self-report its AML/CTF compliance failures, provide evidence of its internal AML/CTF control environment, and actively demonstrate that it is prepared to undertake sufficient remedial actions. In the case of AML/CTF legislative breaches that constitute a criminal offence, taking such steps may pave the way for a deferred or non-prosecution agreement, and allow an institution to avoid the legal costs, reputational damage and penalties that may stem from a corporate prosecution.

It should be noted however that an institution will not always be capable of mitigating its AML/CTF legal risk following the identification of an AML/CTF compliance failure. As demonstrated by the case studies contained in the following two Chapters of this thesis, regulatory authorities will typically elect to exercise their formal enforcement powers in circumstances where an institution's AML/CTF deficiencies are pervasive, unresolved or of serious regulatory concern. Thus, although the last few years have seen several institutions escape criminal culpability by voluntarily making a large settlement payment and instituting sweeping internal reforms, 'prevention' may be better than 'cure' as far as AML/CTF compliance is concerned. Even where an institution breaches AML/CTF legislation and manages to limit its AML/CTF legal risk through the adoption of a mitigation strategy, it may nevertheless incur considerable reputational and financial damage. Whilst the avoidance of formal enforcement proceedings is likely to be a desirable regulatory outcome for an institution, it will not necessarily ensure that they remain unscathed in the aftermath of an AML/CTF compliance failure.

Chapter 6

Riggs Bank: A Criminal Exception to Civil Regulation

"Banking establishments are more dangerous than standing armies" - Thomas Jefferson

6.1 Introduction

Since it first came to the attention of regulatory officials and members of the public, Riggs Bank has become a glorified textbook case study in relation to many of the AML/CTF challenges facing financial institutions in the wake of September 11 and the enactment of the USA PATRIOT Act. Viewed by many as a 'poster child' for non-compliance with AML/CTF legislation, the bank provides a practical demonstration of the possible legal, reputational and financial consequences stemming from a series of AML/CTF compliance failures. Further, it showcases the potential limits on the ability of banking regulators to enforce AML/CTF compliance, and raises a number of issues relating to international cooperation around the investigation and prosecution of money laundering offences. 452

Whilst several Chapters of this thesis have already discussed the propensity for regulatory authorities to pursue AML/CTF compliance through the use of civil enforcement tools, Riggs Bank highlights the circumstances in which such authorities may be prepared to initiate criminal enforcement proceedings against a non-compliant institution. It demonstrates how an institution that fails to manage its AML/CTF legal risk via a risk avoidance or risk mitigation strategy, can face a broad spectrum of legal consequences — including criminal prosecution, civil enforcement actions, foreign lawsuits, shareholder derivative suits, and other civil claims filed by related parties. Essentially, the case of Riggs Bank provides financial institutions with a clear roadmap of what *not* to do in terms of managing and mitigating their ongoing risk — both prior to, and following, the commission of a money laundering/terrorism financing offence and/or an AML/CTF compliance failure.

⁴⁵¹ 'The Pinochet Affair: A Landmark Case Study on AML Controls' (2005) 16(4) Money Laundering Alert

^{1.} ⁴⁵² Ibid.

This Chapter uses Riggs Bank as an in-depth case study to demonstrate how a string of public and persistent AML/CTF compliance failures can transform an institution once considered to be "the most important bank in the most important city in the world", 453 into the most criticised bank in the most unforgiving city in the world. It seeks to:

- detail Riggs Bank's most highly publicised AML/CTF compliance failures, and the damage it suffered as a result of those failures;
- highlight the risks that the bank faced and, in certain circumstances, inflamed as a result
 of its lax AML/CTF controls and its refusal to execute any of the risk mitigation
 strategies outlined in Chapter 5 of this thesis;
- address the way in which an institution's non-compliance with AML/CTF legislation may expose it to a range of unforeseen civil claims, as well as formal regulatory actions; and
- outline the potential limitations on the ability of AML/CTF regulators to monitor and enforce compliance in risk-based regimes.

6.2 Corporate war crimes: Terrorism and corruption

As previously discussed, money laundering and terrorism financing became critical concerns for the U.S. government following the events of September 11. Whilst money laundering had previously received some government attention courtesy of legislation such as the *MLCA*, the 2001 terrorist attacks were the catalyst for a new, tougher period of AML/CTF regulation. U.S. Congress swiftly introduced the *USA PATRIOT Act* to strengthen the *Bank Secrecy Act* and bolster the country's AML/CTF framework. In doing so, it brought money laundering and terrorism financing into sharper public focus by requiring a range of regulated institutions to develop effective compliance programs, implement a range of associated AML/CTF controls, and screen their customers against lists of suspected terrorists and designated persons.⁴⁵⁴

⁴⁵³ Op cit n42.

Office of the Comptroller of the Currency, Money Laundering: A Banker's Guide to Avoiding Problems (2002) 2 http://www.occ.treas.gov/moneylaundering2002.pdf> at 18 June 2007.

However, despite the enactment of the *USA PATRIOT Act* and the heightened cultural sensitivity surrounding money laundering and terrorism financing, Riggs Bank engaged in gross violations of U.S. AML/CTF laws in the years following the September 11 attacks. Many of these violations specifically related to the bank's handling of funds owned by high profile, foreign customers. It failed (and at times refused) to conduct adequate customer due diligence, monitor the accounts of higher risk customers, and report suspicious transactions carried out in relation to higher risk accounts. As a result, the bank heightened its AML/CTF legal risk, suffered reputational and financial damage, and faced a spate of previously unforeseen civil lawsuits. Most importantly however, it became one of the very few institutions to be criminally pursued for its AML/CTF compliance failures.

6.2.1 Saudi Arabian accounts and the September 11 attacks

Whilst the relationship between the U.S. and Saudi Arabia was already strained, the events of September 11 fuelled the U.S. government's criticism of the Middle Eastern country. The government decried Saudi Arabia's perceived involvement in terrorism and its alleged funding of terrorist organisations through payments disguised as charitable contributions. Spurred on by this criticism, a number of journalists and government officials started to investigate the activities of U.S. financial institutions known to conduct business on behalf of certain Middle Eastern countries. Their analysis ultimately led to the identification of several suspect transactions carried out by Riggs Bank for Saudi Arabian government officials.

Prior to September 11, Riggs Bank provided banking services to most of the foreign embassies located in Washington, including the Royal Embassy of Saudi Arabia. Whilst it had conducted business on behalf of the Saudi Arabian embassy for more than two decades, the terrorist attacks prompted the U.S. House-Senate Joint Intelligence Committee to conduct a formal inquiry into the transactions previously processed by the bank for its Saudi Arabian customers. The results of that inquiry suggested that Riggs Bank might have partially financed the September 11 attacks by facilitating payments from one of its Saudi Arabian customers to the hijackers.

⁴⁵⁵ Prados, A.B., and Blanchard, C.M., *Saudi Arabia: Terrorist Financing Issues* (Congressional Research Service Report for Congress, Washington D.C., 2004) 1.

Unfortunately for Riggs Bank, the findings of the U.S. House-Senate inquiry received widespread public attention after they were published in the November 2002 edition of U.S. magazine *Newsweek*. The magazine accused the institution of assisting one of its customers; Princess Haifa Al-Faisal (**Princess Al-Faisal**), the wife of Saudi Arabia's long-standing U.S. ambassador, to send funds to the September 11 hijackers in the lead-up to the attacks. Despite the fact she was a PEP (or, at the very least, a close associate of a PEP), Aliggs Bank seemingly did little to monitor her accounts and/or mitigate the increased ML/TF risk she represented. Several months before the September 11 attacks, the institution had begun processing a steady stream of USD\$3,500 payments from Princess Al-Faisal to students closely associated with Khalid Almidhar and Nawaf Alhazmi; two of the hijackers responsible for crashing American Airlines Flight 77 into the Pentagon. Also

That said, even if Riggs Bank had subjected Princess Al-Faisal's transactions to greater scrutiny and due diligence, it is unlikely to have identified anything particularly suspicious about them prior to the September 11 attacks. At that time, many Saudi Arabian dignitaries provided financial assistance to students studying in the U.S. Further, consistent with the hallmarks of terrorism financing, the amounts of money involved in the relevant transactions were so small that they are unlikely to have triggered any transaction monitoring alerts. Even if the beneficiaries of Princess Al-Faisal's funds had been screened against terrorist or other sanctions lists, they would not have provided a positive match. They were not yet considered to be terrorists, so the bank's risk-based systems and controls would arguably have been unable to identify the real nature of their activities.

Nevertheless, the speculation surrounding Riggs Bank's potential financing of the September 11 attacks caused reputational damage for the institution and greatly increased its AML/CTF legal risk. Shortly after the *Newsweek* article was published, the F.B.I. launched an investigation into Riggs Bank's embassy accounts, its dealings with Saudi Arabian

⁴⁵⁶ Isikoff, M., '9-11 Hijackers: A Saudi Money Trail?', *NewsWeek*, 22 November 2002 http://www.truthout.org/docs-02/11.26A.newswk.911.htm at 12 December 2006.

⁴⁵⁷ Section 312 of the USA PATRIOT Act articulates that the term applies to senior foreign political figures, their immediate family members and their close associates.

⁴⁵⁸ On cit n456.

officials, and the transactions it conducted on behalf of Princess Al-Faisal. Whilst this investigation ultimately identified a number of instances where the bank failed to report suspicious transactions conducted by its Saudi Arabian customers, failed to find any evidence that Princess Al-Faisal or Riggs Bank intended to funnel money to the September 11 hijackers.

Despite the absence of any positive evidence of terrorism financing, the mere suggestion that Riggs Bank had somehow helped to fund one of the most brazen terrorist attacks ever carried out in the U.S., created further AML/CTF legal risk for the institution. Following the publication of the F.B.I.'s findings, U.S. banking regulators launched their own investigations into whether the bank's poor control environment led to the processing of suspect transactions for other Saudi Arabian political figures. 462 Conducted in early 2003, these investigations uncovered improprieties in relation to more than 150 of the institution's Saudi Arabian accounts. They identified numerous occasions where Riggs Bank failed to adequately screen, monitor the accounts of, and/or properly report the suspicious transactions conducted by, many of its Saudi Arabian customers.

In order to address the institution's various AML/CTF control failures, U.S. regulators issued a cease and desist order requiring the bank to undertake extensive corrective action. Whilst the order gave Riggs Bank an opportunity to contain its reputational damage and mitigate its ongoing AML/CTF legal risk, it was an opportunity the bank did not seize. It continued to process questionable transactions for Saudi Arabian customers and, in doing so, further

Op cit n42. See also King, J., 'FBI Probes Possible Saudi, 9/11 Money Ties', CNN News, 23 November 2002 http://archives.cnn.com/2002/US/11/23/saudi.fbi.911/ at 11 December 2006.

O'Hara, T., 'Riggs Bank Agrees to Guilty Plea and Fine', *The Washington Post* (Washington D.C.), 28 January 2005, A01.

⁴⁶¹ New York State Society of CPA's, Riggs Bank is Sued over 9/11 Attacks (2004)

http://www.nysscpa.org/home/2004/904/2week/article4.htm> at 14 April 2007. See also National Commission on Terrorist Attacks upon the United States, The 9/11 Commission Report (W.W. Norton & Company, New York, 2004) 498. According to that report, there was no evidence "that Saudi Princess Haifa al Faisal provided any funds to the [9/11] conspiracy, either directly or indirectly".

⁴⁶² Op cit n42.

tarnished its corporate reputation, incurred a USD\$25 million civil monetary penalty in May 2004, 463 and left itself exposed to two related civil lawsuits.

6.2.2 The September 11 lawsuits

The damage suffered by Riggs Bank as a result of its association with two of the September 11 hijackers, was undoubtedly drawn out by two civil lawsuits brought against the institution. The first of these law suits; *Vadhan, et al. v. Riggs National Corp., et al.*, 04 Civ. 7281 (RCC) (**the Vadhan Action**), was filed on 10 September 2004 in the U.S. District Court for the Southern District of New York. It involved 2,440 claimants⁴⁶⁴ and sought compensatory, punitive and/or exemplary damages from Riggs Bank on the grounds that its deficient AML/CTF program led to its failure to identify and report the suspicious transactions related to the September 11 terrorist attacks. According to the claimants, the bank's "constant failure to comply with banking oversight laws resulted in funds being forwarded from high risk Saudi Embassy accounts at Riggs Bank to at least two September 11 hijackers". 465

The Vadhan Action ran until June 2005, when PNC Financial Services Group Inc. (PNC), the corporation that had since acquired Riggs Bank, agreed to make a sizeable settlement payment to a September 11 charity. By that time however, the bank had already become embroiled in another case regarding its alleged financing of the September 11 attacks. This lawsuit; Cantor Fitzgerald & Co., et al. v. American Airlines, et al., 04 Civ. 7318, hinged upon almost identical grounds to those asserted in the previous action. Filed on 13 September 2004 in the New York Federal Court, the suit was instituted by several World Trade Centre tenants who sought compensatory, punitive and/or exemplary damages from Riggs National Corp. for the property losses they suffered as a consequence of the

Financial Crimes Enforcement Network, Assessment of Civil Money Penalty in the Matter of Riggs Bank N.A., No. 2004-01 (2004) http://www.fincen.gov/riggsassessment3.pdf> at 2 January 2007.

The action was originally initiated by a general, purported class of persons who suffered physical injury and/or who represented persons killed as a result of the terrorist attacks. However, on 24 March 2005 an amended complaint was filed on behalf of 2,440 specific individuals. See In Re Riggs National Corporation, Notice of Pendency of Class and Derivative Action, Proposed Settlement of Class and Derivative Action, Settlement Hearing and Right to Appear, Court of Chancery for the State of Delaware in and for New Castle County, 14 September 2005, 2.

Simpson, G.R., 'Riggs Bank Is Sued over 9/11 Attacks', *The Wall Street Journal* (New York), 13 September 2004, B.3.

September 11 attacks. Whilst it was conditionally resolved in April 2005 when PNC entered into a Memorandum of Understanding with the claimants, this lawsuit caused Riggs Bank to incur significant legal and consulting fees, and exacerbated the reputational damage it had already suffered during the high-profile Vadhan Action. 466

6.2.3 Corruption, profiteering and a dictatorship

Whilst the F.B.I was reviewing Riggs Bank's handling of various Saudi Arabian accounts, another scandal was emerging regarding the institution's poor oversight of its Equatorial Guinea accounts. Embarrassingly for U.S. regulators though, this scandal was only brought to light following yet another media exposé.

In January 2003, the *Los Angeles Times* published claims that Riggs Bank had facilitated suspicious transactions on behalf of several government officials from Equatorial Guinea. According to the newspaper, these transactions had gone largely unmonitored, undocumented and unreported by the institution because one its executives, Mr Simon P. Kareri (**Mr Kareri**), maintained a close relationship with the leader of Equatorial Guinea, Teodoro Obiang Nguema Mbasago (**Mr Obiang**). In addition to being the dictator of Equatorial Guinea, a politically tumultuous country plagued by corruption, Mr Obiang was internationally renowned for committing various human rights abuses.

Whilst the *USA PATRIOT Act* does not prohibit financial institutions from on-boarding PEPs such as Mr Obiang, 31 U.S.C. § 5318(i) requires them to conduct enhanced due diligence on such individuals during the length of their customer relationship. Typically, this enhanced due diligence will involve collecting further information to identify/verify the nature of a PEP's business activities, available income and assets, and overall financial position. Fundamentally, its purpose is to determine if the funds used by a PEP to conduct financial transactions potentially stem from corruption or other illicit activities.

⁴⁶⁶ Op cit n464.

⁴⁶⁷ Ibid.

The U.S. Department of State, as well as various non-governmental and human rights groups, had previously cited the government of Equatorial Guinea as one of the most corrupt in the world.

If Riggs Bank had properly conducted enhanced due diligence with respect to Mr Obiang's accounts and transactional activities, it might have noticed a number of highly suspicious transactions conducted on his behalf by Mr Kareri. Indeed, whilst he was responsible for overseeing the treasury accounts of the Equatorial Guinea government, and the private accounts of Mr Obiang and a number of his associates, Mr Kareri assisted his customers to launder money by:

- carrying around large amounts of money in suitcases for them;⁴⁶⁹
- enabling them to make cash transfers to offshore shell corporations; and
- allowing certain officials to wire more than USD\$35 million in oil receipts to companies controlled by them and their family members.⁴⁷⁰

However, whilst Mr Kareri was personally responsible for processing many suspect transactions, Riggs Bank was wilfully blind to evidence that suggested it might have been laundering the proceeds of corruption for government officials from Equatorial Guinea. Although millions of dollars were funnelled out of the government's accounts, and more than USD\$13 million was deposited into such accounts between 2000 and 2003 inclusive, ⁴⁷¹ the institution failed to scrutinise and/or report those transactions. This is despite the fact that many of the deposits into its Equatorial Guinea accounts were mysteriously deemed to be "gifts" from large U.S. oil companies.

Following the oil boom experienced by Equatorial Guinea at the turn of the century, U.S. oil companies such as Exxon Mobil, Amerada Hess and Marathon Oil, developed close relationships with Mr Obiang and his government. According to some sources, the companies formed business ventures with Equatorial Guinea government officials, hired companies associated with Mr Obiang, and rented property owned by officials and their

⁴⁶⁹ According to a U.S. Senate report on Riggs Bank's activities, on one occasion Mr Kareri packed approximately USD\$3 million received from Equatorial Guinean leaders into suitcases, and walked the money right out of the bank. See O'Brien, T.L., Op cit n42.

⁴⁷⁰ See Simpson, G.R., 'Senate Panel Blasts Riggs Bank; Scathing Report Claims Corruption Flourished Amid Inadequate Oversight', *The Wall Street Journal* (New York), 15 July 2004, A.3.

World-Check, Reputation Damage: The Price Riggs Paid 3 http://www.world-check.com/media/d/content whitepaper reference/whitepaper-3.pdf> at 14 December 2006.

families. ⁴⁷² Further, a number of them made large payments – typically referred to as "gifts", ⁴⁷³ and sometimes in increments as high as USD\$250,000 – into accounts held by Equatorial Guinea officials and their relatives. However, despite evidence that these payments may have related to profiteering and corruption, ⁴⁷⁴ Riggs Bank turned a blind eye to their suspicious nature and potential illegality under the *U.S. Foreign Corrupt Practices Act of 1977* (15 U.S.C. §§ 78dd-1, et seq.). This is perhaps largely attributable to the fact that the government of Equatorial Guinea had by that time become the bank's largest and most important customer, with accounts totalling more than USD\$700 million. ⁴⁷⁵

Whilst Riggs Bank subsequently admitted criminal liability and incurred a USD\$16 million fine for its failure to monitor and report the suspicious activities undertaken by Equatorial Guinea officials, this did not occur until two years after the bank's questionable relationship with Mr Obiang was uncovered by reporters. In the meantime, Riggs Bank suffered significant political backlash in relation to its lax oversight of Equatorial Guinea accounts. Perhaps cemented by the strong public reaction to the institution's activities and the indictment of Mr Kareri for money laundering and other charges, 476 many U.S. government officials sharply criticised the bank's AML/CTF compliance failures. One member of the U.S. Senate even publicly declared that the institution's relationship with Mr Obiang was "abominable". Whilst this and similar comments caused Riggs Bank reputational damage, the institution still refused to take any steps to avoid or mitigate the AML/CTF legal risk attached to its dealing with PEPs from Equatorial Guinea.

⁴⁷² Blum, J., 'Equatorial Guinea, USA: US Oil Firms Entwined in Equatorial Guinea Deals', *The Washington Post* (Washington D.C.), 9 September 2004

http://www.globalpolicy.org/nations/launder/regions/2004/09090ilfirms.htm at 15 April 2008.

According to a U.S. Senate Report dated 14 July 2004, at least 60 of the accounts maintained at Riggs Bank for Equatorial Guinean officials contained supposed "gifts" made by U.S. oil companies. See Riggs Bank N.A., (Written statement before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs of the United States Senate, Washington D.C., 15 July 2004) 8.

474 Op cit n470.

⁴⁷⁵ Op cit n460.

⁴⁷⁶ Stemming from an internal Riggs Bank investigation which revealed that Mr Kareri had diverted funds from two Equatorial Guinea accounts for his own benefit, on 3 June 2005 Mr Kareri and his wife were indicted on 27 counts of conspiracy to defraud the bank and other related charges such as bank fraud, wire fraud, money laundering and income tax evasion.
477 On cit n42.

6.2.4 Civil penalties, civil lawsuits and stranded customers

Owing to the fact that Riggs Bank's non-compliance with U.S. AML/CTF legislation was ongoing and potentially harmful to the public and other financial institutions. 478 on 13 May 2004 the OCC imposed a USD\$25 million civil monetary penalty upon the bank.⁴⁷⁹ Issued concurrently with a USD\$25 million penalty assessed by FinCEN. 480 the penalty specifically related to the institution's failure to:

- monitor and report more than two dozen large and unusual transactions (including "tens of millions of dollars in cash withdrawals, international drafts... and numerous sequentially numbered cashiers' checks "481") relating to its Saudi Arabian and Equatorial Guinean customers: 482 and
- meet its obligations under 31 U.S.C. § 5318(h)(1) by designing "a program tailored to the risks of its business that would ensure appropriate reporting... and responding to classic 'red flags' of suspicious conduct". 483

Given Riggs Bank's size and profit margins, the USD\$25 million civil monetary penalty imposed upon it was particularly significant. Indeed, the institution's combined earnings for 2002 and 2003 were only USD\$14 million. 484 Thus, the penalty represented a heavy price for the institution to pay – both in terms of its bottom line and its reputation. However, it is arguable that its imposition should not have come as a surprise for the bank. In accordance with the commentary contained in earlier Chapters of this thesis, prior to the invocation of the civil monetary penalty U.S. regulatory authorities had attempted to address Riggs Bank's compliance failures through the use of less damaging, more cooperative means.

See Assessment of Civil Money Penalty in the Matter of No. 2004-01, United States of America Department of the Treasury, Financial Crimes Enforcement Network v Riggs Bank N.A, 13 May 2004, 8. Office of the Comptroller of the Currency, Consent Order of Civil Money Penalty in the Matter of Riggs Bank N.A. (2004) http://www.occ.treas.gov/ftp/eas/EA2004-44.pdf at 5 January 2007.

In accordance with the 'Consent to the Assessment of Civil Money Penalty' entered into between Riggs Bank and FinCEN on 13 May 2004, both the FinCEN and OCC penalties were to be satisfied by one payment of USD\$25 million to the Department of the Treasury.

⁴⁸¹ Office of the Comptroller of the Currency, OCC Assesses \$25 Million Penalty against Riggs Bank N.A. (2004) http://www.occ.treas.gov/toolkit/newsrelease.aspx?Doc=5AOFP8K.xml at 20 December 2006. Boustany, N., and O'Hara, T., 'After Riggs, Embassy Accounts Can't Find a Home', The Washington Post (Washington D.C), 10 June 2004 http://www.washingtonpost.com/wp-dyn/articles/A29674- 2004Jun9.html> at 8 December 2006.

483 Op cit n478.

⁴⁸⁴ Op cit n460.

On 16 July 2003, almost a year before Riggs Bank was penalised USD\$25 million, the institution and the OCC entered into a comprehensive Consent Order (**the July 2003 Consent Order**). Under this order, the institution agreed to maintain a Board-level compliance committee, identify and monitor high-risk transactions, implement written policies/procedures, and have its *Bank Secrecy Act* compliance independently reviewed. Whilst Riggs Bank did take some steps towards meeting the requirements of the July 2003 Consent Order, ⁴⁸⁵ its obligations remained largely unfulfilled and on 2 March 2004, the OCC and FinCEN advised the institution that its persistent disregard for the order would result in a sizeable civil monetary penalty. ⁴⁸⁶

Ignoring regulators' repeated requests for corrective action not only exposed Riggs Bank to a considerable financial penalty, but also heightened its AML/CTF legal risk and left it vulnerable to civil lawsuits waged by unhappy shareholders. On 7 April 2004, a shareholder derivative action; ⁴⁸⁷ Horgan v. Allbritton, No CA 370-N (Del. Ch. filed Apr. 7, 2004) (the Horgan Action), was filed in New York against a number of Riggs Bank's officers and directors. ⁴⁸⁸ Citing the bank's contravention of the July 2003 Consent Order and the USD\$25 million civil monetary penalty imposed upon it in May 2004, the claimants held that by failing to:

- conduct appropriate due diligence with respect to the institution's Middle Eastern and
 Equatorial Guinea customers, and
- adequately supervise the institution's compliance with AML/CTF legislation; Riggs Bank's officers and directors breached their fiduciary duties of loyalty, honesty and care, and caused a waste of corporate assets. To compensate the bank for the losses it

⁴⁸⁶ United States Senate Permanent Subcommittee on Investigations, *Money Laundering and Foreign Corruption: Enforcement and Effectiveness of the Patriot Act* (Supplemental Staff Report on U.S. Accounts used by Augusto Pinochet, Washington D.C., 2005).

⁴⁸⁵ For instance, it formed a Board-level *Bank Secrecy Act* Compliance Committee in April 2003, launched more than 20 new programs to improve the detection and reporting of suspicious activities in June 2003, and rolled out a new technology platform in September 2003.

These civil lawsuits arise when shareholders launch an action on behalf of their corporation, seeking damages from parties allegedly causing harm to it. As discussed in **Chapter 4** of this thesis, shareholder derivative suits are waged against corporate officers or directors accused of breaching their fiduciary duties to shareholders vis-a-vis the corporation.

These included Joe L. Allbritton, Robert L. Allbritton, J. Carter Beese, Jr., Charles A. Camalier, Timothy C. Coughlin, Lawrence I. Hebert, Steven B. Pfeiffer, Robert L. Sloan, Jack Valenti, William L. Walton and Eddie N. Williams.

allegedly sustained as a result of the directors' breaches of fiduciary duties, the Horgan Action sought a disgorgement of the their salaries, declaratory and injunctive relief, and additional monetary damages.⁴⁸⁹

However, this action was not the only civil lawsuit Riggs Bank ultimately faced as a consequence of its non-compliance with U.S. AML/CTF legislation. The Horgan Action prompted a number of similar shareholder derivative actions to be launched against the bank, including:

- Dickler v. Allbritton, et al., Civil Action No. 04-0002978, filed on 17 April 2004 in the Superior Court of the District of Columbia; and
- Labaton v. Allbritton, et al., Civil Action No. 404-N, filed on 28 April 2004 in the same court. 490

Whilst these shareholder derivative suits caused Riggs Bank financial and reputational damage, the negative press coverage they attracted also impacted the embassies of many African and South American countries. Riggs Bank dominated a niche area of embassy banking and following the widespread publication of its USD\$25 million civil monetary penalty, there were few financial institutions equipped – or prepared – to take on the 100+ embassy clients in need of alternative banking arrangements. In fact, these foreign embassies found it so difficult to secure new banking arrangements that the U.S. Department of State sought regulatory assistance. In the wake of the Riggs Bank scandal, it appears that many U.S. institutions assessed their embassy banking businesses and determined that the benefits attached to offering such services, did not justify the increased ML/TF risk they carried and the heightened AML/CTF legal risk they attracted.

⁴⁸⁹ Op cit n464.

The claims involved with this lawsuit were so similar to those alleged in the Horgan Action that the two cases were consolidated on 21 May 2004 under the title *In re Riggs National Corporation Litigation*, Consolidated Case No. 370-N.

⁴⁹¹ Op cit n482.

6.3 Dealings with Pinochet

The ML/TF risk Riggs Bank assumed by providing banking services to PEPs, did not begin and end with political figures from Saudi Arabia and Equatorial Guinea. The institution also placed itself at significant reputational, financial and legal risk by proactively seeking out the business of General Augusto Pinochet Ungarte (**General Pinochet**); a Chilean military leader accused of human rights abuses, corruption, arms sales and drug trafficking.

Although official Riggs Bank documentation states that General Pinochet and his wife became customers of the bank in 1994, 492 evidence suggests that the couple actually started dealing with the institution as early as 1981, when General Pinochet opened several accounts using the aliases "Daniel Lopez" and "Jose Ramon Ungarte". In and of itself, there was nothing illegal about opening these accounts for General Pinochet and/or providing him with banking services. However, Riggs Bank violated U.S. AML/CTF laws by:

- accepting millions of dollars in deposits from General Pinochet without conducting any due diligence in relation to their source and/or reporting such transactions; and
- assisting General Pinochet to hide millions of dollars in suspect funds in 28 offshore
 accounts and accounts with altered names⁴⁹³ even after he was detained on criminal
 charges and courts in both Spain and Chile issued orders freezing his assets.

In July 1996, General Pinochet was indicted in Spain on charges of genocide, terrorism and the torture of Spanish citizens. ⁴⁹⁴ Nevertheless, Riggs Bank continued to provide him with banking services – even establishing two offshore shell corporations; Ashburton Co. Ltd.

⁴⁹² According to an internal Riggs Bank memorandum dated 3 November 1994, several bank officials travelled to Chile in October 1994 to offer the institution's personal banking services to General Pinochet and other officers in Chile's military. Their trip was successful and by 2002, Riggs Bank had combined deposits and loans in Chile of more than USD\$100 million.

⁴⁹³ 'Pinochet's Web of Bank Accounts Exposed', *Guardian Unlimited*, 16 March 2005 http://www.guardian.co.uk/pinochet/Story/0.,1488929,00.html at 17 December 2006. See also Lopez, J.C., 'Pinochet 'Used Wide Bank Network', *CNN News*, 16 March 2005

http://edition.cnn.com/2005/WORLD/americas/03/16/pinochet.funds/ at 12 December 2006.

494 O'Hara, T., and Day, K., 'Riggs Bank Hid Assets of Pinochet, Report Says', *The Washington Post* (Washington D.C.), 15 July 2004 http://www.washingtonpost.com/wp-dyn/articles/A50222-2004Jul14.html at 24 December 2006.

(**Ashburton**) and Althorp Investment Co. Ltd. (**Althorp**),⁴⁹⁵ to help him disguise and hide his ownership of certain funds from the Spanish authorities. Seemingly, Riggs Bank's executives believed that the heightened risks attached to doing business with General Pinochet, paled in comparison to the benefits associated with maintaining his customer relationship. Even after he was again indicted for human rights violations in Chile on I December 2000, Riggs Bank continued to funnel money through General Pinochet's corporate accounts without filing any Suspicious Activity Reports.

Though the institution placed itself at considerable AML/CTF legal risk by opening – and then failing to monitor – the Ashburton and Althorp accounts, this risk was only heightened by the bank's deliberate attempts to conceal its relationship with General Pinochet from U.S. regulatory authorities. In 2000, when the OCC asked Riggs Bank to disclose all the accounts it held for political figures, the information ultimately provided by the bank omitted any reference to the numerous accounts it maintained for General Pinochet. The institution had a history of trying to obscure its dealings with General Pinochet (by changing his name on bank records⁴⁹⁶ and simply referring to him as "a retired professional" who held a "high paying position in public sector for many years")⁴⁹⁷ and as such, the failure to disclose his accounts was presumably no oversight.

Even as late as 2002, Riggs Bank was still trying to obscure its dealings with General Pinochet. When, during the course of a regulatory review, the OCC identified a number of suspicious accounts seemingly held by General Pinochet, the bank attempted to close the accounts before officials could conduct any in-depth examination of them. However, the institution's dealings with the former Chilean official – and its related AML/CTF compliance failures – were inevitably uncovered, and were responsible for the imposition of a USD\$16 million criminal fine upon the bank on 27 January 2005. Whilst U.S. regulatory

⁴⁹⁵ Riggs Bank N.A., (Written statement before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs of the United States Senate, Washington D.C., 15 July 2004) 7.
⁴⁹⁶ Op cit n42.

⁴⁹⁷ Op cit n494.

⁴⁹⁸ Op cit n471, 2.

⁴⁹⁹ United States Department of Justice, Riggs Bank Enters Guilty Plea and Will Pay \$16 Million Fine for Criminal Failure to Report Numerous Suspicious Transactions, Press Release (Press Release, 27 January 2005).

officials had started to rely more heavily upon cooperative enforcement outcomes by that time, they seemingly believed that Riggs Bank's deliberate attempts to evade regulatory oversight and its persistent disregard for the OCC's requests, justified more aggressive enforcement.

6.3.1 Repercussions in Spain

The Spanish inquisition of Riggs Bank begins

Many of Riggs Bank's legal woes can be traced back to 1996, when a group of lawyers representing the President Allende Foundation (an organisation established for victims of General Pinochet's regime) asked a Spanish judge, Judge Garzon, to accept jurisdiction to criminally prosecute General Pinochet for terrorism, genocide and the torture of hundreds of Spaniards. Under Spanish criminal laws that enable anyone in the world to be tried for the genocide or torture of Spanish citizens, the claim was successful and Judge Garzon agreed to accept such jurisdiction.

Two years after criminal charges were laid against General Pinochet in Spain, he was arrested in London and Judge Garzon issued two orders demanding that all his assets (including all bank accounts controlled by him and his immediate family members) be frozen. These orders had extraterritorial application and were intended to provide a guarantee that if General Pinochet was subsequently convicted of human rights abuses by the Spanish courts, victims of his regime could receive indemnity payments. However, despite their extraterritoriality, Riggs Bank ignored Judge Garzon's orders.

During 2004, when the Spanish proceedings against General Pinochet were still on foot, the U.S. Senate's Permanent Subcommittee on Investigations released a report claiming that from 1994 to 2002 inclusive, Riggs Bank held more than USD\$4-8 million in accounts for General Pinochet. On 19 July 2004, shortly after the release of this report, lawyers acting for the President Allende Foundation petitioned the Central Investigative Court No. 5 of the Audiencia Nacional in Spain (**Spanish Central Investigative Court**), to extend the criminal

These Spanish writs were issued on 19 October 1998 and 10 December 1998 respectively.

complaint against General Pinochet to include the alleged concealment of assets and money laundering offences carried out by seven Riggs Bank executives. 501 Given that Spanish law does not enable corporations to be tried for criminal offences, it was necessary for prosecutors to pursue the institution's officers and directors individually.

According to the lawyers acting for the President Allende Foundation, the seven Riggs Bank executives needed to be held criminally responsible for their deliberate violation of Judge Garzon's orders, 502 and their attempts to "delay, hamper and impede the efficacy of the embargo, blockage and deposit of the bank account balances which Augusto Pinochet held in Riggs Bank... "503 The Spanish Central Investigative Court agreed and on 16 September 2004 the pre-existing criminal action against General Pinochet was expanded to include the executives. According to the court, there was some evidence to indicate that the seven executives entered into a "fraudulent meeting of minds" with General Pinochet to withdraw and hide millions of dollars held for him in multiple Riggs Bank accounts.

Whilst the bank's executives might have foreseen the regulatory scrutiny that their dealings with General Pinochet would attract in the U.S., it is unlikely that they ever considered the AML/CTF legal risk that their activities could attract in other jurisdictions. In the process of establishing and fostering a customer relationship with the former Chilean military leader, it is doubtful that they anticipated that their institution's AML/CTF compliance failures could one day see them personally facing criminal charges in a foreign jurisdiction. Indeed, it is improbable that the extraterritorial reach of Spain's human rights and criminal laws, and Riggs Bank's limited potential criminal responsibility in Spain, would ever have factored into the executives' decision to accept General Pinochet's business.

Although Riggs Bank could not be criminally prosecuted in Spain for its handling of General Pinochet's funds, it nevertheless faced civil liability for its related AML/CTF compliance failures. In petitioning the Spanish Criminal Investigative Court to criminally prosecute the

⁵⁰¹ Under Spanish municipal law, private citizens can initiate criminal proceedings.

See Proceedings Summary 19/1997 C, Separate Proceeding III. Operation Condor for the crimes of terrorism and genocide, in the Central Investigative Court No 5, Madrid, before Garcia Gutierrez S/N on 16 September 2004, 2. Op cit n502, 1.

seven Riggs Bank executives, the lawyers for the President Allende Foundation requested that both Riggs National Corp. and Riggs Bank be added to the criminal action as Defendants with subsidiary civil liability.⁵⁰⁴ The motivations behind this request were likely twofold:

- symbolic because the addition of the two companies would put other foreign financial
 institutions on notice that their non-compliance with extraterritorial Spanish court orders
 would not be tolerated; and
- strategic because the addition of the two companies would ensure that if the officers
 and directors were cleared of criminal liability and/or unable to satisfy any monetary
 penalty assessed against them, the President Allende Foundation could still seek
 compensation from the deep corporate pockets of Riggs National Corp. and Riggs Bank.

Again, the lawyers' request was upheld and the case against General Pinochet and the seven executives was extended to include Riggs Bank. The Spanish court reasoned that the extension of the action was indissolubly linked to the Spanish investigation of General Pinochet, and that the concealment of General Pinochet's assets would not have existed *but* for the orders made previously by a Spanish court. Accordingly, the jurisdiction of the Spanish legal system to deal with the bank was protected by the principle of universal criminal justice and *Article 24.3* of the country's *Organic Law of Judicial Power*. ⁵⁰⁵

Riggs Bank pays for Pinochet

In order to have the charges against Riggs Bank's officers and directors dropped, Riggs National Corp. entered into a settlement agreement with the President Allende Foundation on 27 January 2005. Under this agreement, USD\$9 million was to be paid to the Foundation in exchange for the abandonment of all criminal charges against the executives and all civil charges against Riggs Bank. Whilst USD\$8 million of this settlement amount was to be paid by Riggs Bank, the remaining USD\$1 million was to be paid by two of the individual

⁵⁰⁴ Op cit n502.

⁵⁰⁵ Op cit n502, 2.

O'Hara, T., 'Allbrittons, Riggs to Pay Victims of Pinochet', *The Washington Post* (Washington D.C.), 26 February 2005 http://www.washingtonpost.com/wp-dyn/articles/A53805-2005Feb25.html at 18 December 2006.

Defendants; Joseph L. Allbritton, a former CEO of Riggs Bank, and Robert L. Allbritton, the institution's controlling shareholder (the Allbrittons). 507

In addition to enabling Riggs Bank to avoid civil liability in Spain, the USD\$9 million settlement package created two important milestones. Firstly, it marked the first time that any individual or institution (i.e. other than the Chilean Government) was legally required to compensate the victims of General Pinochet's reign. 508 Secondly, and perhaps more importantly, given that the agreement required the Allbrittons to make a payment to the President Allende Foundation, it also marked the first and only time that any Riggs Bank executive was held personally accountable for the institution's AML/CTF compliance failures.

Despite the settlement agreement and the mitigation of its AML/CTF legal risk, Riggs Bank continued to suffer reputational damage in the aftermath of the Spanish court case – not only because of its customer relationship with a man charged with human rights abuses, but because of its unrelenting refusal to apologise for dealing with him. In stark contrast to nearly every other major corporate scandal in recent times, Riggs Bank never attempted to limit its reputational damage by releasing a public statement expressing regret for hiding or laundering General Pinochet's funds. This is somewhat peculiar given that the settlement presumably represented an attempt by Riggs Bank to contain the AML/CTF legal risk, financial risk and reputational risk stemming from the Spanish lawsuit and its own handling of General Pinochet's funds.

6.3.2 Repercussions in the U.S.

Whilst a spokesperson for Riggs Bank held that the USD\$9 million settlement agreement reached in the Spanish lawsuit essentially "put the matter behind the institution", 509 this was only the case in terms of the bank's ongoing AML/CTF legal risk in Spain. The

Landau, S., and Anderson, S., Blood Deposits and the Riggs Bank: Pinochet's Bank Finally Pays Up (2005) Counterpunch http://www.counterpunch.org/landau03122005.html at 7 December 2006. ⁵⁰⁸ Op cit n506. ⁵⁰⁹ Ibid.

repercussions stemming from its dealings with General Pinochet continued to reverberate in the U.S. long after the Spanish action had concluded. Evidently, the bank's involvement in such a significant and highly publicised piece of foreign litigation only increased its AML/CTF legal risk back in the U.S.

Whilst the Spanish action was before the courts, Riggs Bank was facing criminal enforcement proceedings back in the U.S. with respect to its dealings with General Pinochet. Presumably in an effort to avoid protracted legal proceedings, exorbitant fees and an excessive financial penalty, the bank also tried to swiftly conclude this action. On 27 January 2005 (i.e. the very same day it agreed to pay USD\$9 million to victims of General Pinochet), it pleaded guilty to a single felony count of violating the *Bank Secrecy Act*. Representatives for the institution conceded that it had failed to file Suspicious Activity Reports in relation to transactions undertaken by General Pinochet and several Equatorial Guinea officials, ⁵¹⁰ and conduct sufficient due diligence around the source of the funds deposited into the accounts held by General Pinochet and other high-risk customers. ⁵¹¹

The institution's decision to plead guilty and accept a USD\$16 million criminal fine for its reporting failures, is somewhat unusual considering that U.S. banks pursued for non-compliance with AML/CTF laws have typically preferred to enter into deferred or non-prosecution agreements rather than admit any wrongdoing. However, given Riggs Bank's long-standing AML/CTF compliance failures and the seriousness of its legislative violations, some commentators have speculated that the U.S. Department of Justice insisted on a guilty plea in this case. Allowing the institution to avoid criminal culpability through such an agreement would presumably have undermined the penalty provisions in U.S. AML/CTF legislation, and sent a strong message to other institutions that even the most blatant AML/CTF compliance failures could be addressed through civil enforcement actions.

Wilke, J.R., and Pacelle, M., 'Riggs Is Set to Plead Guilty to Crime', *The Wall Street Journal* (New York), 26 January 2005 http://tania.blythe-systems.com/pipermail/nytr/Week-of-Mon-20050124/012447.html at 13 December 2006.

Blank Rome LLP, Riggs Bank, N.A. Agrees to Plead Guilty to Bank Secrecy Act Violations and Pay \$16 Million Fine (2005) http://www.blankrome.com/index.cfm?contentID=37&itemID=382> at 12 December 2006.

⁵¹² lbid.

During Riggs Bank's formal hearing in the U.S., District Judge Ricardo M. Urbina (**Judge Urbina**) expressed that he was sceptical of the bank's guilty plea. He sharply criticised the institution for being "a greedy corporate henchman of dictators and their corrupt regimes", ⁵¹³ and was so cynical of the motivations underpinning its guilty plea that he only provisionally accepted it. His Honour highlighted Riggs Bank's undeniable history of AML/CTF deficiencies, and its reputation for placing profits before legislative compliance. Throughout the action, Judge Urbina continued to increase the institution's reputational damage by making scathing remarks about its refusal to comply with U.S. AML/CTF laws, and openly questioning whether the USD\$16 million fine imposed upon it would simply be regarded as "a business expense" for the bank.

Judge Urbina's comments regarding the magnitude of Riggs Bank's penalty raise an interesting point about AML/CTF legal risk. It has previously been noted in Chapter 3 of this thesis that an institution's AML/CTF legal risk is often proportionate to the aggressiveness with which AML/CTF laws are enforced in the jurisdictions where it operates. However, this statement should perhaps be qualified as the USD\$16 million fine imposed upon Riggs Bank demonstrates that an institution's AML/CTF legal risk is not only a product of the ferocity which with AML/CTF compliance is enforced, but also of the quantum of the penalties used to enforce compliance. Even if a particular government were to enact and enforce stringent AML/CTF laws, the AML/CTF legal risk faced by financial institutions would still be quite low if the penalties for non-compliance were inconsequential or insignificant compared to the potential benefits of contravention. Given the profits an institution can generate as a result of serving higher risk customers and facilitating money laundering activities – particularly in areas of their business such as Private Banking, where the funds involved may be significant – the potential penalties attached to such activities must be sizeable enough to deter an institution from simply assuming an acceptance risk management strategy.

^{&#}x27;Judge: Riggs was 'Henchman of Dictators' (2005) Washington Business Journal http://www.bizjournals.com/washington/stories/2005/03/28/daily13.html at 4 January 2007.

Importantly, the damage suffered by an institution in connection with a money laundering scandal is unlikely to be limited to a single civil or criminal penalty. Whilst the USD\$16 million fine imposed upon Riggs Bank may suggest that it suffered minimal legal damage relative to its misconduct, the institution's breaches of AML/CTF legislation had broader financial and reputational ramifications than this penalty. Stemming directly from its suspect dealings with General Pinochet and Equatorial Guinean officials, the bank also faced a spate of negative publicity and, during 2004 alone, incurred more than USD\$100 million in civil penalties, criminal fines, and fees attached to its related use of lawyers, consultants and auditors. Collectively, these costs contributed largely to the USD\$98.3 million loss posted by Riggs Bank the following year. 514

6.4 How reputational damage turned to legal and financial damage for Riggs Bank

6.4.1 The souring of a significant commercial deal

Whilst Riggs Bank had historically been viewed as the "cornerstone of the U.S. financial community", 515 the significant reputational, financial and legal damage it suffered as a result of its AML/CTF compliance failures, left it vulnerable to takeovers and buy-outs. In May 2004, the bank began reviewing its "strategic alternatives" after a number of financial services companies expressed an interest in acquiring it. Riggs Bank ultimately accepted an offer from PNC, which indicated that it was prepared to acquire the institution for US\$27 per share of Riggs Bank common stock.

However, following the imposition of the USD\$25 million civil monetary penalty upon the institution in May 2004, PNC decided to decrease its offer to just US\$24.25 per share. The two companies entered into an initial merger agreement to this effect on 16 July 2004 and in this agreement, Riggs Bank made explicit representations and warranties that since

⁵¹⁴ O'Hara, T., 'Judge Backs Riggs's \$16 Million Plea Deal', The Washington Post (Washington D.C.), 30 March 2005 http://www.washingtonpost.com/wp-dyn/articles/A11383-2005Mar29.htm at 23 December 2006.

⁵¹⁵ Op cit n471.
⁵¹⁶ Op cit n510.

31 December 2003, there had been no events or circumstances which were reasonably likely to have a "material adverse effect" on its value.⁵¹⁷

Several months later in January 2005 however, Riggs Bank admitted to contravening the *Bank Secrecy Act*'s reporting requirements and agreed to pay a USD\$16 million criminal fine in order to settle the matter.⁵¹⁸ Under the "material adverse change" clause in the merger agreement, this fine – and the admission of criminal culpability that accompanied it – constituted the "material regulatory impairments" necessary to give PNC a contractual right to terminate the proposed merger. Rather than abandon the deal though, PNC elected to substantially revise its previous buyout offer of USD\$24.25 per share, lowering it by a further 20 per cent to USD\$19.32 per share.⁵¹⁹

Riggs Bank rejected this new offer on 7 February 2005 and immediately filed a civil suit against PNC for anticipatory repudiation and breach of the initial merger agreement. S20 Whilst the bank accused the company of bad faith and trying to "virtually steal" it, S22 PNC held that Riggs Bank's tarnished reputation, excessive staff turnover, s23 exorbitant legal fees and outstanding involvement in several major lawsuits, had diminished its value so greatly that the original contract was redundant. That said, PNC eventually agreed to proceed with the proposed merger at a purchase price of USD\$20.00 per share and in return, Riggs Bank withdrew its legal claims against PNC without prejudice. In February 2005, the

⁵¹⁷ Op cit n464.

⁵¹⁸ 'Riggs National Accepts Reduced PNC Merger Deal', *Finfacts Ireland*, 11 February 2005 http://www.finfacts.com/cgi-bin/irelandbusinessnews/exec/view.cgi?archive=2&num=424 at 20 December 2006

⁵¹⁹ 'After Squabble, Riggs Agrees to \$643 million Buyout by PNC', *The Daily Item* (Pennsylvania) 14 February 2005 http://archive.dailyitem.com/archive/2005/0214/biz/stories/06biz.htm at 12 December 2006.

⁵²⁰ Op cit n471, 8.

O'Hara, T., Riggs, 'PNC Reach New Merger Agreement', *The Washington Post* (Washington D.C.), 11 February 2005 < http://www.washingtonpost.com/wp-dyn/articles/A13829-2005Feb10.html at 3 December 2006.

Pacelle, M., 'Riggs Sues PNC as Deal Collapses', *The Wall Street Journal* (New York), 8 February 2005, A.3.

A.3.

Between August 2004 and September 2005 inclusive, Riggs Bank's former Executive Vice President, R. Ashley Lee, was put on paid leave (August 2004); COO and Executive Vice President, Robert C. Roane, was suspended (September 2004); Chief Legal Officer, Joseph M. Cahill, was replaced (December 2004); and CEO, Robert Allbritton, resigned (March 2005).

Reiker, M., 'Riggs-PNC Looking Alive, Though Initial Price Isn't' (2005) 170(4) American Banker 20.

two companies entered into an *Amended and Restated Agreement and Plan of Merger* (**Amended Merger Agreement**), under which Riggs Bank's shareholders would only receive a final purchase price of USD\$643 million, as opposed to the USD\$779 million they stood to gain under PNC's original offer.⁵²⁵

6.4.2 Shareholder class actions

In addition to diminishing the value of its shares, Riggs Bank's non-compliance with AML/CTF legislation exposed the institution's directors to a string of damaging shareholder derivative suits during 2004 and 2005. As previously noted, the first shareholder derivative suits were filed on 7 April 2004 and 28 April 2004 respectively. These actions cast the bank's dismal compliance record further into the public eye at a time when it was engaged in delicate commercial negotiations and buyout discussions with PNC.

Generally, there are two broad bases of liability in shareholder derivative suits – breach of a fiduciary duty of care and breach of a fiduciary duty of loyalty – and the claimant shareholders in this case hinged their actions upon both heads of liability. They sought monetary damages and equitable relief on the basis that the Respondents "breached their fiduciary duties of loyalty, honesty and care, and caused a waste of corporate assets". According to the shareholders, the directors failed to conduct appropriate due diligence on Riggs Bank's customers, and exercise reasonable control and supervision in relation to the institution's compliance with federal AML/CTF legislation. 526 They allegedly breached their fiduciary duty of care by failing to manage Riggs Bank's corporate affairs honestly and in good faith, and breached their fiduciary duty of loyalty by personally profiting at the expense of the bank. Strategically, it was important for the shareholders to base their suits upon both

⁵²⁵ United States Federal Reserve, The PNC Financial Services Group, Inc., Pittsburgh, Pennsylvania: Order Approving the Merger of Bank Holding Companies (2005)

http://www.federalreserve.gov/boarddocs/press/orders/2005/200504262/attachment.pdf at 14 December 2006.

⁵²⁶ Op cit n464. See also Mazzucca, T., 'Shareholder Suit in Riggs' Future' (2004) 22(51) Washington Business Journal 3.

heads of liability because if they were unable to prove that the directors violated their duty of care, they could potentially still succeed on the basis of their duty of loyalty claims. 527

Whilst the two lawsuits were later settled, there was little reprieve for Riggs Bank. The institution's poor AML/CTF compliance record was again thrust into the public arena when another shareholder derivative suit; *Freeport Partners, L.L.C. v. Allbritton*, No. 04-CV-02030 (D.D.C. filed Nov. 18, 2004) (**the Freeport Partners Action**), was filed against a number of the bank's executives on 18 November 2004. At that time, Riggs Bank had just been sued over its alleged financing of the September 11 attacks, and was facing additional legal proceedings in Spain relating to its questionable dealings with General Pinochet.

The claimants in the Freeport Partners Action alleged that Riggs Bank's directors violated the U.S. *RICO Act* by maintaining a deficient AML program and laundering money on behalf of General Pinochet and officials from Equatorial Guinean. In the aftermath of the diminished PNC takeover deal, they alleged that the respondents' racketeering activities were "the proximate cause of a decline in value" of Riggs Bank because they "made the sale of [the bank] necessary and reduced the price at which that sale could be made". 528 Whilst this action was subsequently resolved when the directors agreed to a USD\$5.25 million settlement, 529 a similar class action and derivative complaint had already been filed on 19 November 2004 by another class of shareholders (the Delaware Plaintiffs).

The claimants involved in this action argued that the directors' failure to prevent the bank from breaching U.S. AML/CTF laws and/or engaging in illegal activities, constituted a

Typically, this latter head of liability has proven to be far a more effective basis for securing a successful shareholder derivative suit. See Advisen, Shareholder Derivative Suits: A Growing Concern for Corporate Directors and Officers (2005) 1 < http://www.cnapro.com/pdf/ShareholderDeriviativeSuits_Advisen.pdf at 25 June 2006.

⁵²⁸ O'Hara, T., 'PNC Settles Last Riggs Shareholder Suit', *The Washington Post* (Washington D.C.), 13 October 2005 < http://www.washingtonpost.com/wp-dyn/content/article/2005/10/12/AR2005101202163_pf.html at 23 December 2006.

See Freeport Partners LLC v. Joseph L. Allbritton, Notice of Pendency of Class Action and Proposed Settlement, Settlement Hearing, Motion for Attorneys' Fees and of Right to Appear, Civil Action No. 04-2030 (GK), United States District Court for the District of Columbia, 30 November 2005. See also Cohen, Milstein, Hausfeld & Toll P.L.L.C., PNC Settles Last Riggs Shareholder Suit (2005) http://www.cmht.com/cases-riggsarticle.php at 12 December 2006.

breach of their fiduciary duties. With specific reference to the PNC agreement, the shareholders accused the directors of breaching their fiduciary duties of care and loyalty by trying to sell Riggs Bank in a "fire sale" at an "unfair price". ⁵³⁰ Further, in an amended shareholder class action and derivative suit subsequently filed by the claimants on 22 February 2005 (**the Second Amended Complaint**), they alleged that the directors breached their duty to maximise shareholder value by failing to auction the bank after PNC attempted to abandon the original buyout agreement.

In addition to damages and legal costs, the Delaware Plaintiffs sought declaratory and injunctive relief against the finalisation of the proposed agreement with PNC. However, in March 2005, PNC agreed to pay the claimants USD\$2.7 million. Size Given that shareholder derivative actions are notoriously disruptive to institutions, this was seemingly a strategic move on the part of PNC. By agreeing to settle the lawsuit, the company effectively kept its commercial deal afloat and avoided some of the ongoing AML/CTF legal risk it would otherwise have faced following the execution of that deal. If the suit had arisen earlier, it might have been better for PNC to stay removed from the proceedings. Doing so may have subjected Riggs Bank to further regulatory scrutiny and reputational damage, and further lowered its value so that any buyout price could again be revised downwards. However, as PNC and Riggs Bank had already formalised their merger agreement before the commencement of the shareholder suit, it was in PNC's best interests to bring about a quick and quiet resolution.

Undoubtedly, the numerous shareholder derivative actions launched against Riggs Bank's executives during 2004 and 2005, impacted the bank's commercial negotiations with PNC. However, they also had broader compliance implications for other institutions. Such actions sent a strong message to other directors that the responsibility for oversight of their institutions' AML/CTF compliance fell squarely on their shoulders. They could no longer hide behind an opaque corporate veil to avoid accountability for AML/CTF compliance

⁵³⁰ Op cit n464, 3.

⁵³¹ Op cit n464, 3.

⁵³² In order to resolve the Second Amended Complaint, the Delaware Plaintiffs, Riggs Bank and the individual Defendants executed a Memorandum of Understanding on or about 1 March 2005.
⁵³³ Op cit n527.

failures – regulators and shareholders could now hold them to a far higher standard of knowledge regarding their organisation's activities.⁵³⁴

6.5 The resulting regulatory environment

The impact that September 11 has had on the U.S. financial system and regulatory environment cannot be overstated. The events of that day prompted the enactment of the USA PATRIOT Act and provided the catalyst for a dramatic widening of the responsibilities and powers of U.S. banking regulators. Essentially, they created an environment in which the U.S. Federal Government and the public now expect:

- *institutions* to strictly adhere to AML/CTF laws by implementing robust AML programs and internal controls; and
- regulatory authorities to swiftly identify, pursue and reprimand any institution that fails to comply with its legislative AML/CTF obligations.

Whilst Riggs Bank clearly failed to meet these expectations, so too did the regulatory officials charged with overseeing its AML/CTF compliance. After the bank's egregious violations of AML/CTF laws were uncovered, U.S. banking regulators were harshly and very publicly criticised for failing to be more interventionist with respect to the identification and punishment of its compliance failures. This criticism was particularly emotive in the wake of September 11, and in the midst of the U.S. Government's campaign to prevent terrorists, corrupt leaders and other criminals from misusing the country's financial system.

Although Riggs Bank had been cited for technical deficiencies in its *Bank Secrecy Act* compliance program as early as 1997, the OCC did not start to closely supervise the institution until 2002, when a number of media reports were published by journalists who seemingly knew more about the bank's suspect dealings than regulatory authorities did. Repeatedly, key enforcement actions against Riggs Bank were simply reactive; having been

⁵³⁶ Op cit n470.

Keenan, C., Weighty Challenges: Legal Issues for Bank Boards (2004) 14(3) Bank Director Magazine 36.

Bakerplatt, Riggs Bank the fall of an Institution – A Salutary Lesson for All? (2005) 3 http://www.bakerplatt.com/upload/public/Files/1/artriggsbank.pdf at 15 May 2007.

taken only after negative press reports publicly questioned the institution's AML/CTF control environment. For example, the OCC's detailed reviews of the bank's Saudi Arabian accounts and its Equatorial Guinea accounts were both prompted by the publication of articles connecting those accounts to undesirable customers and potentially illicit activity.

Even when U.S. regulatory authorities did take some steps towards addressing Riggs Bank's legislative breaches, they did not act as decisively or aggressively as might have been expected by an ever-watchful public audience. Despite the institution's ongoing disregard for its AML/CTF requirements, no officer or director of the bank was ever held criminally liable for its AML/CTF failings. Whilst several of Riggs Bank's directors were prosecuted in Spain with respect to their dealings with General Pinochet, the charges against them were subsequently abandoned subject to a settlement agreement. No comparable charges were ever brought against the institution's executives in the U.S., despite the fact that there was likely enough evidence to justify the initiation of criminal proceedings.

Nevertheless, U.S. regulatory authorities did launch criminal enforcement proceedings against Riggs Bank and that is more than they have done in many other cases of corporate non-compliance with domestic AML/CTF laws. As discussed in **Chapter 3** of this thesis, the difficulties inherent in mounting criminal proceedings against well-resourced corporations (and the possible ramifications attached to corporate prosecutions) have seen most institutions escape criminal liability for their AML/CTF compliance failures. However, owing to its flagrant disregard for U.S. AML/CTF regulations and its continued attempts to evade regulatory oversight, Riggs Bank provides a rare exception to the common practice of pursuing institutions through the use of civil actions.

Despite facing a range of enforcement actions and lawsuits, it is uncertain why Riggs Bank never felt the full force of the harsh civil and criminal penalties available under U.S. AML/CTF legislation. Although it was subject to large criminal fines and civil monetary penalties, some commentators may believe that the severity of the bank's AML/CTF compliance failures justified greater punishment. When the penalties are viewed in isolation, this may in fact be true. Indeed, no restrictions were ever placed on the institution's banking

licence, and at no stage did its deposit insurance appear to be at risk as a result of its admissions of criminal liability. However, when viewed collectively and in light of their broader commercial consequences, others may consider that the penalties imposed upon Riggs Bank were in fact appropriate. Undoubtedly, they created such reputational and financial damage for Riggs Bank that the institution was ultimately bought by a competitor for far less than its original value.

Ultimately, the criticism U.S. banking regulators received for their retroactive and lackadaisical approach to Riggs Bank's compliance failures, prompted a reappraisal of their effectiveness in combating money laundering and terrorism financing activities. Following the Riggs Bank scandal, some commentators accused FinCEN and the OCC of failing to ensure that the institution met its AML/CTF requirements in a satisfactory and timely manner. Sara Several high-profile political figures went further than this; condemning the regulatory authorities for taking "five years to act in any substantive way" with regards to the bank's grossly inadequate AML/CTF program. They held that the damage stemming from Riggs Bank's activities could have been greatly minimised, had regulatory officials taken swifter and more decisive enforcement action against the bank.

The allegedly inadequate response of regulatory authorities to Riggs Bank's AML/CTF compliance failures has prompted the U.S. Government to consider overhauling the way in which they oversee the activities of financial institutions. Following the Riggs Bank scandal, the U.S. Senate Banking Committee has questioned the capability of regulators to effectively identify and address institutions' non-compliance with AML/CTF regulations. Further, the U.S. Senate Permanent Subcommittee on Investigations has placed increased pressure on federal banking regulators to:

- require the prompt correction of all AML/CTF deficiencies;
- make greater use of their formal enforcement tools; and

⁵³⁷ Borchersen-Keto, S., OCC says Mistakes Made in Oversight of Riggs Bank's Compliance with BSA (2004) Compliance Headquarters

http://www.complianceheadquarters.com/AML/AML_Articles/6_4_04.html at 28 December 2006.

⁵³⁸ Op cit n521.
⁵³⁹ Op cit n537.

 publish the results of their AML/CTF assessments in the annual Report on Examination they provide to U.S. banks.⁵⁴⁰

Arguably, if U.S. banking regulators had previously taken such steps and been more assertive in their enforcement of AML/CTF laws, Riggs Bank's directors might have prioritised their AML/CTF compliance and made a concerted effort to implement appropriate safeguards.

Though no major structural changes have yet been made to the U.S. regulatory landscape, banking regulators have certainly suffered a backlash as a result of their poor handling of Riggs Bank's AML/CTF deficiencies. In the coming years, this may translate into a more aggressive AML/CTF regulatory approach and give rise to additional AML/CTF legal risk for other institutions. It is anticipated that regulators such as the OCC and FinCEN will try to avoid further reputational damage in the future by demonstrating that they are proactively using their enforcement powers to correct institutions' AML/CTF shortcomings. Whilst this does not necessarily mean they will be more willing to initiate criminal enforcement actions against non-compliant institutions, this would seemingly become a desirable (or at least, a more plausible) outcome if another institution were to engage in legislative breaches as numerous and flagrant as those of Riggs Bank.

6.6 Conclusion

Given its chequered AML/CTF compliance record and its merger with PNC, Riggs Bank has become a striking and oft-cited example of how an institution that spent nearly two centuries building a reputation for integrity, security and trustworthiness, shattered it by engaging in a string of AML/CTF compliance failures. It has become emblematic of lax compliance with AML/CTF laws and weak Board oversight. Whilst many pieces of municipal AML/CTF legislation now stipulate that Boards of directors and senior management bear the ultimate responsibility for the success (or otherwise) of their institution's AML/CTF program, ⁵⁴¹ the

⁵⁴⁰ Op cit n486, 7.

Office of the Superintendent of Financial Institutions, Guidelines on Deterring and Detecting Money Laundering and Terrorist Financing: Sound Business and Financial Practices (2003) 6 http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/guidelines/sound/guidelines/B8 e.pdf> at 29 April 2008.

directors of Riggs Bank sought to ignore its glaring AML/CTF compliance failures. They did not take an active interest in AML/CTF compliance and they fostered a corporate culture where profit making was prioritised before legislative adherence.⁵⁴²

Given Riggs Bank's strong embassy banking business and high profile customer base, the institution was always going to be exposed to heightened levels of ML/TF risk. However, its risk profile would not have created so much regulatory exposure had it actually sought to design and implement controls commensurate to its ML/TF risk. Whilst Riggs Bank actively solicited business from PEPs and other individuals based in higher risk jurisdictions, it seemingly did little, if anything, to monitor their accounts or report their suspicious transactions. Though it may have coveted the business of PEPs such as General Pinochet in an era when they were in fact highly desirable customers, the institution should nevertheless have subjected its customers to ongoing due diligence in the aftermath of September 11 and the enactment of the USA PATRIOT Act.

As previously noted, risk-based approaches to AML/CTF are not intended to restrict the activities of institutions to lower risk products/channels, customers and jurisdictions. On the contrary, they implicitly empower institutions to assume the levels of ML/TF risk that they are comfortable with. However, the legislative qualification on this freedom is the requirement that institutions address their levels of risk through appropriate AML/CTF systems and controls. If they are essentially exposing themselves – and the financial system – to increased levels of ML/TF risk, then they must take additional steps to ensure that the risk is adequately mitigated (for instance, through additional staff training, greater due diligence, and closer monitoring activities).

Evidently, the ML/TF risk that Riggs Bank faced was not just a result of external factors but also its internal employees. Whether driven by his friendship with Mr Obiang or perverse financial incentives offered within the bank, Mr Kareri was able to facilitate money

By many accounts, Riggs Bank's management created a corporate culture where some staff were encouraged to dissociate their ethics from their conduct, and worked amidst "fear of reprisal and of losing their jobs" if they lost a client. See O'Hara, T., 'In Cultivating International Clients, Riggs Went Down a Perilous Path', The Washington Post (Washington D.C.), 21 March 2005

http://www.washingtonpost.com/ac2/wp-dyn/A52084-2005Mar20?language=printer> at 24 December 2006.

laundering activities for his Equatorial Guinean customers over an extended period of time. Though Riggs Bank could not have pre-empted Mr Kareri's activities via any kind of employee screening, it could nevertheless have monitored them more closely (if it had wanted to of course) via an AML/CTF employee due diligence program.

By prioritising profits and customer retention before legislative compliance, Riggs Bank increased its legal, financial and reputational risk. Its disregard for U.S. AML/CTF laws, as well as its persistent failure to take corrective action and employ a risk management strategy, not only heightened the bank's AML/CTF legal risk but also exposed it to a number of civil enforcement proceedings, monetary penalties, shareholder derivative suits and even criminal prosecution. Its flagrant breaches of AML/CTF legislation saw U.S. prosecutors dispense with their preference for deferred and non-prosecution agreements, and the institution become one of the few entities to be criminally pursued for its AML/CTF compliance failures in the aftermath of several significant corporate collapses.

Importantly, Riggs Bank's repeated AML/CTF compliance failures not only had implications for the bank itself, but also created reputational risk for U.S. banking regulators, and increased the risk for other financial institutions. The bank's questionable dealings prompted a campaign by the U.S. Government to urge federal banking regulators to more actively enforce the *Bank Secrecy Act* and other AML/CTF legislation. In turn, this triggered a crackdown on money laundering by U.S. financial institutions, and led to the immediate investigation of more than half a dozen other banks for AML/CTF violations similar to those facilitated by Riggs Bank. Evidently, Riggs Bank's non-compliance with federal AML/CTF legislation had far wider, systemic repercussions than the bank, regulatory authorities, or other financial institutions may have initially foreseen.

Chapter 7

Banco Delta Asia: USA PATRIOT Games

"Reputation is an idle and most false imposition; oft got without merit, and lost without deserving" – William Shakespeare, Othello

7.1 Introduction

Retribution for certain AML/CTF offences can, on occasion, be swift and extensive. As previously discussed in **Chapters 3 and 4** of this thesis, individuals and institutions in breach of their AML/CTF requirements may face a range of civil and criminal enforcement proceedings, and associated penalties. As evidenced from cases such as Riggs Bank, an institution that has fallen foul of AML/CTF laws may incur criminal and civil penalties, and face a range of related lawsuits initiated by interested third parties (including, in jurisdictions such as the U.S., its own shareholders). Interestingly however, the experience of Banco Delta Asia, a small financial institution based in Macau, demonstrates that an institution's AML/CTF legal risk is not always confined to the initiation – and resolution – of formal legal proceedings.

Even in the absence of legal proceedings, formal fact-finding exercises, the presentation of evidence or a final determination of guilt, an institution may still face considerable AML/CTF legal risk. Banco Delta Asia's designation as a "primary money laundering concern" under Section 311 of the USA PATRIOT Act⁵⁴³ provides a striking illustration of the way in which an institution deemed to be associated with money laundering activities might be impacted by extraterritorial laws, unsubstantiated regulatory claims, and public opinion. Further, it showcases the extent to which an institution's AML/CTF legal risk may be hinged upon international relations and the delicate political relationships between particular nation states.

⁵⁴³ See 31 U.S.C. § 5318A.

As opposed to the quantifiable criminal and civil penalties typically imposed upon institutions under AML/CTF legislation, the effects of a designation under Section 311 may be unpredictable, unreliable and uncertain. In contrast to a number of standard enforcement tools, an institution's designation as a "primary money laundering concern" cannot be kept confidential from the public. Indeed, the practical effect of such a designation, as well as any accompanying government rulemaking, is to use publicity as a criminal sanction; stigmatising and imposing some degree of shame on the designated entity. 544

This Chapter outlines the allegations against Banco Delta Asia, the activities leading to its designation under U.S. extraterritorial legislation, the political environment in which the designation occurred, and the events that have subsequently unravelled since the institution's expulsion from the U.S. financial system. It seeks to use the bank as an in-depth case study to:

- demonstrate the scope and influence of U.S. extraterritorial AML/CTF laws;
- showcase the interrelationship that may arise between AML/CTF laws, politics, government-sponsored crime and national security;
- identify the potential limitations on an institution's risk management capabilities; and
- address the claims of many commentators that links to money laundering may cause irreparable reputational damage to an institution.

7.2 The beginning of the end for Banco Delta Asia

As at 14 September 2005, Banco Delta Asia was a small, family-owned institution operating in Macau's Special Administrative Region.⁵⁴⁵ Rather than handling large cash deposits in foreign currency, the bank's operations were geared towards the receipt of small retail deposits and consumer loans in Macau's pataca currency.⁵⁴⁶ Less than 24 hours later

Netter, B., 'Avoiding the Shameful Backlash: Social Repercussions for the Increased Use of Alternative Sanctions' (2005) 96(1) Journal of Criminal Law & Criminology 187.

⁵⁴⁵ 'U.S. Money Laundering Accusation Ignites Resentment in Macau', *People's Daily Online* (Beijing), 17 September 2005 http://english.peopledaily.com.cn/200509/17/eng20050917_209027.html at 9 January 2007.

Lawder, D., 'Macau Bank Struggles to Shake Off North Korea Links', *Reuters UK*, 21 December 2006 http://uk.reuters.com/article/featuresNews/idUKSP15073620061222 at 25 April 2007.

however, this seemingly unremarkable financial institution became entangled in an international money laundering scandal that would ultimately attract unwanted regulatory attention and diminish the bank's reputation in the eyes of both the media and the public.

On 15 September 2005, the U.S. Treasury Department deemed Banco Delta Asia to be of "primary money laundering concern" under Section 311 of the USA PATRIOT Act. It publicly accused the bank of representing an "illicit financial threat" to U.S. financial institutions, and acting as "a willing pawn for the North Korean government to engage in corrupt financial activities through Macau". 547 According to the U.S. Treasury Department, Banco Delta Asia had a long history of assisting North Korean government agencies and front companies to place counterfeit currency in the international financial system, 548 make surreptitious cash deposits and withdrawals, 549 and launder funds derived from fake cigarettes, drug trafficking and the proliferation of weapons. 550

Given that Banco Delta Asia received no notice of its impending designation, it was perhaps incapable of appreciating the extent of its AML/CTF legal risk under U.S. extraterritorial legislation. Further, given its potential inability to gauge its AML/CTF risk, the bank was unlikely to have been in a position to mitigate or avoid such risk by engaging with U.S. regulatory officials, terminating all of its relationships with North Korean customers, or implementing stricter KYC and transaction monitoring controls. The U.S. Treasury Department seemingly intended for its *Section 311* designation to cause maximum impact and prejudice to the bank.

54

United States Department of the Treasury, Treasury Designates Banco Delta Asia as Primary Money Laundering Concern under USA PATRIOT Act (Press Release, 15 September 2005).

United States authorities alleged that between 1989 and 2005 inclusive, Banco Delta Asia was the primary outlet for more than USD\$45 million in North Korean-made counterfeit American \$100 bills. See Gertz, B., 'U.S. Sanctions Cost North Korea Millions', *The Washington Times* (Washington D.C.), 16 June 2006 http://www.washingtontimes.com/national/20060615-105145-9374r.htm at 18 January 2007.

⁵⁴⁹ Laundering Charge Hits Macau Bank', *BBC News*, 19 September 2005 http://news.bbc.co.uk/1/hi/business/4261450.stm at 30 December 2006.

⁵⁵⁰ Greenless, D., 'Macau Inquiry Clears Bank of Money Laundering for N. Korea', *International Herald Tribune – Asia Pacific* (New York), 12 March 2007

http://www.iht.com/articles/2007/03/12/news/bank.php at 20 March 2007.

Section 311 of the USA PATRIOT Act empowers the U.S. Secretary of the Treasury to designate any foreign money laundering or terrorism financing threats a "primary money laundering concern". Under the Act, these threats may include:

- foreign jurisdictions perceived to have an inadequate AML/CTF regime;
- classes of foreign accounts or transactions deemed to represent an unacceptably high money laundering risk; or
- in the case of Banco Delta Asia, foreign financial institutions believed to support (either knowingly or unwittingly) money laundering or terrorism financing activities. ⁵⁵¹

Evidently, the provisions enshrined in *Section 311* are somewhat underpinned by the notion that the integrity of a nation state's AML/CTF regime, is partially dependent upon the quality (and the relative strength) of the AML/CTF controls in neighbouring countries. They are innately hinged upon a perception that weaknesses in the control environments of foreign institutions and foreign countries have the ability to place others at risk. In essence, they convey a belief that as far as effective AML/CTF regulation is concerned, the 'chain' is only as strong as its weakest 'link'. 552

Whilst supporters of Section 311 regard it as a "diplomatic sledgehammer that gets results", 553 many critics consider it to be simply a tool for the U.S. Treasury Department to sidestep international and national legal practices by using an Executive Branch administrative procedure to accuse — and find a foreign institution or jurisdiction guilty — of certain wrongdoing. 554 They claim that any designation made under the Section not only

⁵⁵¹ See Aufhauser, D., 'Terrorism: Growing Wahhabi Influence in the United States' (Testimony before the United States Senate Committee on the Judiciary, 26 June 2003).

Interestingly however, some commentators have argued that a country's lax or unregulated control environment will not necessarily attract greater levels of money laundering or terrorism financing. On the contrary, investors – even those with illicit motives – want to ensure that their funds are safe and not vulnerable to theft, corruption and other crimes. See Rodrigues, A.G., 'The Prevention and the Combat of Money Laundering and Terrorist Financing: A Social Responsibility' (Speech delivered at the Anti-Money Laundering and Counter-Terrorism Financing Conference 2009, Managing Risk: Australian and International Perspectives, Sydney, 1 April 2009).

Hall, K.G., 'Under Patriot Act, Treasury Casts a Wide Net', McClatchy Newspapers (Sacramento), 12 March 2007 http://www.mcclatchydc.com/148/story/15754.html at 26 January 2009.

Hauben, R., North Korea's \$25 Million and Banco Delta Asia: Another Abuse under the U.S. Patriot Act (2001) (2007) NewsGroups 2 http://newsgroups.derkeiler.com/pdf/Archive/Soc/soc.culture.korean/2007-03/msg00027.pdf at 26 January 2009.

presumes an institution's guilt,⁵⁵⁵ but denies it the due process otherwise afforded to U.S. citizens by the Fifth and Fourteenth amendments of the U.S. Constitution. Indeed, the actions taken by the U.S. Treasury Department under *Section 311* are not managed, reviewed, overseen or adjudicated by a local or foreign court or legislature.⁵⁵⁶

Once a foreign institution is deemed to be of "primary money laundering concern" under Section 311, the U.S. Secretary of the Treasury may order U.S. financial institutions to take one or more "special measures". ⁵⁵⁷ The Act contains five special measures which, collectively, provide a graduated tool that the U.S. government can use to strategically focus and intensify its AML/CTF efforts in relation to a single institution, financial sector, or aspect of a foreign government's operations. ⁵⁵⁸ These measures range in severity from enhanced due diligence, recordkeeping and reporting, up to and including the termination of correspondent banking relationships. Whilst Section 311 stipulates that these measures "may be imposed in such sequence or combination as the Secretary shall determine", it is interesting to note that the most severe special measure was applied in the case of Banco Delta Asia. Prior to that time, only four other institutions (i.e. Myanmar Mayflower Bank, Asia Wealth Bank, the Commercial Bank of Syria and VEF Banka) and one jurisdiction (i.e. Myanmar) had felt the full force of the same measure. ⁵⁵⁹

Shortly after the bank's designation, FinCEN issued a proposed rulemaking that, if subsequently formalised, would prohibit U.S. financial institutions from establishing, maintaining, administering or managing any correspondent account in the U.S. for, or on behalf of, Banco Delta Asia. This proposed rule evidently carried significant financial risk

_

⁵⁵⁵ Ibid.

⁵⁵⁶ Op cit n553.

⁵⁵⁷ See 31 U.S.C. § 5318A(b)(1)-(5).

See United States Department of the Treasury – Office of Public Affairs, Treasury Department Designates Burma and Two Burmese Banks to be of "Primary Money Laundering Concern" and Announces Proposed Countermeasures Under Section 311 of the USA PATRIOT Act (Press Release, 19 November 2003)

Although several other institutions and jurisdictions had previously been the subject of Notices of Proposed Rulemaking in relation to the same special measure, they all managed to avoid the imposition of a Final Ruling by undertaking the U.S. government's desired remedial actions. See McGlynn, J., 'Banco Delta Asia, North Korea's Frozen Funds and US Undermining of the Six-Party Talks: Obstacles to a Solution', Japan Focus, 9 June 2007 http://japanfocus.org/products/details/2446 at 29 June 2008.

for the bank, given that it maintained a number of correspondent accounts in Europe, Asia, Australia, Canada and the U.S at that time.⁵⁶⁰

Although representatives of Banco Delta Asia and the Macau government lobbied the U.S. Treasury Department to rescind the bank's designation and the proposed rulemaking, FinCEN finalised the rule on 14 March 2007. It again accused the bank of providing financial services to corrupt North Korean entities, and conducting such grossly inadequate due diligence that those entities were able to:

- suppress the identity and location of their transaction originators;
- repeatedly transfer large, round-figure sums with no apparent legitimate purpose to and from accounts held at other banks; and
- routinely use cash couriers to move around significant sums of currency, in the absence of any credible explanation as to the origin or purpose of such transactions.⁵⁶¹

The final rule, which came into force on 13 April 2007, prevents Banco Delta Asia from accessing the U.S. financial system. ⁵⁶² It not only prohibits U.S. financial institutions from *directly* opening or maintaining correspondent accounts for the bank, but also compels them to take reasonable steps to ensure that they do not allow the bank to *indirectly* access the U.S. financial system via another one of their correspondent accounts. As this final rule effectively constitutes a U.S. federal regulation, it can only be withdrawn by the U.S. Treasury Department following the publication of a 'Notice to Rescind' in the U.S. Federal Register. ⁵⁶³ Though this would not be an overly arduous task for the U.S. Treasury Department, it is unlikely to occur any time in the imminent future. In the history of

These accounts were held at a range of financial institutions, including Wachovia in the U.S., Standard Chartered in Hong Kong, and ANZ Bank in Australia.

United States Department of the Treasury, Treasury Finalizes Rule Against Banco Delta Asia: BDA Cut Off From U.S. Financial System (Press Release, 14 March 2007).

Financial Crimes Enforcement Network, Advisory: Guidance to Financial Institutions on the Provision of Banking Services to North Korean Government Agencies and Associated Front Companies Engaged in Illicit Activities (2005) http://www.fincen.gov/advisory.pdf at 14 March 2007.

Whilst the U.S. Treasury Department can apply and/or rescind the four less severe special measures at will, the process to withdraw a final rule in relation to the fifth special measure is more formal.

Section 311, there is no precedent for the withdrawal of a final rule made against a foreign financial institution. 564

7.2.1 Banco Delta Asia's response to the allegations

Immediately following its designation as a "primary money laundering concern", Banco Delta Asia attempted to mitigate its AML/CTF legal risk and reputational risk by vigourously denying the accusations levelled against it and dismissing them as a blatantly unsubstantiated, "ridiculous joke". Whilst the bank's representatives admitted to conducting business on behalf of some North Korean entities, they claimed that various U.S. agencies (and even the monetary authorities in Hong Kong and Macau), had known about its trade relationship with North Korea for many years. Further, they held that prior to the bank's designation, it had never been approached or questioned by any U.S. government agency regarding its dealings with North Korea. Services of the service

Despite rejecting the U.S. Treasury Department's allegations however, the groundswell of public and commercial pressure generated by them forced Banco Delta Asia to implement enterprise-wide controls. Shortly after its designation, the bank froze all of its North Korean accounts and agreed to "enhance [its] operational stability as well as facilitate the addressing of the allegations raised by the U.S. Treasury Department". ⁵⁶⁸ It comprehensively overhauled its AML/CTF procedures, replaced the heads of its nine business departments, and handed control of its management to a three-person Administrative Committee appointed by the Macau government. ⁵⁶⁹ Additionally, and perhaps in an attempt to seek the U.S. Treasury Department's favour and mitigate its

⁵⁶⁴ Op cit n559.

⁵⁶⁵ Op cit n549.

Coleman, Z., 'Banco Delta Board Yields Control', *The Standard* (Hong Kong), 29 September 2005 http://www.thestandard.com.hk/news_detail.asp?we_cat=4&art_id=2338&sid=4782658&con_type=1&d_st=20050929 at 23 January 2007.

⁵⁶⁷ Op cit n545.

⁵⁶⁸ Ibid.

⁵⁶⁹ The Macau government took control of Banco Delta Asia's affairs after all the members of the bank's Board of directors suspended the exercise of their responsibilities, and entrusted management of the institution to a government-appointed committee. This committee included members of the Monetary Authority of Macau.

ongoing regulatory risk, it publicly pledged that it would never deal with North Korean entities again in the future.

In light of these remedial actions, Macau government officials and representatives of the bank urged FinCEN to revoke its notice of proposed rulemaking. However, given that the U.S. Treasury Department subsequently finalised the proposed rule, it evidently did not believe that Banco Delta Asia's organisational changes were sufficient to rescind the proposed rulemaking and withdraw the special measure. That said, it is unclear what additional steps the bank could have taken to quell the U.S. Treasury Department's ongoing concerns about its activities with those North Korean customers considered to be unsavoury by the U.S. government. The desirability of Banco Delta Asia's customer relationships was seemingly judged in hindsight. If this is the case, apart from the due diligence presumably carried out by Banco Delta Asia at the time of on-boarding its North Korean customers, no number of additional controls could have spared the institution from the U.S. government's subsequent claims that its customers were connected with organised crime.

7.2.2 The broader attack on Macau

Whilst the U.S. Treasury Department held that the Section 311 designation was specifically leveled at Banco Delta Asia as an institution, rather than Macau as a jurisdiction, its claims against the bank were accompanied by harsh criticism of the country's lax and immature AML regime. In publishing its notice of proposed rulemaking in the U.S. Federal Register, the U.S. Treasury Department held that money laundering had been a long-standing and "significant problem" in Macau, and one which had enabled a number of the country's institutions to "launder counterfeit currency and the proceeds from government-sponsored illegal drug transactions" for North Korean government entities and front companies. 571

⁵⁷⁰ Op cit n549.

See United States Department of the Treasury, 'Finding That Banco Delta Asia SARL is a Financial Institution of Primary Money Laundering Concern', *Federal Register*, Vol. 70, No. 181, 20 September 2005, 55215.

Interestingly however, this criticism of Macau came about less than 12 months after the U.S. Department of State praised the country's government for supporting global anti-terrorism efforts, drafting new AML/CTF legislation, and continuing to open up its economy. ⁵⁷²
According to a report issued by the U.S. Department of State in 2004, in the aftermath of September 11 the Macau government had, amongst other things:

- prepared a draft AML law creating a national FIU;
- increased the customer screening and due diligence standards, and extended the suspicious activity reporting requirements, imposed upon institutions;
- created an AML legal framework in line with international standards and United Nations
 Security Council Resolutions (UNSCRs); and
- worked collaboratively with U.S. law enforcement agencies on AML/CTF issues.⁵⁷³

The U.S. Treasury Department's criticism of Macau's AML/CTF efforts in 2005, is clearly in contrast to the U.S. Department of State's praise of such efforts only a year earlier. Arguably, the vast disparity between the views held by these U.S. government agencies suggests that the bank's designation was part of a broader, country-specific strategy in the fight against money laundering and terrorism financing. A country's economy is only as strong as its financial system, and by tainting the reputation of Banco Delta Asia and launching a stinging attack against Macau's broader AML/CTF environment, the U.S. Treasury Department jeopardised the stability of Macau's entire economy.

The Macau government attempted to refute the U.S. Treasury Department's criticism by arguing that the country strictly observes all UNSCRs aimed at thwarting financial crime, and has a stringent regulatory framework where all authorised financial institutions are supervised by the Monetary Authority of Macau (MAM). However, the national government's claims were seemingly deafened by the media releases questioning its AML/CTF control environment, and disregarded by the many financial institutions and

United States Department of State, *U.S.-Macau Policy Act Report* (2004) http://www.state.gov/p/eap/rls/rpt/35706.htm at 27 January 2007.

⁵⁷³ Ibid.

⁵⁷⁴ Op cit n545.

national AML/CTF regulators prepared to accept the U.S. Treasury Department's claims without any supporting evidence or analysis.

Ultimately, the negative publicity generated by the U.S. Treasury Department's proposed rulemaking meant that the Macau government had little choice but to announce an independent investigation into Banco Delta Asia's activities. Whilst Macau's government officials urged depositors to "have faith and confidence in the financial system of Macau, and continue to support the long-term stability and prosperity" of the region, 575 there was seemingly little else the government could do to instil confidence in the U.S. Treasury Department and the international community that it regarded money laundering as a serious global issue.

7.3 The fallout from the designation

Although the U.S. Treasury Department's proposed rulemaking was not finalised until March 2007, Banco Delta Asia had already suffered immense reputational and financial damage following its September 2005 release. The adverse publicity that accompanied the U.S. Treasury Department's proposed rulemaking had stigmatised the bank and significantly undermined customer confidence in both its operations, and the safety and security of their funds. As is typical in many cases of severe reputational damage, ⁵⁷⁶ this in turn led to an erosion of Banco Delta Asia's brand value, a reduction in its deposits, and a decrease in its customer base.

Whilst the proposed rulemaking did not legally compel U.S. financial institutions to cut all commercial ties with Banco Delta Asia, it immediately prompted an informal financial embargo of the bank; one of the few independent financial institutions left in Macau.⁵⁷⁷ Less than 24 hours after it was deemed to be of "primary money laundering concern", depositors

Lee, J., 'Macau Calls for Calm in Wake of U.S. Money-Laundering Charge', *Radio Free Asia*, 17 September 2005 http://www.rfa.org/english/news/2005/09/17/Macau_bank/ at 10 January 2007. Klein, A., 'Losses Rise If Reputation is Compromised' (2007) 20(3) Bank Technology News 38.

^{&#}x27;HK PRESS: Macau's Banco Delta Asia Seeking Buyer', *The Standard* (Hong Kong), 27 February 2006 http://asia.news.yahoo.com/060227/5/2ghrt.html at 4 January 2007.

collectively withdrew more than USD\$5 million from the institution.⁵⁷⁸ The bank's AML/CTF legal risk had swiftly translated into reputational and financial damage, and despite calls for calm from both the bank and the Macau government, the situation only escalated. Less than 48 hours after the U.S. Treasury Department accused the bank of laundering funds for corrupt North Korean entities, concerned customers had withdrawn more than USD\$37.5 million (i.e. approximately ten per cent) of the institution's total deposits.⁵⁷⁹ The run on Banco Delta Asia's deposits continued and eventually depleted the institution's funds by USD\$133 million; about one third of its total deposits.⁵⁸⁰ It caused the bank to borrow USD\$62.5 million from the Macau government, and seek additional funds from its parent company to handle the crisis.⁵⁸¹

The severity and extent of the financial damage suffered by the bank as a result of its designation under *Section 311* of the *USA PATRIOT Act*, was evident just several months later, in the financial reports of its parent company. At the end of the 2005 financial year, the Delta Asia Financial Group reported revenues of 182.6 million patacas against 214.3 million patacas in expenses, with a negative balance of 31.7 million patacas. This was in contrast to the significant profits made by Banco Delta Asia and the Delta Asia Financial Group during the preceding financial year, and the most apparent justification for this notable turnaround in the companies' financial standing is the damage they suffered as a result of the U.S. Treasury Department's proposed rulemaking. 583

The financial hardship suffered by Banco Delta Asia in the aftermath of its designation was not simply attributable to the run on its deposits but also the freezing of several of its accounts. Shortly after Macau authorities took control of the bank, they froze approximately

⁵⁷⁸ Op cit n545.

Batchelor, M., 'Macau Gets Control of Banco Delta', *Bloomberg News*, 29 September 2005 http://www.iht.com/articles/2005/09/29/bloomberg/sxbanco.php at 1 January 2007.

⁵⁸⁰ Greenless, D., and Lague, D., 'Trail Led to Macao as Focus of North Korean Corruption', *The New York Times* (New York), 13 April 2007

< http://www.nytimes.com/2007/04/13/world/asia/13macao.html? r=2&oref=slogin&oref=slogin> at 16 April 2007.

⁵⁸¹ Op cit n545.

Owning Up: Delta Asia Admits Selling Pyongyang Gold', *Macau Business*, 1 January 2007 http://www.macaubusiness.com/index.php?id=672 at 28 April 2007.

Delta Asia Financial Group, Delta Asia Financial Group 2004 Annual Report (DAFG, Hong Kong, 2005).

50 accounts held on behalf of North Korean citizens, corporations and government entities. 584 Collectively, these accounts contained an estimated USD\$25 million. 585

The freezing of accounts impacted Banco Delta Asia's North Korean customers, as well as its broader customer base. A number of its corporate customers had their accounts frozen even though the funds in their accounts were traceable to legitimate business practices. One corporate customer; a foreign-operated bank in Pyongyang called Daedong Credit Bank (**Daedong**), had more than USD\$6 million frozen at Banco Delta Asia at the behest of the U.S. Treasury Department. This was despite the fact that:

- Daedong's owners could demonstrate that the funds were derived from legitimate business dealings in North Korea;⁵⁸⁶ and
- of the USD\$49 million in cash moved by Daedong through Banco Delta Asia in recent years, "only three individual, old \$100 bills were labeled as suspect. Not counterfeit, only suspect". 587

For Daedong and a number of Banco Delta Asia's other customers, there were few legal avenues they could pursue to have their funds unfrozen. Until the U.S. Treasury Department made a final determination regarding Banco Delta Asia's status as a "primary money laundering concern", the funds had to remain as they were.

7.4 All for one and one for all: Unilateral sanctions

Technically, the U.S. Treasury Department's notice of proposed rulemaking should not, in and of itself, have carried the degree of AML/CTF legal risk that it ultimately did. Indeed, the notice did not require U.S. financial institutions to cease their commercial dealings with Banco Delta Asia. It was simply a public statement putting such institutions on notice that in the future, restrictions *may* be placed upon their activities with the bank. Operationally

⁵⁸⁴ Op cit n580.

⁵⁸⁵ Chinoy, M., 'Macau Focus of Push on NK Activity', CNN News, 23 July 2006

<hattp://www.cnn.com/2006/WORLD/asiapcf/05/18/nkorea.Macau/index.html> at 2 January 2007. See also Greenless, D., Op cit n550.

Johnson, T., 'Seizure of a Tiny Bank Linked to N. Korea May Soon End', *Monterey Herald* (Monterey), 8 March 2007 http://www.montereyherald.com/mld/montereyherald/news/world/16862840.htm at 12 March 2007.

Thid.

however, the proposed rulemaking carried significant AML/CTF legal risk and had an immediate impact on the willingness of institutions to conduct business with Banco Delta Asia. Many institutions treated the notice as a formal, legal prohibition against dealings with the bank, and immediately began taking steps to terminate their relationships with Banco Delta Asia.

Several AML/CTF specialists have privately suggested that U.S. institutions started cutting all ties to Banco Delta Asia as a defensive or self-protective measure to limit their related AML/CTF legal risk. Given the extensive requirements placed upon them with respect to their correspondent banking relationships under the *USA PATRIOT Act*, it is possible that in the course of conducting their own due diligence on Banco Delta Asia, a number of U.S. institutions learned of the bank's dealings with North Korean government entities. If this is the case, then it is understandable from a risk mitigation perspective that these institutions might have sought to terminate their commercial dealings with Banco Delta Asia as soon as the U.S. Treasury Department's notice of proposed rulemaking was published.⁵⁸⁸

Without any clear evidence to the contrary, both U.S. and foreign financial institutions bestowed a de facto legal status upon the notice of proposed rulemaking in an effort to mitigate their own legal exposure. Whilst a proposed rulemaking under *Section 311* is neither formally binding nor enforceable, it certainly does indicate to institutions that the U.S. Treasury Department considers a particular entity/jurisdiction to represent an unacceptably high level of ML/TF risk. As previously noted in this thesis, AML/CTF regulators and institutions operating under risk-based regimes might occasionally have different views on the products/channels, customers and jurisdictions representing a particularly pronounced ML/TF risk. Notices of proposed rulemaking may be considered to partially close the gap between public and private sector perceptions of ML/TF risk because they provide institutions with a clear indication of the level of ML/TF risk assigned to a designated entity by U.S. regulatory authorities. Therefore, any failure on the part of a U.S. institution to address that perceived level of risk – even if not legally required to do so until the relevant

That said, there is no publicly available evidence to support the theory that particular institutions knew of, or condoned, the bank's relationships with allegedly corrupt North Korean customers.

rulemaking is finalised – may leave that institution exposed to a degree of legal and reputational risk.

In the aftermath of the U.S. Treasury Department's notice of proposed rulemaking, U.S. institutions were not the only entities to sever their commercial ties to Banco Delta Asia. Fearing their own exclusion from the U.S. banking system, many foreign financial institutions (including Korea Exchange Bank, Bank of Tokyo-Mitsubishi UFJ and Mizuho Corporate Bank)⁵⁸⁹ also ceased their dealings with the bank;⁵⁹⁰ effectively locking it out of USD business and much of the international financial system.⁵⁹¹ These institutions set off an informal financial embargo of the bank and Macau,⁵⁹² despite the fact that no U.S. law, regulation or rule actually prohibited them (or U.S. institutions for that matter) from conducting business with Banco Delta Asia at that time.⁵⁹³ The deterrent and indirect effects of this embargo were arguably as damaging, if not more damaging, than the ruling made by the U.S. Department of the Treasury in the first place.

The fact that many foreign financial institutions chose to voluntarily comply with the notice of proposed rulemaking as a matter of course is understandable. Since September 11, such institutions have increasingly been incorporating the U.S. Treasury's rules and designation lists into their own due diligence processes. This is not because they have been strictly required to follow the U.S. Treasury Department's directives, but because they have wanted to protect their own fiduciary interests. ⁵⁹⁴ Though most foreign financial institutions are geared towards profit-creation, the past few years have increased the need for them to balance their financial goals with their shareholder responsibility to manage commercial risks. Foreign institutions that ignore the U.S. Treasury Department's designations and

Anonymous, Hong Kong Joins Delta Asia's Unhappy Club, *Macau Business*, 1 March 2006. Accessed at http://www.Macaubusiness.com/index.php?id=402 on 18 January 2007.

⁵⁹⁰ Op cit n585, on 2 January 2007.

⁵⁹¹ 'No Sign of Thaw for Delta Asia', Macau Business, 1 January 2006

http://www.Macaubusiness.com/index.php?id=367> at 3 January 2007.

⁵⁹² Op cit n580.

Heller Ehrman LLP, Banco Delta Asia has Terminated its North Korean Business and Will Implement a New Anti-Money Laundering Program (2006)

http://www.hellerehrman.com/en/news/press/press 3289.html> at 3 January 2007.

Levitt, M., Pulling Tehran's Purse Stings: Leveraging Sanctions and Market Forces to Alter Iranian Behavior (2007) The Washington Institute http://www.washingtoninstitute.org/templateC07.php?CID=333 at 8 April 2007.

proposed rulemakings may find themselves locked out of the U.S. financial system as a result of a designation under *Section 311* of the *USA PATRIOT Act*.

The significant extraterritorial leverage that the U.S. Treasury Department has with respect to the activities of foreign institutions⁵⁹⁵ is cemented by the dominance of the U.S. in the international financial system. Whilst the U.S. remains at the core of the global economy, any institution seeking to conduct business internationally must be able to conduct transactions in USD. It follows that any jurisdiction seeking to protect (or indeed, grow) its economy must ensure that its financial institutions can access the U.S. financial system. Evidently, this is what a number of jurisdictions sought to do following the release of the U.S. Treasury Department's notice of proposed rulemaking. Shortly after Banco Delta Asia's initial designation as a "primary money laundering concern" under Section 311, a number of foreign FIUs (including the Hong Kong Monetary Authority) requested that all their local banks formally report any relationship they had with the bank. ⁵⁹⁶

Some foreign regulatory bodies and FIUs were slightly less direct in their guidance to financial institutions. For instance, Australia's AML/CTF regulator and FIU, AUSTRAC, released an Information Circular:

- informing Australian financial institutions of Banco Delta Asia's designation;
- giving such institutions access to the U.S. Treasury Department's related advisory; and perhaps most importantly
- informing them that they should take the U.S. government's advisory into account when "considering whether particular transactions should be reported to AUSTRAC as suspicious". 597

Whilst the Information Circular did not instruct Australian institutions that transactions involving Banco Delta Asia or Macau should be regarded as suspicious, in practical terms it is likely to have had such an effect. As with the U.S. Treasury Department's advisory and its

⁵⁹⁵ Ibid.

⁵⁹⁶ Op cit n566.

Australian Transaction Reports and Analysis Centre, AUSTRAC Information Circular No. 45 – U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN) – Advisory Regarding North Korea (2006) http://www.austrac.gov.au/files/aic_45_fincen_advisory_regarding_north_korea.pdf at 27 January 2009.

non-binding notice of proposed rulemaking, the Information Circular explicitly communicated to institutions the fact that AUSTRAC may be inclined to attach a higher level of ML/TF risk to dealings with the Macau bank, or Macau more generally.

7.5 PATRIOT Act politics

Section 311 of the USA PATRIOT Act has typically been characterised as a legal shield; an administrative procedure that can be used by the U.S. Treasury Department to protect the U.S. financial system from significant money laundering threats. However, the action taken against Banco Delta Asia demonstrates that whilst it may have initially been designed as a defensive measure, Section 311 is nevertheless capable of being wielded as a political sword for the purposes of attacking financial institutions and jurisdictions. This is particularly apparent when the events surrounding the bank's designation are viewed in terms of the political environment within which they occurred.

Whilst Banco Delta Asia's activities had allegedly been under the watchful gaze of several U.S. government agencies (including the U.S. Secret Service) since 1994,⁵⁹⁸ scrutiny of the bank's practices seemingly increased as the U.S. government intensified its efforts against North Korea. During 2005, the U.S. ushered in a political campaign that sought to curb North Korea's illicit activities by cutting off the country's access to foreign financial institutions and the international banking system.⁵⁹⁹ As this campaign gained greater momentum, so too did the regulatory and commercial pressure placed upon Banco Delta Asia.

At this time, several officials of Zokwang Trading Co., a Macau firm run by North Koreans, were arrested by Macau police on suspicion of attempting to pass a large number of counterfeit U.S. bills. Some of these bills were later traced to Banco Delta Asia.

Gertz, B., 'U.S. Sanctions Cost North Korea Millions', *The Washington Times* (Washington D.C.), 16 June 2006 http://www.washingtontimes.com/national/20060615-105145-9374r.htm at 18 January 2007. See also Chinoy, M., Op cit n585.

7.5.1 The involvement of North Korea

At the time the U.S. Treasury Department published its notice of proposed rulemaking under *Section 311*, the U.S. and North Korea had long been embroiled in a dispute regarding North Korea's nuclear program and alleged criminal activities. Interestingly however, Banco Delta Asia's designation occurred just as the U.S. had commenced delicate multilateral negotiations (**the six-party talks**) in relation to North Korea's nuclear weapons development program. This timing raises some suspicion about whether the bank simply became a victim of a strategic game of 'cat and mouse' led by the U.S. and intended to isolate North Korea throughout the nuclear negotiations.

As previously discussed in **Chapter 3** of this thesis, since the events of September 11 the U.S. government has increasingly used economic sanctions and other financial measures to degrade the "ability of state sponsors of terror and [weapons] proliferators to access the international and U.S. financial system".⁶⁰⁴ In recent years, the U.S. has demonstrated a heightened interest in combating nuclear proliferation by:

- taking steps to implement UNSCRs 1540, 1695, 1718, 1737 and 1747;
- encouraging other jurisdictions to implement activity-based financial prohibitions against countries with nuclear programs; and
- designating ten individuals and entities as supporters of North Korea's missile and
 Weapons of Mass Destruction programs.

The FATF has generally supported and supplemented these actions by adding nuclear proliferation financing to its focus of attention, developing a study on the trends and

⁶⁰⁰ 'Macau Bank drops North Korean Clients', *BBC News*, 16 February 2006 http://news.bbc.co.uk/1/hi/business/4718922.stm at 2 January 2007.

These negotiations were referred to as the "six-party talks" because they involved six jurisdictions; North Korea, China, Japan, South Korea, Russia and the United States.

Simpson, G.R., Fairclough, G., and Solomon, J., 'U.S. Probes Banks' North Korea Ties', The Wall Street Journal (New York), 8 September 2005, A.3.
 Op cit n591.

Glaser, D., and Szubin, A.J., 'Isolating Proliferators and Sponsors of Terror: The Use of Sanctions and the International Financial System to Change Regime Behavior' (Joint Testimony before the Joint Hearing of the Terrorism, Non-proliferation & Trade Subcommittee of the House Foreign Affairs Committee & the Domestic and International Monetary Policy, Trade & Technology Subcommittee of the House Financial Services Committee, 110th Congress, 18 April 2007).

techniques associated with proliferation financing activities, ⁶⁰⁵ and releasing guidance on the implementation of relevant UNSCRs. ⁶⁰⁶

The timing of Banco Delta Asia's designation suggests that the U.S. Treasury Department's notice of proposed rulemaking was not intended to safeguard the U.S. financial system but rather, was fundamentally designed to weaken North Korea's negotiation powers in the lead-up to the six-party talks. As at September 2005, Banco Delta Asia was one of the few remaining institutions providing banking services to North Korean government entities. As a result, the notice of proposed rulemaking not only placed significant pressure on the Macau bank to cease dealing with North Korea, but also prompted a number of foreign financial institutions to do the same. According to one of the U.S. Treasury Department's senior officials, Banco Delta Asia's designation as a "primary money laundering concern" was essentially a "shot heard round the world for national bankers who cut off relations with North Korea, fearing that something like what happened to [the Macau bank] could happen to them". In practical terms, Banco Delta Asia's designation dismantled North Korea's financial flows and cut off one of the impoverished country's few remaining lifelines to the international banking system.

If the U.S. Treasury Department's ultimate goal was to exert financial pressure on North Korea in the lead-up to the six-party talks, it succeeded – if not a little too spectacularly. The implications of its notice of proposed rulemaking affected North Korea so greatly that the country blatantly refused to join the nuclear negotiations until the financial constraints upon Banco Delta Asia were removed. Whilst this ultimatum may have been designed to stall North Korea's participation in the six-party talks, it had negative repercussions for the bank. At the very least, it further blackened Banco Delta Asia's reputation by validating that the

⁶⁰⁹ Op cit n546.

Sassoon, J., 'Chairman's Address' (Paper delivered at the Financial Action Task Force, Paris Plenary, 12 October 2007) 3 http://www.fatf-gafi.org/dataoecd/0/23/39485130.pdf at 5 February 2008.

⁶⁰⁶ Financial Crimes Enforcement Network, Advisory: Guidance to Financial Institutions on the Increasing Money Laundering Threat Involving Illicit Iranian Activity, FIN-2007-A001, 16 October 2007. Accessed at http://www.fincen.gov/guidance_fi_increasing_mlt_iranian.pdf on 5 February 2008.

⁶⁰⁷ Op cit n600.

McGlynn, J., Banco Delta Asia, North Korea's Frozen Funds and US Undermining of the Six-Party Talks: Obstacles to a Solution. Part III (2007) Japan Focus < http://www.japanfocus.org/-John-McGlynn/2446> at 5 May 2009.

steps taken against it by the U.S. government were having a material affect upon North Korea.

To convince the traditionally intransigent North Korea to rejoin the stalled six-party talks, the U.S. government agreed to explore the possibility of removing the financial constraints it had placed upon Banco Delta Asia. Following this, the nuclear negotiations again resumed until North Korea demanded that the USD\$25 million it had frozen in accounts at Banco Delta Asia, be unfrozen and deposited into an account held at the North Korean Foreign Trade Bank. This could not occur until such time as U.S. authorities made a final determination with respect to Banco Delta Asia's alleged activities. Thus, in an effort to further progress the discussions around North Korea's nuclear program, the U.S. government agreed to swiftly conclude its investigation into Banco Delta Asia's alleged money laundering activities. Whilst the investigation had previously proceeded at a relatively sluggish pace for the preceding 18 months, it was completed less than one month after the U.S. government's agreement with North Korea.

Shortly after the conclusion of its investigation, the U.S. Treasury Department finalised its proposed rulemaking on 14 March 2007. In doing so, it cleared the way for North Korea to reclaim its frozen funds and gave Macau authorities the power to determine whether to release those funds. However, whilst the finalisation of the rulemaking technically rendered the MAM responsible for deciding whether to release the frozen funds to its North Korean customers, its ability to make such a decision impartially was undermined by the U.S. government. Even before any such determination could be made by the MAM, the U.S. Department of State had already assured North Korean officials that the funds would be transferred to a North Korean-owned account held at the Bank of China.

Given the agreement between the U.S. and North Korean governments, it is highly debateable whether the Macau authorities ever had any real discretion regarding the release

⁶¹⁰ Cody, E., 'U.S. Says Macau to Release \$25M in Frozen N. Korean Funds', *The Washington Post* (Washington D.C.), 10 April 2007 http://www.washingtonpost.com/wp-dyn/content/article/2007/04/10/AR2007041000165.html?hpid=moreheadlines at 17 April 2007.

United States Department of the Treasury, Statement by DAS Glaser on the Disposition of DPRK-Related Funds Frozen at Banco Delta Asia (Press Release, 19 March 2007).

of the frozen funds. North Korea had already declared that it would not shut its main nuclear reactor until the frozen funds were released, and the MAM would have been acutely aware of the fact that any delay in returning the USD\$25million may have derailed the six-party talks and further aggravated the situation between Macau and the U.S. By that stage, the Macau government already understood first-hand just how much damage could be suffered by jurisdictions seen to be non-cooperative in the U.S.-led war on terror.

At the time of finalising the proposed rule against Banco Delta Asia, the U.S. Treasury Department stressed its ability to review and rescind the special measure prohibiting U.S. institutions from maintaining correspondent or interbank accounts on behalf of the bank. Given that the U.S. government had already beaten Macau and Banco Delta Asia with a very big 'stick' before dangling an equally big 'carrot' in front of them, it is understandable that Macau officials decided to release the frozen funds to North Korea. Strategically, freeing up those funds would enable the MAM to pacify the U.S. government, minimise its reputational damage, and lessen its ongoing AML/CTF legal risk.

7.5.2 A trial with a jury (but without evidence)

By making certain allegations against Banco Delta Asia, the U.S. government was clearly able to place significant economic pressure upon North Korea in the lead-up to delicate nuclear negotiations. As noted earlier, this calls into question whether the U.S. government made unverified or exaggerated claims against the bank in order to strain North Korea's finances and freeze more than USD\$25 million in its accounts. Suspicions regarding the U.S. Treasury Department's motives are merely bolstered by the timing of the six-party talks, the apparent lack of evidence supporting its allegations, and the fact that two

^{612 &#}x27;China says it Regrets US Treasury Decision on N. Korea', CNN News, 15 March 2007

http://edition.cnn.com/2007/WORLD/asiapcf/03/15/china.macau.bank.reut/index.html at 20 March 2007.

613 Lague, D., 'Macao Set to Resolve North Korea Snag, U.S. Says', The New York Times (New York), 11

April 2007 http://www.nytimes.com/2007/04/11/world/asia/11korea.html at 17 April 2007.

The U.S. Treasury indicated that this would perhaps be the case where Banco Delta Asia took further remedial steps to change its business methods, and was brought under the long-term control of responsible management and ownership.

Landay, J.S., and Hall, K.G., 'U.S. Claims about Macau Bank Questioned', *The Seattle Times* (Seattle), 2 March 2007 http://archives.seattletimes.nwsource.com/cgibin/texis.cgi/web/vortex/display?slug=nkorea02&date=20070302 at 12 March 2007.

subsequent investigations into the bank's activities failed to find any evidence that it laundered money for North Korean customers.

Within days of the release of the U.S. Treasury Department's notice of proposed rulemaking in September 2005, the Macau government engaged international accounting firm Ernst & Young to investigate Banco Delta Asia's supposed activities. At the conclusion of that investigation, Ernst & Young criticised the bank's internal record keeping procedures, poor information technology systems and lack of written AML policies, but held that it could find no evidence of the bank laundering money for North Korean government agencies or front companies. Another investigation carried out by the Macau Government confirmed this finding and was also unable to identify any evidence of criminal misconduct by Banco Delta Asia or its employees.

Regardless of the findings (or lack thereof) stemming from these two external investigations however, the U.S. Treasury Department has continued to stand by its original allegations against Banco Delta Asia. Without mentioning either investigation into the bank's dealings, officials from the U.S. Treasury Department have declared that their own 18-month investigation confirmed Banco Delta Asia's alleged "willingness to turn a blind eye to illicit activity, notably by its North Korea-related clients". However, U.S. authorities have never publicly provided further evidence to substantiate this assertion.

7.5.3 Justification for the lack of evidence

Whilst the U.S. Treasury Department has continually held that Banco Delta Asia is of "primary money laundering concern", it has garnered little evidence to support its claims. To this day, the results of the U.S. Treasury Department's extensive 18-month investigation into Banco Delta Asia remain confidential. The Macau institution has never been given an

Hall, K.G., 'Accounting Firm Finds No Evidence of Money Laundering', McClatchy Newspapers (Sacramento), 1 March 2007 < http://www.realcities.com/mld/krwashington/16812231.htm at 12 March 2007

^{&#}x27;Treasury Bars Deals with Macau's Banco Delta', CNN News, 14 March 2007

http://money.cnn.com/2007/03/14/news/international/macau.reut/index.htm?postversion=2007031417 at 20 March 2007.

opportunity to see, let alone evaluate or challenge, the evidence used to justify its designation under Section 311.618 However, this is not particularly unusual for an action taken under Section 311. Given that many designations under that Section have been hinged upon classified information, institutions deemed to be of "primary money laundering concern" have generally been denied access to, and an ability to refute, the alleged evidence against them.

What makes the situation with respect to Banco Delta Asia so troubling is that the U.S. Treasury Department has not only refused to release any incriminating evidence it has about the bank to the public, but also to present any such evidence to U.S. Congress – in either an open or closed session of one of its oversight committees. 619 This has prompted some commentators to speculate that in the course of making the bank the subject of a Section 311 designation, the U.S. government simply conducted a 'kangaroo court', with its "verdict being justified retrospectively through a drip feed of innuendo and speculation that would be considered scandalous and defamatory were it directed against a bigger bank in a more powerful jurisdiction".620

Arguably, the U.S. Treasury Department's evasiveness regarding the justification for its proposed and final rules makes Banco Delta Asia's designation appear more like part of a political campaign than any substantive regulatory action. It also raises questions around whether the U.S. government's refusal to provide evidence of the bank's alleged activities is fair or just, considering the financial and reputational damage suffered by the institution in the aftermath of the proposed rulemaking.

Nowhere does the USA PATRIOT Act require the U.S. government to formally unveil any evidence it has to support an action taken against a foreign financial institution under Section 311. Thus, despite any perception of unfairness towards Banco Delta Asia, the U.S. Treasury Department has acted within its legal rights when refusing to present evidence supporting the bank's designation. Due to the foreign nature of the threats covered by

⁶¹⁸ Op cit n553.
619 Op cit n559.
620 Op cit n591.

Section 311, the evidence underpinning a designation may be comprised of sensitive intelligence that is classified and protected from public disclosure. Accordingly, the U.S. Treasury Department was entitled to deem Banco Delta Asia a "primary money laundering concern" without furnishing any evidence to substantiate its accusations.

The issue over how much evidence, if any, should be provided with respect to allegations made against a designated institution, is an interesting one. As already established, Section 311 of the USA PATRIOT Act effectively enables the U.S. Treasury Department to 'defame' a foreign entity or jurisdiction without publicly presenting any supporting evidence. It legally empowers the U.S. government to punish and reprimand any foreign institution of its choosing, and simply hide behind an opaque veil of 'national security' to prevent the subjects of its designations from formally contesting their status as a "primary money laundering concern".

That said, given that money laundering relies upon the creation of transactional veils of anonymity, perhaps the withholding of evidence is simply a way for the U.S. Treasury Department to 'fight fire with fire' so to speak; addressing money laundering using one of its key elements – secrecy. It may be argued that presenting comprehensive evidence in support of a designation or proposed rule could actually weaken the U.S. government's ability to combat money laundering and terrorism financing abroad. Sharing intelligence with respect to an institution's illicit activities could enable other entities to modify their money laundering methods in order to evade similar detection.

Conversely however, it may be contended that publicly releasing such intelligence will only strengthen the U.S. Treasury Department's ability to combat financial crime. As evidenced by the various typologies released by national regulators and international bodies such as the FATF, one of the most effective tools in the fight against money laundering is knowledge about its existence and the ways it may be facilitated. Whilst the provision of evidence may enable some institutions to reengineer their money laundering methods, it may allow many more to appropriately refine their AML/CTF detection scenarios, strengthen their transaction monitoring capabilities and improve their staff training.

Regardless of the various arguments regarding whether or not the U.S. Treasury Department should provide evidence to justify a foreign financial institution's designation under the USA PATRIOT Act, there has been a growing push for the U.S. government to publicly release evidence of Banco Delta Asia's allegedly illicit dealings. However, even if it were now to release its evidence against the bank and, as anticipated by Macau officials and Banco Delta Asia's management, such evidence was deemed to be fabricated or flawed, it is questionable what this would achieve - beyond perhaps assisting the bank to claim a moral victory and rebuild some of its diminished credibility. Much of the damage suffered by Banco Delta Asia occurred in the immediate aftermath of its designation.

As perception is generally considered to be reality in today's commercial environment, the lack of evidence provided by the U.S. Treasury Department around its notice of proposed rulemaking, did not prevent the Macau bank from incurring a run on its deposits, or suffering significant reputational and financial damage. The mere suggestion that Banco Delta Asia had laundered money for North Korea was enough to blacken its name and empty its accounts. Any evidence to the contrary now would do little, if anything, to recoup the losses already sustained by the Macau institution.

7.5.4 Banco Delta Asia's legal position

Whilst a spokesperson for the U.S. Treasury Department has claimed that accused institutions have rights and maintain the ability to challenge any action taken against them under Section 311,621 this only appears to be true in theory as opposed to in practice. Two years after the U.S. Treasury Department finalised its proposed rulemaking, the legal wrangling around Banco Delta Asia's designation and the release of any supporting material retained by the U.S. government, continues. Shortly after the final rule was codified, legal representatives for both Banco Delta Asia and its parent company submitted petitions to the U.S. Treasury Department claiming that the final rule was "arbitrary and capricious", and demanding that it be "rescinded immediately". 622 However, the arguments underpinning these petitions remain almost as shrouded in secrecy as the U.S. Treasury Department's

⁶²¹ Op cit n553. ⁶²² Op cit n559.

supposed evidence. The full contents of the petitions have never been formally released and those members of the public seeking to access them must file a Freedom of Information request in the U.S.

Whilst it is uncertain whether the U.S. Treasury Department has ever formally responded to the petitions, Banco Delta Asia still appears to have one primary legal avenue open to it. Whilst it cannot pursue damages for the reputational and financial damage it sustained following its designation, the bank can file a suit in a U.S. Federal Court seeking the removal of the final rule on both substantive and legal grounds. In accordance with its petition, the bank could theoretically contend that the imposition of the special measure was "arbitrary and capricious". Further, it could argue that the U.S. Treasury Department did not have reasonable grounds under Section 311 to conclude that it was a "primary money laundering concern". 623

However, despite the technical availability of this legal avenue, it is debateable whether Banco Delta Asia could ever succeed with such an action. This is particularly so, given that the bank's legal representatives are unlikely to be given full access to the U.S. government's alleged evidence. The U.S. Treasury Department's 18-month investigation into the institution was heavily reliant upon classified sources, and according to a footnote accompanying the final rule, "[c]lassified information used in support of a [Section 311 designation] and imposition of special measure(s) may be submitted by Treasury to a reviewing court ex parte and in camera". Thus, in any court proceedings, the U.S. government could potentially present its evidence behind closed doors, depriving Banco Delta Asia of the opportunity to hear the evidence against it.⁶²⁴

Banco Delta Asia cannot take any decision about the initiation of legal proceedings lightly. There is no guarantee that such proceedings would be successful, and there is every probability that they would be costly, resource intensive and further damaging to the bank's reputation. Considering that no foreign institution has ever been successful in seeking to

⁶²³ Ibid.

⁶²⁴ Ibid.

have a final rule rescinded by the U.S. Treasury Department, the institution may consider its legal options and determine that the best way to mitigate its ongoing legal, financial and reputational risk is in fact not to formally contest the rulemaking through the U.S. legal system.

7.6 Risk implications

Banco Delta Asia's designation as a "primary money laundering concern" under Section 311 of the USA PARTIOT Act illustrates the significant AML/CTF legal risk faced by institutions with supposed ties to customers and/or jurisdictions considered by the U.S. government to be conducting illicit activities. It also showcases the significant financial loss and reputational damage that may stem from the imposition of a special measure under U.S. extraterritorial AML/CTF laws. Whilst an institution's AML/CTF legal risk typically hinges upon formal legal proceedings, fact-finding exercises, the provision of supporting evidence and formal judgments, Banco Delta Asia's designation demonstrates the extent to which it may arise in isolation from these factors; instead being determined by political agendas and international relations.

The case highlights how an institution that is never sent to trial for money laundering offences, can nevertheless be tried and convicted of such offences in the courts of public opinion. The U.S. Treasury Department's claims that Banco Delta Asia laundered money on behalf of North Korean agencies and front companies, were sufficient to cause the bank significant reputational and financial damage. Although unsupported by publicly available evidence, they caused an extensive run on the bank's deposits and prompted its customers to empty their accounts. Essentially, the U.S. Treasury Department's allegations saw Banco Delta Asia publicly convicted of money laundering – even though the bank never had an opportunity to see the evidence against it or defend itself in the course of formal legal proceedings.

Banco Delta Asia also demonstrates the way in which an institution's size and AML/CTF legal risk may be inversely proportionate. According to a former official of the U.S.

Department of State, despite the fact that the U.S. Treasury Department had evidence that several Macau institutions had laundered counterfeit funds for North Korean entities, Banco Delta Asia proved to be an easy target for the imposition of a special measure. The bank was large and important enough to have an impact on North Korea's financial flows, but not so large and important that its blacklisting or failure would cause excessive damage to Macau's financial system or create significant political tension between the U.S. and China. If this is correct, then it may be that the size of Banco Delta Asia's operations left it exposed to a greater level of AML/CTF legal risk than other institutions with a more notable presence in Macau's financial system and/or international commerce.

In addition to its teachings on the potential relationship between an institution's size and its level of AML/CTF risk, Banco Delta Asia provides a striking example of the various ramifications that may stem from an institution's alleged involvement in money laundering activities and/or on-boarding of customers deemed by the U.S. to be undesirable. It also proves that an institution can survive the imposition of the harshest sanction under U.S. extraterritorial AML/CTF legislation. Despite having its reputation shredded and its deposits withdrawn following its designation as a "primary money laundering concern" in September 2005, Banco Delta Asia is still – years later – operational in Macau. Whilst it may not have the extensive network of correspondent banking relationships that it once did, the fact that it still provides banking services to customers, demonstrates that an institution may recover from even the most strenuous attack on its credibility. It also undermines the common claims that an institution believed to be involved in money laundering activities may face irreparable damage and, in severe cases, closure. Banco Delta Asia has survived the imposition of one of the most extreme extraterritorial sanctions; namely, exclusion from USD business and the U.S. financial system.

Whilst illustrating the practical operation of a bank's legal, financial and reputational risk, the events surrounding Banco Delta Asia's designation illustrate the systemic risk that may

625 Op cit n559.

Greenlees, D., and Lague, D., 'The Money Trail That Linked North Korea to Macao', *The New York Times* (New York), 11 April 2007 < http://www.nytimes.com/2007/04/11/world/asia/11cnd-macao.html at 5 July 2008.

emanate from an institution's dealings with supposedly tainted funds and/or jurisdictions considered to represent an unacceptably high level of ML/TF risk. Almost 18 months after the U.S. Treasury Department's notice of proposed rulemaking, HSBC found itself the subject of unflattering media reports after sources revealed that it had been responsible for screening all the large cash deposits made by Banco Delta Asia's North Korean customers.

In early 2007, a lawyer for Banco Delta Asia told U.S. investigators that HSBC's New York branch analysed all wholesale USD deposits for the bank before they were credited to depositors' accounts. As Banco Delta Asia did not have the technology necessary to screen large batches of U.S. currency for fake bills, it relied upon HSBC's sophisticated processing technology to identify any counterfeit funds entering its accounts. However, whilst it has never denied screening the suspect North Korean funds for Banco Delta Asia, HSBC has never been reprimanded – formally or informally – by the U.S. Treasury Department. Even if it had incurred similar financial and reputational consequences to Banco Delta Asia, it is highly unlikely to have felt them considering its size, the scope of its international operations, and the profits enshrined in its balance sheets.

Nevertheless, the fact that HSBC screened all wholesale USD cash deposits for Banco Delta Asia strongly supports the view that the U.S. government's case against the Macau institution is weak. It not only raises concerns regarding the potential unreasonableness of the bank's designation as a "primary money laundering concern", but brings into sharp focus the unaccountability of the U.S. government in the broader international fight against money laundering.

7.6.1 Risk management for institutions

In terms of risk management, it is unclear exactly what Banco Delta Asia could have done to avert, or even better mitigate, the fallout arising from its dealings with North Korean entities. Unlike Riggs Bank and other institutions found to be in breach of their AML/CTF legislative

⁶²⁷ Courtenay, A., 'HSBC Screened N Korean Assets for Macau Bank' (2007) 14 Money Laundering Intelligence 4.

⁶²⁸ Op cit n615.

obligations, there were few risk mitigation tools available to Banco Delta Asia. Given the expansive construction of *Section 311* and the fact that designations under that Section do not entail or require formal legal proceedings, many of the risk management techniques detailed in **Chapter 5** of this thesis have not been available to the bank. Given the absence of formal legal proceedings, it could not self-report its allegedly suspect customer transactions to U.S. authorities (and indeed, it was under no obligation to), seek a deferred or non-prosecution agreement, or deflect its liability by mounting a legally recognised defence. The action taken against Banco Delta Asia under the *USA PATRIOT Act* was virtually incontestable; shrouded in secrecy and backed by one of the most powerful governments in the world.

Not all of the four traditional risk management strategies could have been effectively used by the bank to safeguard its reputation, deposit base and commercial standing. Risk avoidance might have been a financially viable option for Banco Delta Asia if, as held by some of its representatives, the relevant North Korean accounts only constituted three per cent of its total business. Whilst losing that percentage of its funds is likely to have been undesirable for any bank, for a small, family-owned institution such as Banco Delta Asia, three per cent of its total business is clearly far less than the financial damage it ultimately sustained as a result of its designation as a "primary money laundering concern".

That said, given that the U.S. government supposedly knew of the bank's long-standing relationship with North Korea for more than 20 years before publishing its notice of proposed rulemaking in September 2005, Banco Delta Asia is unlikely to have believed that the adoption of a risk avoidance strategy – and the consequent termination of its commercial ties to North Korea – was necessary. This is apparent considering that Banco Delta Asia had only encountered one instance of counterfeit U.S. currency prior to its designation. That was in 1994, when the bank identified two deposits of counterfeit U.S. currency and immediately informed the Macau police and the MAM of its suspicions regarding the legitimacy of the

funds. Its proactive reporting led to criminal charges being laid against the relevant account holders, and Banco Delta Asia never suffered any repercussions as a result of the incident.⁶²⁹

Although the adoption of a risk acceptance strategy might have sounded like an inappropriate option for Banco Delta Asia, this is seemingly the approach taken by the bank. For several decades, the bank continued to accept customers domiciled in North Korea – a jurisdiction fiercely at odds with the U.S. over a range of domestic and international issues. Whilst the U.S. government may have known of this fact for many years before designating Banco Delta Asia a "primary money laundering concern", the significant financial and reputational damage stemming from that designation demonstrates that the adoption of a risk acceptance strategy left the institution exposed to a number of risks, and related consequences.

Whilst Banco Delta Asia's employment of a risk acceptance strategy was likely to be unintentional and inadvertent (arguably, the institution never appreciated the risks it was accepting in the first place), so too was its partial adoption of a risk transfer strategy. By engaging HSBC New York to screen all large cash deposits received from its North Korean customers, Banco Delta Asia was able to transfer some of the ML/TF risk inherent in its business dealings with North Korean customers. Whilst the bank's decision to outsource its deposit screening functions was most likely a commercial decision driven by a lack of technological capability rather than any risk management concerns, its practical effect was to transfer a degree of AML/CTF legal risk to HSBC New York. Though it ultimately did not spare Banco Delta Asia from becoming the subject of a designation under *Section 311*, the revelation that HSBC New York actually vetted the suspect deposits should have lessened – at least theoretically – some of the fierce criticism previously shouldered by Banco Delta Asia.

Given the limitations of a risk transfer strategy, Banco Delta Asia may have supplemented its risk transfer activities with a number of controls designed to mitigate its AML/CTF legal risk

⁶²⁹ It should be noted however, that this situation occurred prior to September 11 and before AML/CTF issues were thrust upon the global stage and elevated in terms of their importance to U.S. national security.

under U.S. extraterritorial AML/CTF legislation. Whilst two investigations into the bank's dealings have failed to identify any evidence that it laundered money for North Korean government entities or front companies, they have highlighted ways in which the bank could have better managed its ML/TF risk through the implementation of tighter AML/CTF controls. For instance, the bank could have mitigated its ML/TF risk exposure by improving its transaction monitoring capabilities, conducting enhanced due diligence on its North Korean customers, and implementing a more effective AML/CTF program.

However, despite the AML/CTF controls and risk management strategies ultimately employed by Banco Delta Asia, the bank's designation might have arisen irrespective of the additional safeguards it implemented. Due to the political context and environment within which the designation occurred, employing stronger AML/CTF controls may have ultimately made little difference to the detriment inevitably suffered by the institution. If, as believed by many commentators, Banco Delta Asia was simply "a pawn on the chessboard of [the six-party] talks", 630 it is unlikely that any risk management strategy would have been capable of sparing the bank from its designation and the notice of proposed rulemaking issued by the U.S. Treasury Department in September 2005.

7.7 Conclusion

Banco Delta Asia's designation as a "primary money laundering concern" under Section 311 of the USA PATRIOT Act, demonstrates the way in which business, politics, statesponsored crime and AML/CTF legislation may intersect on the global stage. It highlights the fact that an institution's AML/CTF legal risk is not limited by geographic borders or the confines of domestic AML/CTF legislation. Such risk may also arise as a result of extraterritorial laws, the activities of foreign AML/CTF regulators and even, on occasion, political tensions between foreign jurisdictions.

Section 311(c)(2)(B) explicitly states that the purpose of Section 311 is to "guard against international money laundering and other financial crimes". However, whilst the special

⁶³⁰ Op cit n546.

measures enshrined in the *USA PATRIOT Act* may be intended to provide the U.S. government with an economic shield that can be used to protect the country's financial system, their invocation in relation to Banco Delta Asia suggests that they may also be used as a political sword to pursue the government's international agenda. Given the relative timing of Banco Delta Asia's designation and the commencement of the six-party talks, it may be contended that the U.S. Treasury Department ostensibly used *Section 311* to weaken North Korea's bargaining power in the lead-up to the delicate nuclear negotiations. The bank's designation and the publication of a proposed rulemaking had undeniable financial consequences for North Korea at a time when greater financial stability would have enabled the typically intransigent country to resist the U.S. government's persistent attempts to shut down its nuclear program.

Thus, although the U.S. Treasury Department has repeatedly claimed that Banco Delta Asia represents an unacceptable money laundering risk, some commentators have questioned whether its designation is solely attributable to the U.S. government's concerns about "Macau, Macau's government, China, the Chinese government and their complicity and their accommodative behavior toward North Korea's illegal activities, proliferation activities and leadership financial activities". ⁶³¹ If this is indeed the case, the U.S. Treasury Department's actions under the USA PATRIOT Act might have somewhat undermined international AML/CTF efforts. By politicising AML and taking actions that may be viewed as an abuse of power (even if such actions fall within the boundaries of municipal U.S. legislation), support for U.S. enforcement proceedings and AML/CTF activities may diminish amongst other foreign governments. If it appears that the U.S. government and U.S. regulatory authorities are enforcing their AML/CTF laws selectively and according to the political climate at any point in time, foreign officials may believe that their own AML/CTF efforts are potentially powerless to prevent their country/financial institutions from feeling the wrath of a Section 311 designation.

In the event that Banco Delta Asia simply became an unwitting pawn in the U.S. government's strategy to fight the war on terror via corporate balance sheets, it is likely to

⁶³¹ Op cit n580.

have been inconsequential what risk management strategy/strategies the institution employed with respect to its AML/CTF legal risk under the *USA PATRIOT Act*. Its inherent ability to identify, mitigate and manage its ongoing risk would have always been constrained by the U.S. government's political imperatives and international influence. Even if the bank had previously implemented an AML/CTF program, it may nevertheless been deemed a "primary money laundering concern" under Section 311.

The case of Banco Delta Asia illustrates that whilst institutions can design and employ elaborate risk management tools and strategies, these will generally be unable to anticipate or counter strong external forces such as foreign politics and international relations. Where a powerful, foreign government decides to declare, retrospectively, that an institution has engaged in questionable business practices and/or otherwise dealt with undesirable customers, the institution will generally be powerless to defend itself. As the case of Banco Delta Asia demonstrates, no risk management tool or strategy will ever be capable of entirely safeguarding an institution against potential reputational damage, particularly in circumstances where members of the global community are willing to accept something for which they have no hard evidence.

As opposed to many other recent, high profile cases of corporate money laundering, there is a distinct lack of transparency with respect to Banco Delta Asia's designation, and the apparent activities leading to that designation. There is surprisingly little documentation available to the public in relation to those factors identified by the U.S. Treasury Department as rendering the bank a "primary money laundering concern". However, in addition to the lack of supporting evidence provided by the U.S. Treasury Department, the MAM has also offered little information in relation to its subsequent reviews of Banco Delta Asia's dealings with North Korean customers. Both the MAM's 2005 and 2006 annual reports fail to mention the bank or the actions taken against it by the U.S. Treasury Department. This is despite the size of Macau's economy, the limited number of independent financial institutions operating there, and the fact that the U.S. Treasury Department's actions against Banco Delta Asia would have created one of the most pressing international regulatory issues for the MAM in recent times, if not ever.

In the absence of publicly available, incriminating evidence with respect to its alleged money laundering activities, Banco Delta Asia was seemingly convicted of such activities by members of the international community willing to accept the U.S. Treasury Department's claims without question. Evidently, the U.S. government has an unparalleled ability to enact municipal orders that are so sweeping in scope that they ultimately translate into informal international sanctions. The run on Banco Delta Asia's deposits and the termination of many of its correspondent banking relationships occurred because the U.S. Treasury Department's notice of proposed rulemaking assumed a de facto legal standing beyond U.S. borders. Though not legally bound to do so, many foreign financial institutions promptly cut commercial ties to, and many foreign AML/CTF regulators discouraged dealings with, the Macau bank.

As a result, Banco Delta Asia suffered significant reputational and financial damage in the aftermath of its designation under *Section 311*. As a result of the U.S. Treasury Department's unsupported accusations and innuendos, the bank lost a significant number of its customers, deposits and commercial relationships. Nevertheless, it should be noted that two years after the U.S. Treasury Department finalised its rulemaking and formally barred U.S. institutions from conducting business with Banco Delta Asia, the Macau bank is still operating. This tends to dispel the common assertion that an institution's alleged involvement in a money laundering scandal may prove to be institutionally fatal. The bank's continued existence shows that even where an institution incurs the most severe penalty available under extraterritorial AML/CTF laws, it may still survive commercially – albeit in a greatly restricted capacity.

Chapter 8

Conclusion

"We need to ensure that we do not impose regulatory requirements on the industry without the promise of real anti-money laundering and anti-terrorist funding benefits" — Robert Werner

8.1 The front line

Risk-based approaches to AML/CTF inherently recognise the ability – and indeed, the responsibility – of financial institutions to reinforce international security. Accordingly, whilst the popularity of risk-based regimes continues to grow, institutions are increasingly expected to act as the first line of defence against money laundering and terrorism financing activities. They are required to manage their ongoing ML/TF risk, and take responsibility for implementing systems and controls commensurate to that risk. Whilst risk-based approaches to AML/CTF do not anticipate that institutions will necessarily be able to prevent all possible instances of money laundering and terrorism financing, they do expect that such entities will mitigate the ML/TF risk represented by their businesses.

In risk-based AML/CTF regimes, an institution's risk is not confined to situations where it has actively facilitated money laundering or terrorism financing activities. It may also extend to circumstances where it has flouted or fallen short of compliance with legislative risk-based requirements (for instance, by failing to train or screen employees in accordance with the ML/TF risk represented by their role/business unit). Although non-compliance with risk-based requirements may not carry the same emotional response or attract the same reputational risk as the commission of a money laundering/terrorism financing offence, it may nevertheless see an institution suffer legal, financial and reputational damage.

⁶³² Hoffman, K.E., 'AML Security Emphasizes Detection and Prevention' (2005) 81(1) Banking Strategies 54.

Whilst institutions in many jurisdictions have lobbied for risk-based AML/CTF regimes, it is clear that compliance with risk-based legislative requirements may at times prove challenging for regulated entities. They might find it operationally difficult to identify their ML/TF risk profile, and conceptually difficult to determine what they should consider to be an acceptable risk and an acceptable cost. Given the various points of view from which the acceptability (or otherwise) of particular ML/TF risks can be judged, some institutions might be at a loss to identify the potential consequences attached to accepting, mitigating or avoiding different risks.

Drawing on the conclusions reached in the preceding Chapters of this thesis, this Chapter seeks to:

- identify the types of risk and the levels of risk that institutions operating under certain risk-based regimes are likely to face;
- challenge the common assertion that breaches of AML/CTF legislation may lead to the imposition of financially debilitating, or even commercially fatal, penalties;
- discuss and critically analyse some of the apparent benefits of risk-based approaches to AML/CTF; and
- provide an overview of the way in which AML/CTF issues and risk-based AML/CTF regimes can help enrich institutional understandings of the phenomena of risk.

8.2 The importance of understanding and assessing ML/TF risk

Considering that risk-based AML/CTF regimes require regulated entities to be accountable for their own ML/TF risk profile, it is imperative that financial institutions understand how to (and indeed, how they are expected to) identify, assess, evaluate and treat their ML/TF risk exposures. As discussed in **Chapter 2** of this thesis, the assessment and ongoing management of ML/TF risk has received heightened attention during the past two decades as risk-based approaches to AML/CTF have been adopted in a number of jurisdictions.

⁶³³ Op cit n15. 8.

Although money laundering received some legislative attention during the 1980s, it was not until the 1990s that the scope and the broader ramifications of this crime were acknowledged. At that time, national governments and international bodies began to acknowledge that money laundering was not simply a 'local' crime related to the drug trade, but an 'international' crime associated with many kinds of illicit activities. Further, they became increasingly aware of the need to work cooperatively with financial institutions to combat money laundering activities and prevent money launderers from accessing the broader financial system. Whilst the release of the *FATF 40 Recommendations* and similar guidance saw government interest in AML grow during the 1990s, it is the following decade that is largely responsible for defining modern day approaches to ML/TF risk management.

As reiterated throughout this thesis, the events of September 11 have had a profound effect on the way that national governments address AML/CTF, and the way in which many financial institutions are now expected to conduct their operations and manage their ML/TF risk. The 2001 terrorist attacks became the precursor for a raft of new corporate risk management obligations, and are largely responsible for the sizeable role that financial institutions are currently expected to play in protecting national and international financial systems from abuse. They heightened government awareness of terrorism financing issues, generated unprecedented concern for AML/CTF, and provided the catalyst for the enactment of legislation such as the *USA PATRIOT Act*. In many ways, the events of September 11 ushered in a new era of risk-based AML/CTF regulation.

Since 2001, a number of international bodies including the Basel Committee, FATF and Wolfsberg Group, have issued guidance with respect to the ongoing management of ML/TF risk. As increasing numbers of jurisdictions and institutions have followed the international best practice standards published by these bodies, pressure has mounted upon others to also do the same. ⁶³⁴ In turn, this has created greater demand for more streamlined approaches to ML/TF risk management, and cemented a deliberate shift away from prescriptive regulation

⁶³⁴ Chapman, A., and Guerts, J., Working in an Anti-Money Laundering Environment: The Banker's View, Presentation delivered at the Money Laundering Symposium, Reserve Bank of Australia, Sydney, 30 September 2002. Accessed at http://www.aic.gov.au/conferences/2002-ml/chapman.pdf on 24 February 2008.

towards risk-based approaches that render financial institutions accountable for identifying, assessing, mitigating and managing their ML/TF risk.

Whilst many institutions are currently assessing their ML/TF risk in terms of the 'three bases', they should not confine their perceptions of risk (or their risk evaluation and treatment activities) to such inward-looking risk assessment exercises. Whilst institutions certainly need to understand the levels of ML/TF risk represented by their products/channels, customers and different jurisdictions, there are a number of more traditional risk types that they should also consider when trying to comprehensively manage their risk exposures and design more holistic risk management controls. As detailed in Chapter 2, viewing their ML/TF risk in the context of reputational risk, financial risk and other traditional risk types should enable financial institutions to better assess the 'consequence risk' stemming from particular breaches of AML/CTF legislation. Further, it should enable them to make more informed decisions about how far they should extend their individual risk-based approaches and tighten their internal AML/CTF controls. Institutions that become preoccupied with their internal ML/TF risk may believe that taking a minimalist approach to the design of their systems and controls is satisfactory for the purposes of mitigating their risk. However, institutions that seek to broaden their understanding of ML/TF risk by framing it in terms of more traditional risk types, may determine that a minimalist approach is unsatisfactory because it will only mitigate their legal risk, and not their related reputational or financial risk.

Given that an individual's or an organisation's perception of ML/TF risk will generally depend upon where they stand in the broader regulatory system, ⁶³⁵ institutions operating under risk-based regimes should seek to clarify the way in which regulatory authorities view such risk. Where there is uncertainty around how regulatory officials define and assess ML/TF risk, institutions may end up implementing risk-based systems and controls that, whilst seemingly adequate by all internal measures, are vastly inadequate when framed in terms of the risk models and benchmarking exercises employed by the regulator. Thus, by expanding their knowledge of ML/TF risk and broadening their understanding of how

⁶³⁵ Op cit n14, 111.

regulatory authorities view such risk, institutions may better understand how to achieve AML/CTF compliance and avoid any unwanted regulatory or media scrutiny.

8.3 The diminishing risk of incurring criminal liability

Given the extent to which the regulatory terrain has changed in many jurisdictions following the events of September 11, the AML/CTF legal risk faced by financial institutions has risen considerably during the past decade. In the years immediately following the terrorist attacks, governments in the U.S., the U.K. and a host of other countries including Australia, enacted new AML/CTF legislation and demonstrated a willingness to institute criminal enforcement proceedings against those entities in breach of their requirements. The provision of AML/CTF international best practice standards, coupled with the emotion underpinning legislation such as the *USA PATRIOT Act*, ensured that many institutions faced – both theoretically and operationally – a greater degree of AML/CTF legal risk than they had prior to the 2001 terrorist attacks.

According to some AML/CTF professionals and media commentators, institutions face more AML/CTF legal risk today than ever before. There are a myriad of AML/CTF laws now in place in many jurisdictions and, as noted in **Chapter 3** of this thesis, a significant proportion of these provide harsh criminal penalties for breaches of particular AML/CTF obligations. These penalties include large fines and, in more severe cases of non-compliance, lengthy terms of imprisonment for responsible officers/employees.

Whilst there is no formally recognised hierarchy of AML/CTF offences, it is clear that breaches of certain legislative provisions generally carry heavier penalties than others. As opposed to breaches of risk-based requirements, which will typically only attract civil penalties, breaches of prescriptive requirements can often attract criminal liability. By way of example, given how pivotal transaction reporting is to the identification of predicate offences, in many AML/CTF regimes a failure to properly file Suspicious Activity Reports is seemingly more likely to be accompanied by criminal penalties. A review of recent AML/CTF enforcement proceedings in countries such as the U.S. and the U.K. highlights

how many regulatory actions hinge upon reporting failures, and how those financial institutions with inadequate reporting controls might directly assume far higher levels of AML/CTF legal risk.

Although a number of regulatory officials, AML/CTF professionals and industry participants have held that the imposition of criminal penalties (and its reputational implications) may be financially debilitating or even commercially fatal for an institution, the veracity of these claims is debatable. Whilst the past few years have seen a number of governments enact risk-based legislation and widen the risk management responsibilities placed upon financial institutions, the extent of the AML/CTF legal risk currently faced by many institutions is questionable. Providing criminal penalties for certain offences is one thing, but actually imposing these penalties upon non-compliant institutions appears to be another entirely.

Whilst the level of AML/CTF risk faced by institutions was quite pronounced in the immediate aftermath of September 11, it appears to have been scaled back somewhat in the past few years. Even in the U.S., a jurisdiction widely regarded as the international vanguard for AML/CTF regulation and enforcement, the likelihood of an institution being prosecuted today for a money laundering offence or a criminal AML/CTF compliance failure is relatively low. (Arguably, the likelihood of an institution being *convicted* of a money laundering-related offence is even lower.) Though the criminal penalties available for certain breaches of AML/CTF legislation may be significant, recent sentencing statistics suggest that criminal actions against non-compliant institutions are currently the exception rather than the rule in the U.S.

Given the many issues often associated with prosecuting corporate entities (particularly in recent years), regulatory and law enforcement authorities are deliberately shifting their activities away from the initiation of criminal proceedings. This appears to be the case even in circumstances where such proceedings have a high probability of success. In the U.S., increased reliance is being placed upon cooperative regulatory outcomes such as deferred and non-prosecution agreements. Such agreements not only enable regulatory officials to avoid the time and expense typically associated with corporate prosecutions, but also enable

them to demonstrate the presence of an active regulatory/enforcement environment by mandating that certain entities undertake sweeping institutional reforms.

Whilst the apparent lack of prosecutions is attributable to a number of factors, it has certainly been influenced by the "catastrophic collateral consequences" that may stem from launching a sweeping criminal enforcement action against a major financial institution. After prosecuting several large corporations for their misdeeds earlier this decade, U.S. regulatory authorities have become acutely aware of the consequences that a criminal action may have for an institution's reputation, financial standing, employees and creditors. After witnessing the significant systemic fallout caused by the aggressive pursuit of companies such as Arthur Andersen, regulatory officials now appear reluctant to prosecute corporate crimes and potentially hold employees, shareholders and even other institutions to ransom for the legislative failures of one institution.

Indeed, there are a number of potential complications involved with prosecuting large corporate entities and they all raise interesting questions about the relationship that may exist between an institution's size/importance, and its levels of AML/CTF legal risk. A number of AML/CTF professionals working in larger institutions may perceive that their AML/CTF legal risk is greater because their activities are subject to closer regulatory scrutiny and their compliance failures can be exploited by regulatory officials keen to demonstrate that non-compliance will not be tolerated.

However, rather than facing heightened levels of AML/CTF legal risk, larger institutions may find that their size and the scale of their operations actually shields them from a certain degree of AML/CTF legal risk. In jurisdictions such as Australia, where just four major banks dominate the financial services landscape, these larger institutions may find themselves in an unrivalled regulatory position with respect to protection from forceful criminal actions. Were AUSTRAC to prosecute any of the 'Four Pillars' of the Australian financial services sector for AML/CTF compliance failures, the consequences could be

⁶³⁶ Lichtblau, E., 'Leniency for Big Corporations in the U.S.', *International Herald Tribune* (New York), 9 April 2008 http://www.iht.com/articles/2008/04/09/business/justice.php at 16 May 2008.

devastating – not just for the relevant institution and its associated parties, but for the Australian financial system as a whole.

Complex 'collateral damage' issues aside, the financial resources and political sway maintained by some institutions may render them particularly unattractive targets for criminal enforcement actions. Depending upon the alleged contraventions committed by an institution, the risk appetite of its executives and their willingness to incur possible reputational damage during court proceedings, regulatory officials may find themselves tied up in court proceedings for many years against a large, well-resourced entity. Evidently, this is an altogether undesirable outcome for a regulatory authority that may well be under funded, under resourced, and under pressure from the public to achieve results.

Rather than criminally pursuing larger entities for their legislative breaches, regulatory officials may choose to only prosecute smaller institutions without the same levels of financial backing as their peers. Doing so may enable them to demonstrate their regulatory/enforcement powers to the public, conclude proceedings faster (and without the political wrangling potentially associated with larger entities), and send a strong message to smaller institutions that whilst they may not be subject to the intense oversight often afforded to major banks, they are not immune from regulatory action. Their relative ML/TF risk may be lower than that of other regulated entities, but it must nevertheless be addressed through appropriate risk-based systems and controls.

8.4 The increasing risk of incurring civil liability

Whilst an institution's level of AML/CTF legal risk largely hinges upon its exposure to criminal penalties and enforcement actions, it also rests upon its risk of facing civil proceedings in relation to any AML/CTF compliance failure and/or contravention of AML/CTF legislation. Whilst there has been an evident decline in the willingness of regulatory authorities to criminally prosecute breaches of AML/CTF legislation, institutions should not be lulled into believing that their resulting AML/CTF legal risk is minimal. Indeed, regulatory authorities have not altogether abandoned their pursuit of non-compliant

institutions; they have simply changed their *modus operandi* and shifted their activities towards the civil resolution of AML/CTF compliance failures.

As discussed in **Chapter 4** of this thesis, the less onerous civil standard of proof enables regulatory authorities to secure a positive result (and the imposition of appropriate penalties) far more easily than they might have been able to through the use of criminal enforcement proceedings. Criminal prosecutions attract a higher standard of proof and must be conducted within the confines of particularly strict rules of evidence. Accordingly, where the primary purpose of a particular enforcement action is simply to embarrass a noncompliant institution and cause it to rectify its internal control environment, regulatory officials can just as easily, if not more easily, achieve this outcome via civil proceedings.

An institution's exposure at civil law is not limited to its compliance or non-compliance with applicable AML/CTF legislation. It will generally also extend to the existence of third party rights and the ongoing interaction between AML/CTF legislation and other areas of the law. For instance, in addition to civil enforcement actions, an institution might also – depending upon the jurisdiction(s) within which it operates – face AML/CTF legal risk in the form of various civil claims. For instance, whilst institutions in the U.S. may face liability in the form of shareholder derivative suits, institutions operating in the U.K. may face liability in the form of constructive trust claims initiated by third parties.⁶³⁷

In certain countries, an institution may be deemed to be a constructive trustee in circumstances where it knows that customer funds in its possession are connected to a breach of trust or fiduciary duty, but it nevertheless pays them away or deals with them in a manner that is inconsistent with, or detrimental to, the interests of a beneficiary. ⁶³⁸ In recent years, the enactment of tougher AML/CTF legislation might have increased the potential

As discussed in **Chapter 4** of this thesis, constructive trust claims technically arise in equity and not under the umbrella of civil law. However, for ease of reference, these types of actions are addressed at the same time as a range of civil proceedings and enforcement actions.

Financial Services Commission Mauritius, Code on the Prevention of Money Laundering and Terrorist Financing (Intended for Management Companies) (2003) 25 http://72.14.253.104/search?q=cache:cQ-YAl2-

dooJ:www.gov.mu/portal/sites/ncb/fsc/download/amlcftmc.pdf+U.S.+constructive+trust+money+laundering &hl=en&ct=clnk&cd=24&gl=au> at 26 August 2007.

exposure of institutions under constructive trust principles. By outlining precise compliance obligations, certain AML/CTF laws may have given courts a solid, objective standard upon which to judge the honesty and reasonableness of an institution's actions. To illustrate, if an institution blindly accepted and paid away the proceeds of a fraud without conducting adequate KYC procedures and/or otherwise monitoring their customers' transactional behaviour, a U.K. court might find that – in addition to contravening its explicit legislative requirements – the institution did not act as an honest and reasonable banker might have been expected to in the same circumstances.

It should be noted that an institution's AML/CTF legal risk and potential liability under constructive trust principles is likely to be higher where there is some uncertainty or tension between its contractual obligations to customers, and its statutory requirements to report suspicious activities and not 'tip off' a customer about whom a SAR has been filed. As evidenced by recent case law in the U.K., institutions may find themselves in a precarious legal position where there is a lack of clarity around the interplay between their contractual and legislative obligations, and their potential liability as a constructive trustee.

Any uncertainty around their legal obligations and, more specifically, which obligations should take precedence over others, may lead some institutions to compromise (or entirely forego) compliance with their civil law obligations in order to avoid liability for breaches of their criminal law obligations (or vice versa). As demonstrated by the string of authorities discussed in **Chapter 4**, in certain circumstances an institution's compliance with one set of legal requirements (for instance, its statutory reporting and 'tipping off' requirements), may heighten its AML/CTF legal risk with respect to others (for instance, its contractual requirements and its obligations to third parties under constructive trust principles).

Although many institutions are likely to focus their AML/CTF compliance efforts upon the avoidance of criminal liability, it is clear that they should not ignore their potential liability at civil law. Institutions that deliberately disregard their exposure at civil law may, depending on the jurisdiction(s) within which they operate, unnecessarily increase their

AML/CTF legal risk and their exposure to civil 'breach of contract' claims and equitable constructive trust claims. Further, and perhaps more importantly, they may heighten their vulnerability to lengthy and intrusive regulatory reviews/audits that are not only resource-intensive, but also potentially damaging to their reputation.

8.5 AML/CTF legal risk and enforcement

Whilst an institution's AML/CTF legal risk is largely determined by the criminal and civil penalties available under AML/CTF legislation, it also hinges upon the enforcement environment(s) within which they operate. In the absence of a strong regulatory and enforcement environment, national AML/CTF laws are – regardless of how tightly they are drafted – unlikely to have a material effect on the way institutions conduct their activities and manage their ML/TF risk. Whilst the benefits of AML/CTF controls have frequently been noted (for instance, KYC procedures have often been held to help entities identify other financial crimes such as fraud), many institutions may believe that the costs associated with implementing these controls can be justified without any apparent ramifications for non-compliance.

Unless there is an appreciable level of AML/CTF legal risk, some institutions might deliberately take a minimalistic approach with respect to the fulfilment of their risk-based requirements. This is because in some cases it is likely to be AML/CTF legal risk – and not risk-based approaches – that are driving institutional attitudes towards AML/CTF compliance. As opposed to prioritising their compliance activities based upon their relative ML/TF risk, a number of institutions may determine their compliance objectives solely on the basis of recent enforcement actions and their accompanying legal risk (i.e. those AML/CTF compliance failures and enforcement proceedings that have recently been pursued by regulatory authorities). 639

Oavis, E., 'What's Wrong With a Risk-Based Approach?' (2007) 8(11) OpRisk & Compliance http://www.opriskandcompliance.com/public/showPage.html?page=479962 at 20 January 2009.

In jurisdictions where efforts to curb organised crime are disorganised or disjointed, institutions are likely to face much lower levels of domestic AML/CTF legal risk. By comparison, in jurisdictions such as the U.S., where regulatory and enforcement efforts have become increasingly coordinated in recent years, institutions are likely to face far higher levels of risk. Although several money laundering scandals (including the Riggs Bank affair) have exposed weaknesses and vulnerabilities in the U.S. enforcement environment, institutions operating there at still at risk of being penalised for non-compliance with domestic AML/CTF laws. Many banking regulators are currently involved in the enforcement of U.S. AML/CTF legislation, and whilst the resulting mosaic of regulatory powers has at times led to duplications of process on the one hand, and buck-passing and blame shifting on the other, it has generally created a more aggressive enforcement environment since the enactment of the *USA PATRIOT Act*. 640

That said, the AML/CTF legal risk faced by many institutions does not appear to be as high as many regulatory officials, AML/CTF practitioners, consultants and institutions seem to believe. Whilst it may be technically true that an institution's non-compliance with AML/CTF legislation might attract an array of criminal and civil penalties, the frequency with which such penalties are imposed in practice, remains contentious and raises questions about the real levels of risk faced by entities. Although the last few years have seen a number of institutions reprimanded for their AML/CTF compliance failures, these institutions have typically incurred civil monetary penalties for breaches of their prescriptive, as opposed to their risk-based, legislative requirements. Contrary to the claims of commentators, none of these penalties have been institutionally fatal.

The lack of harsh criminal penalties and AML/CTF enforcement actions taken in recent years is perhaps reflective of a regulatory environment that is now less geared towards strict command and control, and more geared towards a strong regulatory dialogue in which institutions are encouraged (if not expected) to participate. If AML/CTF regulation and enforcement was viewed in terms of a continuum that stretches from exacting and strong rule

⁶⁴⁰ Op cit n190, 56.

at one end, through to maintenance of the status quo at the other,⁶⁴¹ the current regulatory environment would seemingly fall between the middle and latter end of that spectrum. As opposed to launching formal enforcement proceedings against non-compliant institutions, a number of regulatory authorities appear to have developed – or are in the process of developing – a management regulatory approach that emphasises education and cooperation.

Considering the uncertainty that may accompany risk-based legislative requirements, the regulatory preference for education and reform – as opposed to prosecution and penalties – is understandable. Just as some institutions may find it difficult to accurately assess and address their ML/TF risk, regulatory authorities might find it equally challenging to identify and substantiate any perceived shortcomings in an institution's risk-based AML/CTF program. This is perhaps demonstrated by the minimal number of civil lawsuits concerning institutional contraventions of risk-based legislative requirements.

Nevertheless, whilst the AML/CTF legal risk faced by institutions in the U.S. and the U.K. appears to have diminished in the past few years, the risk faced by foreign institutions may have risen during the same period. Since the events of September 11, the U.S. government has continually demonstrated a willingness to invoke special measures in relation to foreign entities deemed to represent an unacceptable risk to the U.S. financial system. Under *Section 311* of the *USA PATRIOT Act*, the U.S. Treasury Department can take – and has taken – such action against foreign entities without needing to concern itself with due process, legal proceedings, or collateral damage.

In addition to their exposure under extraterritorial legislation, the AML/CTF legal risk faced by many institutions has risen in recent years as a number of jurisdictions have sought to implement and strengthen their AML/CTF regimes. This is particularly evident with respect to institutions operating in the Asia-Pacific region, where several countries have tried to secure membership of the FATF (or similar, regional-style bodies) by improving the drafting, design and enforcement of their local AML/CTF laws. In recent years, new

⁶⁴¹ Serrano, M., and Kenny, P., 'The International Regulation of Money Laundering' (2003) 9(4) Global Governance 433.

AML/CTF laws have been enacted in India, Indonesia, the Philippines and Vietnam, and additional AML/CTF regulations have been implemented in Thailand, Taiwan and Korea. If this trend in AML/CTF law reform continues, the enforcement of AML/CTF legislation may become more stringent and the AML/CTF legal risk faced by many institutions is likely to be heightened.

According to some banking professionals, regulators in the U.S. and many other jurisdictions are expected to monitor and enforce AML/CTF compliance more tightly in the coming years. It is anticipated that they will draft regulations more stringently, supervise institutional AML/CTF efforts more intensely, conduct investigations more regularly, and address compliance lapses more fiercely.⁶⁴² It should be noted however that this may take several years to occur in countries such as Australia, where AML/CTF laws are still being implemented and regulatory officials are likely to – at least for the next two or three years – address any legislative breaches through the use of negotiated outcomes (i.e. rather than formal enforcement proceedings).

In some respects though, it is perhaps undesirable that the international enforcement environment moves too quickly – or too far – towards exacting and strong rule. Whilst such an environment may cause institutions to spend more time designing, implementing and maintaining their risk-based AML/CTF controls, it might also give rise to over-compliance and encourage institutions to file a barrage of SARs⁶⁴³ that ultimately detract from real instances of money laundering. Although strong and persistent enforcement efforts may reinforce the importance of AML/CTF compliance, they are only likely to heighten institutions' AML/CTF legal risk up to a certain point, beyond which they might actually decrease such risk by impeding regulatory authorities from properly monitoring AML/CTF compliance and executing their functions.

Byrne, J., 'How AML/CTF is Being Managed in the United States: The Impact of the Global Market
 Crisis on AML/CTF Including Information Sharing Between Jurisdictions and Institutions' (Paper presented at the Anti-Money Laundering and Counter-Terrorism Financing Conference 2009, Sydney, 2 April 2009).
 Clearly, if institutions respond to zealous enforcement efforts by defensively filing Suspicious Activity
 Reports, this may be just as problematic as institutions filing too few reports. See Krebsbach, K., 'Policing
 Global Pirates on the River of Money' (2004) 17(4) Bank Technology News 20.

8.6 Risk-based regimes in theory and practice

A risk-based approach should mean just that. From a regulatory perspective, it should enable authorities to gear their resources towards those institutions, industries and business activities deemed to represent the greatest ML/TF risk. From an institutional perspective, it should theoretically provide flexibility, deliver cost-savings, and encourage thoughtful engagement with the concepts of AML and CTF. As opposed to rigid, checklist-driven compliance exercises, a risk-based approach should require institutions to have a greater awareness and understanding of the ML/TF risk attached to their provision of financial services.

Interestingly however, the alleged benefits of risk-based approaches may not always be evident when such approaches are viewed in practice. Firstly, whilst risk-based approaches inherently provide institutions with flexibility regarding the design and implementation of their AML/CTF programs, the degree of flexibility that they allow for is questionable. Whilst the FATF has held that such approaches "mean that no two financial institutions are likely to adopt the exact same detailed practices", 644 it appears that the flexibility afforded to institutions under risk-based regimes may have been eroded in recent years by institutional and regulatory attempts to benchmark AML/CTF compliance.

Benchmarking by regulatory authorities and institutions

Whilst a basic premise of risk-based approaches is that institutions' AML/CTF systems and controls should be individually stylised to – and judged in light of – their own ML/TF risk profiles, a number of regulatory authorities have been particularly transparent regarding their use of benchmarking exercises. For instance, the U.K. FSA has explicitly acknowledged its use of benchmarking to "enable supervisors to compare a firm's antimoney laundering arrangements with those of its peers, with a view to informing [their] judgement of the quality of the firm's controls". 645 Such an approach to AML/CTF regulation appears to be sanctioned by international bodies such as the FATF, which has

⁶⁴⁴ Op cit n16, 4. ⁶⁴⁵ Op cit n19, 5.

previously conceded that risk-based approaches to supervision should "permit relevant comparisons between financial institutions". 646

The adoption of vastly different AML/CTF programs amongst institutions may clearly pose a significant challenge for regulatory officials. In effect, it may require them to identify and understand the individual ML/TF risk profile of each institution subject to their review/oversight. Given that this is not operationally feasible, it is understandable that many regulatory authorities do – if not consciously then at least inadvertently – compare and contrast the AML/CTF programs implemented by different institutions. This may be problematic however, where it enables regulatory comparisons between institutions that are alike in terms of their size, operations and product offerings, but considerably different in terms of their customer bases, risk appetites and jurisdictional reach.

That said, it should be noted that in risk-based AML/CTF regimes, regulatory authorities are not necessarily alone in their use of benchmarking exercises. In Australia for instance, many institutions are currently undertaking their own benchmarking activities as a way of ensuring that their AML/CTF controls and risk appetites do not deviate greatly from those of their competitors. Evidently, the aim of such exercises is to ensure that they are not exposed to a greater degree of legal and reputational risk by having dissimilar AML/CTF programs. Importantly though, whilst benchmarking may go some way towards protecting institutions against undue and unwanted regulatory attention, it will likely undermine their ability to fully capitalise on the potential flexibility and cost benefits provided by risk-based approaches.

Given the advent of benchmarking as a common compliance exercise amongst many regulatory authorities and institutions, it may be that risk-based approaches are actually setting the bar for compliance far higher than it would otherwise have been under prescriptive approaches to AML/CTF. In some jurisdictions, it appears that 'best practice' AML/CTF standards are now becoming the 'norm' amongst certain types of financial institutions. In the U.S., a number of U.S. banking executives have already expressed

⁶⁴⁶ Op cit n16, 10.

concern that the 'best practice' sections of regulatory guides and examination manuals are being construed as the standard benchmark for institutions' AML/CTF compliance. As opposed to specifically tailoring their AML/CTF programs to their own business activities, some institutions are holding themselves to (and/or finding themselves held to) more arduous standards than their ML/TF risk profiles may require. This is perhaps the case in the U.K., where a 2006/2007 PricewaterhouseCoopers survey revealed that 82 per cent of financial institutions believed that they had not experienced any cost benefits since the implementation of their country's risk-based regime. As

8.6.2 Uncertainty around the nature and scope of risk-based requirements

In addition to the use of benchmarking and comparative compliance exercises, the cost savings allegedly provided by risk-based approaches may be undermined by a lack of clarity around what some regulatory authorities will deem to be appropriate risk-based controls. In jurisdictions where there are potential inconsistencies between the expectations and understandings of regulators and the regulated,⁶⁴⁹ institutions may try to demonstrate the seriousness with which they regard AML/CTF compliance by implementing systems and controls that are far more elaborate than those required by their ML/TF risk profile.

Even in countries where the financial services sector has lobbied for a risk-based AML/CTF regime, the lack of clarity and precision around some risk-based obligations has at times led institutions to call for additional regulatory guidance. This currently appears to be the case in Australia, where many financial institutions and industry bodies continue to approach AUSTRAC for more detailed explanations around the nature and scope of their obligations. Previously, it has also been the case in the U.K., where the U.K. FSA has inevitably had to provide institutions with more detailed guidance regarding how to achieve compliance with risk-based legislative requirements. ⁶⁵⁰ On 15 December 2007, new AML

⁶⁴⁷ Op cit n639.

Fagg, S., Risk-based Laundering Approach Yields Little Fruit (2007) Lawyers Weekly http://www.lawyersweekly.com.au/articles/Risk-based-laundering-approach-yields-little-fruit_z70171.htm

Chalmers, R., Risk-based Approach to AML/CTF, United Kingdom Financial Services Authority http://www.fscey.gov.tw/public/Attachment/7103115302771.pdf> at 30 September 2008.

Op cit n283, 8.

Regulations were brought into effect in the U.K. to clarify a number of legislative customer due diligence obligations. Though these Regulations are still hinged upon risk-based decision-making and controls, their level of detail suggests that U.K. institutions have required further guidance in respect of how to meet – operationally if not strictly legally – their AML requirements.

That said, especially in newer or developing AML/CTF regimes such as Australia, institutions should always strategically consider whether they approach regulatory authorities for additional guidance on particular legislative requirements. Whilst some organisations may perceive that the provision of more detailed guidance will lower their individual AML/CTF legal risk, such guidance may in fact heighten the level of risk for all institutions. Though a clearer regulatory direction may assist entities to design their risk-based systems and controls, it might also give regulatory authorities clear and unequivocal benchmarks against which they can assess institutions' compliance with AML/CTF legislation. Detailed guidance can remove some of the discretion otherwise given to institutions, and see them held to a far higher standard of compliance than they would have applied to themselves under their individual risk-based approaches.

Even where institutions have designed and implemented risk-based AML/CTF controls, they will not necessarily be immune from formal enforcement proceedings. Just as some AML/CTF regulatory authorities have held that their own action (or, at times, their inaction) in relation to certain banking failures has been judged retrospectively, 652 it appears that so too has the risk-based decision-making of many financial institutions. Following the commission of a money laundering/terrorism financing offence and/or an AML/CTF compliance failure, an institution's *past* risk-based decisions may be judged in light of *current* understandings of ML/TF risk and risk exposures.

If an institution's risk assessment methodology previously determined that a certain part of its business represented a lower ML/TF risk, regulatory authorities may question the

652 See McCarthy, C., Op cit n20.

⁶⁵¹ HM Treasury, Money Laundering Regulations 2007: An Information Sheet for Firms (2007) http://www.hm-treasury.gov.uk/media/2/6/moneylaundering_guide150807.pdf at 26 July 2008.

soundness of that methodology if the relevant business area is later found to have facilitated money laundering or terrorism financing activities. Even in circumstances where regulatory officials decide that the institution's risk methodology is defensible, they might nevertheless question the appropriateness of the institution's systems and controls commensurate to its risk model. Despite regulatory recognition of the fact that institutions may be unable to prevent all instances of money laundering/terrorism financing, where such crimes have occurred it may be difficult (reputationally, if not legally) for an institution to sufficiently justify why they had previously deemed their internal, risk-based controls to be sufficient for the purposes of mitigating their ML/TF risk.

8.6.3 The retrospective application of rules-based models

Evidently, the risk-based approaches enshrined in legislation are not always reflected in accompanying regulatory efforts. Rather than applying risk-based models and decision-making to regulation, some authorities might occasionally seek to assess an institution's compliance by applying a rules-based approach retrospectively. As discussed in **Chapters** 6 and 7 of this thesis, this was seemingly the case with Riggs Bank and Banco Delta Asia, which both had the desirability of their customers judged in hindsight by U.S. government and regulatory officials.

Whilst Banco Delta Asia's relationship with certain North Korean entities ultimately led to its expulsion from the U.S. financial system, the legitimacy of the bank's customer relationships was seemingly judged in retrospect. If officials from Banco Delta Asia are correct and U.S. authorities did in fact know about the institution's ties to North Korean companies for approximately two decades, then FinCEN clearly had a significant amount of time to communicate and address any concerns about those companies. However, rather than proactively raising any issues with Banco Delta Asia and enabling the bank to take corrective action and/or otherwise employ an appropriate risk management strategy, the U.S. government publicly denounced the bank without warning. Perhaps driven by their desire to force the closure of North Korea's nuclear program, U.S. authorities issued a proposed rule

under Section 311 of the USA PATRIOT Act designed to cause maximum prejudice to Banco Delta Asia and Macau.

However, the subsequent application of rules-based models has not been strictly reserved for foreign entities. In the aftermath of September 11, U.S. regulatory authorities have also retrospectively judged the desirability of certain customer relationships entered into by local institutions. This was seemingly the case in relation to Riggs Bank's relationship with General Pinochet. Whilst the institution's relationship with the Chilean military official attracted unflattering publicity and unwanted regulatory attention, General Pinochet was actually a highly desirable customer when the bank coveted his business. At that time, he was a wealthy public figure and a vocal supporter of the U.S., and the laws in relation to PEPs had not yet been enacted. Even if they had, General Pinochet's status as a foreign, senior military official might not have caused any great concern for Riggs Bank. After all, the institution had long built its business – and its reputation – around providing banking services to prominent public figures.

Despite his initial desirability, when the U.S. government subsequently decided that General Pinochet was not a particularly esteemed customer, Riggs Bank became the subject of intense regulatory scrutiny. By that time, risk-based approaches had started to gain momentum, as had regulatory expectations that institutions would undertake additional due diligence and take extra steps to identify and monitor the activities of PEPs. Thus, whilst the bank contravened U.S. AML/CTF legislation by failing to carry out adequate ongoing customer due diligence with respect to General Pinochet's transactions, its decision to pursue him as a customer appears to have been criticised unfairly. At the time his business was sought in the 1980s, the institution was not likely to believe that it was assuming an unacceptably high ML/TF risk. Indeed, the concept of ML/TF risk management had not yet emerged. It is only when the decision to provide banking services to General Pinochet was judged in hindsight using rules-based models that it appeared questionable to regulatory authorities.

8.6.4 Risk-based approaches and terrorism financing

In addition to highlighting the way in which regulatory actions may not always reflect the risk-based approaches enshrined in AML/CTF legislation, the Riggs Bank scandal also demonstrates the limitations of applying risk-based approaches to the issue of terrorism financing. Although the bank was scrutinised by regulatory authorities and media commentators for failing to identify transactions potentially related to the terrorist acts carried out on September 11, the institution's ability to properly screen and identify such transactions is questionable. Indeed, whilst risk-based approaches are generally held to apply to both AML and CTF, terrorism financing is notoriously more difficult to identify than money laundering. As it can often involve small amounts of money derived from entirely legitimate sources, ML/TF risk assessments and risk-based controls may be of little assistance in isolating those transactions and customers related to terrorism financing.

Risk-based approaches to CTF may be considered to place unrealistic expectations upon institutions; requiring them to identify activities and transactions that are unlikely to exhibit the hallmarks of conventional money laundering. Whilst many financial institutions are equipped to screen the names of their customers against terrorism-related sanctions lists, any obligation to conduct such screening is typically mechanical and not a function of ML/TF risk. In practice, risk-based approaches to AML/CTF will generally only assist an institution to identify and report terrorism financing activities insofar as they involve illegally derived monies and exhibit the use of traditional money laundering methods. 653

In the case of Riggs Bank, screening the names of Khalid Almidhar and Nawaf Alhazmi; the beneficiaries of Princess Al-Faisal's transactions and two of the September 11 hijackers, would not have resulted in a positive match. It is only after the terrorist attacks took place that these individuals were positively identified as terrorists and, retrospectively, Princess Al-Faisal's transactions could be connected with possible terrorism financing activities. Even with a sophisticated transaction monitoring system in place, the relatively anonymous beneficiaries and the small amounts of money being sent to them each month, would have

The Wolfsberg Group, Wolfsberg Statement on the Suppression of the Financing of Terrorism, January 2002. Accessed at http://www.wolfsberg-principles.com/financing-terrorism.html on 15 May 2006.

been unlikely to trigger any alerts or arouse the suspicions of Riggs Bank staff prior to September 11.

8.6.5 Self-regulation

Clearly, the enforcement of risk-based AML/CTF requirements may be problematic for both institutions and regulatory authorities alike. Whilst risk-based regimes require institutions to assess their levels of ML/TF risk, they also require regulatory officials to understand the ML/TF profiles of regulated entities. This may prove to be exceedingly difficult for regulatory authorities and might explain why a number of risk-based regimes are continuing to move further towards meta monitoring and models of institutional self-regulation. By relying on institutions to manage and monitor their compliance with AML/CTF legislation, it is not always necessary for regulatory officials to become involved in the granular assessment of an institution's ML/TF risk profile.

As opposed to actively understanding and identifying each regulated entity's ML/TF risk profile, some regulatory authorities may prefer to monitor the success (or otherwise) of an institution's internal monitoring activities. However, whilst this might reaffirm the notion that risk-based approaches should be flexible and hinged upon institutions' individual levels of ML/TF risk, it may have a number of unintended regulatory consequences that actually undermine other fundamental premises of risk-based regimes. As previously discussed, meta monitoring may in fact encourage the use of benchmarking exercises amongst both institutions and regulatory officials (thereby undermining the potential cost benefits associated with risk-based approaches), and enable regulators to measure institutions' AML/CTF compliance by applying rules-based models in hindsight.

8.7 AML/CTF and the phenomena of risk

Despite some of their challenges and potential shortcomings, it is clear that risk-based approaches – as well as the concepts of AML and CTF – can enhance institutional understandings of the phenomena of risk. At the most basic level, risk-based approaches

require institutions to consciously consider the issue of risk. They require them to acknowledge the existence of ML/TF risk, and assess and mitigate the ML/TF risk that they might reasonably face through their provision of financial products/services. Whilst some regulatory authorities have a broad range of supervisory and enforcement powers, risk-based AML/CTF regimes squarely place responsibility for the ongoing management of ML/TF risk, with regulated entities.

Given their emphasis on risk management and self regulation, risk-based approaches to AML/CTF encourage institutions to more thoughtfully engage with the concept of risk. Unlike prescriptive legislative obligations, risk-based requirements cannot simply be regarded as mechanical compliance exercises. The scope of such requirements necessarily rests upon an institution's ML/TF risk profile and as such, they require regulated entities to periodically assess the risk represented by different areas of their business. Under risk-based regimes, it is not sufficient for institutions to simply assess their risk at the time of designing their original systems and controls. Due to the fact that institutions' risk profiles (and thus, the quality of their AML/CTF compliance) will vary from time to time, risk-based regimes require them to continuously manage their risk.

Whilst the 'three bases' of risk will assist institutions to identify their areas of greatest ML/TF exposure, gaining greater knowledge about the types and levels of risk apparent in different risk-based regimes, will better enable them to assess and address their individual risk exposures. Further, it will assist them to more accurately determine the potential consequence risk represented by their non-compliance with risk-based legislation.

Institutions that fail to undertake their own assessment of the potential reputational, financial and legal risk accompanying their activities under a risk-based regime, may simply accept the claims of many industry professionals and media commentators that non-compliance with AML/CTF legislation is likely to attract unwanted regulatory attraction, aggressive enforcement action and, in certain cases, closure. However, by actually undertaking an analysis of the levels of risk apparent in several risk-based AML/CTF regimes, they may recognise that the past few years have seen a deliberate shift away from such severe

enforcement actions. Rather than penalising employees, shareholders and other institutions for the misdeeds of a non-compliant entity, some regulatory authorities are now pursuing more collaborative and less commercially disruptive enforcement options.

This evident regulatory trend away from aggressive AML/CTF regulation appears to undermine many of the alleged consequences of non-compliance with AML/CTF legislation. It is certainly not doubted that AML/CTF compliance failures can result in large-scale regulatory actions and the imposition of severe criminal and civil penalties. However, it appears that institutions and media commentators have a tendency to overstate their risk exposures under risk-based AML/CTF regimes. Seemingly, they have become "acutely sensitive to the business risks attached to illicit financial activity". 654 Whether this is due to a number of well-publicised enforcement actions and/or the increased political attention paid to AML/CTF issues in the wake of September 11, it is clear that the perceived vulnerability of institutions to regulatory actions and legal penalties has been inflated.

Nevertheless, it is clear that financial institutions should not ignore their various risks under risk-based regimes. To ensure their continued operation in some of the world's largest and most important financial centres, many institutions will need to identify their levels of risk under both domestic and extraterritorial AML/CTF laws, and local and foreign enforcement environments. Further, they will need to employ a risk management strategy (or a selection of risk management strategies) that mitigates their levels of risk without compromising their ability to continue operating and providing financial services to customers.

Whilst an avoidance strategy will undoubtedly provide institutions with the greatest level of protection under AML/CTF legislation, the adoption of such a risk management strategy will not be desirable or financially viable for all institutions, especially those based in smaller jurisdictions with less stringent AML/CTF regimes. Compliance with the AML/CTF obligations enshrined in legislation such as the *USA PATRIOT Act* is likely to prove both burdensome and expensive for a number of institutions in less wealthy nations. This is especially so in circumstances where the costs required to comply with extraterritorial

⁶⁵⁴ Op cit 254, 17.

AML/CTF laws will leave them operating at a competitive disadvantage in their own jurisdiction.

Even in cases where avoidance is an appropriate risk management strategy for an institution, the successful execution of such a strategy may be unclear with respect to risk-based legislative requirements. As previously noted, risk-based obligations do not necessarily give rise to a 'dichotomy of compliance' in the same way that prescriptive requirements generally do. Rather, their innate breadth and their dependency upon institutions' ML/TF risk profiles, tends to give rise to a spectrum of potential compliance options.

Thus, institutions without an acute understanding of their ML/TF risk and/or the operation of risk-based approaches may inevitably adopt a flawed risk management strategy and implement poorly designed AML/CTF programs. If they underestimate their risk, they are likely to implement lax controls that actually heighten their AML/CTF legal risk and regulatory exposure. By comparison, if they overestimate their risk by accepting the popular (but relatively untested) rhetoric about the consequence risk associated with legislative non-compliance, they are likely to spend copious amounts of time and money implementing controls that are not commensurate to their ML/TF risk profile. Evidently, both these compliance options tend to undermine the alleged benefits of risk-based regimes – flexibility, cost-effectiveness, and enhanced engagement with the concepts of AML and CTF.

References

9.1 Legislation

- Annunzio-Wylie Anti-Money Laundering Act of 1992 (12 U.S.C. §§ 1786, 1821)
- Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)
- Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) (Cth)
- Anti-Terrorism, Crime and Security Act 2001 (U.K.)
- Anti-Terrorism, Crime, and Security Amendments to the Terrorism Act 2000 (U.K.)
- Bank Holding Company Act of 1956 (P.L. 84-511, 70 Stat. 133)
- Banking Act of 1933 (P.L. 73-66, 48 Stat. 162)
- Criminal Code Act 1995 (Cth)
- Criminal Justice Act 1988 (U.K.)
- Decree 74/2005/ND-CP on the Prevention and Combating of Money Laundering (Vietnam)
- Depository Institutions Act of 1982 (P.L. 97-320, 96 Stat. 1469)
- Depository Institutions Deregulation and Monetary Control Act of 1980 (P.L. 96-221, 94 Stat. 132)
- Executive Order 13224 Blocking Property and Prohibiting Transactions with Persons who Commit, or Threaten to Commit, or Support Terrorism
- Federal Deposit Insurance Act of 1950 (P.L. 81-797, 64 Stat. 873)
- Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970 (31 U.S.C. § 1051, et seq.)
- Foreign Corrupt Practices Act of 1977 (15 U.S.C. §§ 78dd-1, et seq.)
- International Emergency Economic Powers Act (P.L. 95-223, 91 Stat. 1626)
- International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001 (P.L. 107-56, 115 Stat. 272)
- Money Laundering Control Act of 1986 (P.L. 99-570, 100 Stat. 3207-18)
- Proceeds of Crime Act 2002 (U.K.)

- Racketeer Influenced and Corrupt Organizations Act of 1970 (18 U.S.C. § 1961, et seq.)
- Terrorism Act 2000 (U.K.)
- Trading with the Enemy Act of 1917 (P.L. 65-91, 40 Stat. 411).

9.2 Case Law

- Amalgamated Metal Trading Limited v. City of London Police Financial Investigation Unit & Others [2003] 1 WLR 2711
- Baden v. Societe Generale [1993] 1 WLR 509
- Bank of Scotland v. A Ltd & Ors [2001] 3 All ER 58
- Barlow Clowes v. Eurotrust International Ltd [2006] 1 All ER 333
- Barnes v. Addy (1874) L R 9 Ch App 244
- Belmont Finance Corporation Ltd v. Williams Furniture Ltd [1979] Ch 250
- Cantor Fitzgerald & Co., et al. v. American Airlines, et al., 04 Civ. 7318
- Carl Zeiss Stiftung v. Herbert Smith & Co [1969] 2 Ch 276
- Dickler v. Allbritton, et al., Civil Action No. 04-0002978
- El Ajou v. Dollar Land Holdings plc [1994] 2 All ER 685
- Farah Constructions v. Say-Dee Pty Ltd [2007] 230 CLR 89
- Freeport Partners, L.L.C. v. Allbritton, No. 04-CV-02030 (D.D.C. filed Nov. 18, 2004)
- Horgan v. Allbritton, No CA 370-N (Del. Ch. filed Apr. 7, 2004)
- Hosni Tayeb v. HSBC Bank plc [2004] 4 All ER 1024
- Houghton v. Fayers [2000] 1 BCLC 511
- Humberto Fidel Regalado Cuellar v. United States, 553 U.S. (2008)
- Jose Daniel Ruiz Coronado v. Bank Atlantic Bancorp Inc., 222 F.3d 1315 (11th Cir. 2000)
- N.Y. Central and Hudson River R.R. Co. v. United States, 212 U.S. 509 (1909)
- Labaton v. Allbritton, et al., Civil Action No. 404-N
- Lipkin Gorman v. Karpnale [1992] 4 All ER 409

- Pennsylvania Dept. of Corrections v. Yeskey, 524 U. S. 206, 212 (1998)
- Polly Peck International v. Nadir [1992] 4 All ER 769
- Rv. Dougan (unreported, 2006)
- R v. Duff [2002] EWCA Crim 2117
- Rv. Griffiths and Pattison [2006] EWCA Crim 2155
- Rv. McCartan [2004] NICA 43
- Re Montagu's Settlement Trusts [1987] Ch 264
- Royal Brunei Airlines v. Tan [1995] 3 All ER 97
- Stone v. Ritter, 911 A.2d 362 (Del. 2006)
- Tesco Supermarkets v. Nattrass [1972] AC 153
- The Bank v. A Ltd [2000] All ER (D) 864
- The Governor and Company of the Bank of Scotland v. A Limited [2000] All ER (D) 864
- United States v. \$557,933.89, More or Less, in United States Funds, 287 F.3D 66 (2d Cir. 2002)
- United States v. All Monies (\$477,048.62) In Account No. 90-3617-3, 754 F. Supp. 1467, 1473 (D Haw. 1991)
- United States v. Baker, 227 F.3d 955, 970 n. 4 (7th Cir. 2000)
- United States v. Booker 543 U.S. 220 (2005)
- United States v. Edgmon 952 F.2d 1206 (10th Gr. 1991)
- United States v. Epstein, 426 F.3d 431, 440 (1st Cir. 2005)
- United States v. Flores, 454 F.3d 149, 155-156 (3d Cir. 2006)
- United States v. Funds on Deposit in Account No. 890-0057173 maintained at the Bank of New York by the Union Bank for Savings and Investments Jordan, No. 02-472-B, (D.N.H. Jan. 6, 2005)
- United States v. Jackson, 983 F.2d 757, 764-65 (7th Cir. 1993)
- United States v. McBride 434 F.3d 470,474 (6th Cir. 2006)
- United States v. McGauley, 279 F.3d 62, 76 n. 14 (1st Cir. 2002)
- United States v. Owens 159 F.3d 221 (6th Cir. 1998)

- United States v. Union Bank for Savings and Investment (Jordan), 487 F.3d 8 (1st Cir. 2007)
- Vadhan, et al. v. Riggs National Corp., et al., 04 Civ. 7281 (RCC).

9.3 International Instruments and Guidance

Basel Committee

- Statement of Principles (1988)
- Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering (1988).

Financial Action Task Force

- Forty Recommendations (FATF 40 Recommendations)
- Nine Special Recommendations (FATF 9 Special Recommendations).

Wolfsberg Group

- Anti-Money Laundering Principles for Private Banking (2000)
- Anti-Money Laundering Principles for Correspondent Banking (2002)
- Guidance on a Risk Based Approach for Managing Money Laundering Risks (2006).

United Nations

- United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988)
- United Nations Convention on Terrorist Financing (1999).

9.4 Books, articles and theses

Alexander, K., 'Extraterritorial US Banking Regulation and International Terrorism: The Patriot Act and the International Response' (2002) 3(4) *Journal of International Banking Regulation* 307.

- Alexander, K., 'UK Corporate Governance and Banking Regulation: The Regulator's Role as Stakeholder' (2004) 33 Stetson Law Review 991.
- Alexander, R., and Allen, C., 'Big Price for Lax Anti-Laundering' (2004) 169(204)

 American Banker 11.
- Alexander, R.C., Arlen, J., and Cohen, M.A., 'Regulating Corporate Criminal Sanctions: Federal Guidelines and the Sentencing of Public Firms' (1999) 42(1) *Journal of Law & Economics* 393.
- Altenbaumer-Price, K., Pros and Cons of Deferred Prosecution Agreements [2006] *Executive Legal Adviser* 1.
- Acharya, V.V., Essays in Regulation of Banks and Financial Institutions (Ph.D., New York University, 2001).
- Baldwin, F.N., 'Exposure of Financial Institutions to Criminal Liability' (2006) 13(4) Journal of Financial Crime 387.
- Barlow, D., 'The Evolution of Risk Management' (1993) 40(4) Risk Management 38.
- Beck, U., Risk Society: Towards a New Modernity (1992).
- Bowden, A.R., Lane, M.R., and Martin, J.H., Triple Bottom Line Risk Management:

 Enhancing Profit, Environmental Performance and Community Benefit (2001).
- Braithwaite, J., Markets in Vice, Markets in Virtue (2005).
- Brindle, M., 'The Liabilities of Financial Intermediaries and their Advisers for Handling the Proceeds of Crime' (2002) 9(3) *Journal of Financial Crime* 227.
- Byrne, J.J., and Kelsey, M.D., 'AML Enforcement Actions: What Can We Learn?' (2006) 27(3) ABA Bank Compliance 11.
- Carrol, D., 'Ambiguity in Contemporary Money Laundering Statutes' (2008) *Illinois***Business Law Journal*

 **http://iblsjournal.typepad.com/illinois_business_law_soc/2008/04/i-introductio-2.html>* at 27 July 2008.
- Chaikin, D., 'Investigating Criminal and Corporate Money Trails' in Fisse, B., Fraser, D., and Coss, G. (eds), *The Money Trail: Confiscation of the Proceeds of Crime, Money Laundering and Cash Transaction Reporting* (1992) 257.

- Clough, J., and Mulhern, C., The Prosecution of Corporations (2002).
- Cocheo, S., 'Dear Director: Watch Out For Tougher Moves When Examiners Review Anti-Money-Laundering Effort' (2004) 24(4-8) ABA Bank Directors Briefing 1.
- Courtenay, A., 'HSBC Screened N Korean Assets for Macau Bank' (2007) 14 Money Laundering Intelligence 4.
- Colangelo, A.J., 'Constitutional Limits on Extraterritorial Jurisdiction: Terrorism and the Intersection of National and International Law' (2007) 48(1) *Harvard International Law Journal* 121.
- Cowan, A., 'Scarlet Letters for Corporations? Punishment by Publicity under the New Sentencing Guidelines' (1992) 65 Southern California Law Review 2367.
- Crouhy, M., Galai, D., and Mark, R., Risk Management (2001).
- David, P., 'Ruling in AmSouth Case Offers Boards a Reprieve' (2006) 171(46) American Banker 2.
- Davis, E., 'What's Wrong With a Risk-Based Approach?' (2007) 8(11) *OpRisk & Compliance*http://www.opriskandcompliance.com/public/showPage.html?page=479962 at 20 January 2009.
- De Koker, L., 'Some Thoughts on the Impact of Customer Due Diligence Measures on Financial Exclusion' (2006) 13(1) *Journal of Financial Crime* 26.
- Eatwell, J. and Taylor, L., Global Finance at Risk: The Case for International Regulation (2000).
- Englehart, J.P., 'A Historical Look at Risk Management' (1994) 41(3) Risk Management 65.
- Ewing, M.A., Essays in Banking and Systemic Risk (Ph.D., Princeton University, 1998).
- Federal Financial Institutions Examination Council, *Bank Secrecy Act/Anti-Money Laundering Examination Manual* (2006).
- Fisse, B., and Braithwaite, J., Corporations, Crime and Accountability (1993).
- Fisse, B., and Braithwaite, J., The Impact of Publicity on Corporate Offenders (1983).
- Garner, B.A., Black's Law Dictionary (8th ed, 2004).

- Geary, J., Instant Freezing is a Tip-Off like No Other (2006) 9 Money Laundering Intelligence 1.
- Ginzl, D., Risk Management and the Money Laundering Challenge (2005) 20(4) Commercial Lending Review 41.
- Hoffman, K.E., 'AML Security Emphasizes Detection and Prevention' (2005) 81(1) Banking Strategies 54.
- Hopton, D., Money Laundering: A Concise Guide for all Business (2006).
- Hubbard, D., The Failure of Risk Management: Why It's Broken and How to Fix It (2009).
- Hufbauer, G.C., Schott, J.J., Elliott, K.A., and Oegg, B., *Economic Sanctions Reconsidered* (3rd ed, 2007).
- Hyewon, H., and Wagner, N., 'Corporate Criminal Liability' (2007) 44(2) *The American Criminal Law Review* 337.
- Illovsky, E., Corporate Deferred Prosecution Agreements: The Brewing Debate (2006) 21(2)

 Criminal Justice 36.
- Isaac, W.M., 'Harsh Approach to Regulation is Backfiring' (2005) 170(191) American Banker 1.
- 'Judge: Riggs was 'Henchman of Dictators' (2005) Washington Business Journal http://www.bizjournals.com/washington/stories/2005/03/28/daily13.html at 4 January 2007.
- Keenan, C., 'Overview: Will Risk Fixes Boost Competitive Edge?' (2003) 168(235)

 American Banker 12.
- Keenan, C., Weighty Challenges: Legal Issues for Bank Boards (2004) 14(3) *Bank Director Magazine* 36.
- Klein, A., 'Losses Rise If Reputation is Compromised' (2007) 20(3) *Bank Technology News* 38.
- Krebsbach, K., 'Policing Global Pirates on the River of Money' (2004) 17(4) Bank Technology News 20.
- Lam, J., 'A New Role: Chief Risk Officer' (1999) 64(2) Ivey Business Journal 55.
- Lam, J., Enterprise Risk Management: From Incentives to Controls (2003).

- Leimberg, S.R. et al, The Tools & Techniques of Risk Management & Insurance (2002).
- Levi, M., Money Laundering and Its Regulation (2002) 582 ANNALS American Academy of Political and Social Science 181.
- Li, X., A Comparative Study of Shareholders' Derivative Actions: England, the United States, Germany and China (Ph.D., Kluwer Law International, 2007).
- Looney, R., 'Economic Costs to the United States Stemming From the 9/11 Attacks' (2002) 1(6) Strategic Insights.
- Louisot, J., 'Risk Management in Practice: Reputation' (2004) 6(3) Risk Management: An International Journal 35.
- Lowthers, B., and Shultz, C., 'Integrating Identity Verification into Risk Management' (2004) 25(11) ABA Bank Compliance 36.
- Mainelli, M., 'Anti-Anti Money Laundering, Feed-Back or Fed-Up' (2005) 6(4) *Journal of Risk Finance* 386.
- Mazzucca, T., 'Shareholder Suit in Riggs' Future' (2004) 22(51) Washington Business Journal 3.
- Moll, J., Major, M., and Hoque, Z., 'The Qualitative Research Tradition', Chapter 18 in Hoque, Z. (ed), Methodological Issues in Accounting Research: Theories and Methods (2006) 375.
- Myint, R., 'Solicitors Beware: Money Laundering after R v Duff' (2003) 2(10) Journal of International Trust and Corporate Planning 65.
- Netter, B., 'Avoiding the Shameful Backlash: Social Repercussions for the Increased Use of Alternative Sanctions' (2005) 96(1) Journal of Criminal Law & Criminology 187.
- Mojuyé, B., 'What Banks Need to Know about the Patriot Act' (2007) 124(3) Banking Law Journal 258.
- O'Regan, D., Auditor's Dictionary: Terms, Concepts, Processes (2004).
- Perrin, S., 'The Pitfalls of Flagging up Suspect Bank Transactions' (2004) Financial

 Director 42

 http://images.vnunet.com/v6 static/oracle/pdf/fd/dec laundering fdbrief.pdf> at 16 August 2007.

- Preston, E., 'The US Patriot Act: New Adventures in American Extraterritoriality' (2002) 10(2) Journal of Financial Crime 104.
- 'The Pinochet Affair: A Landmark Case Study on AML Controls' (2005) 16(4) Money Laundering Alert 1.
- Quick, C., 'Money Laundering Get it Wrong, Go to Jail' (2004) 133(1325) Accountancy 46.
- Razzano, F.C., 'American Money Laundering Statutes: The Case for a Worldwide System of Banking Compliance Programs' (1994) 3(277) Journal of International Law & Practice 288.
- Reiker, M., 'Riggs-PNC Looking Alive, Though Initial Price Isn't' (2005) 170(4) American Banker 20.
- Reuter, P., and Truman, E.M., Chasing Dirty Money: The Fight against Money Laundering (2004).
- Robinson, T.L., 'A New Interpretation of the Contemporaneous Ownership Requirement in Shareholder Derivative Suits: In re Bank of New York Derivative Litigation and the Elimination of the Continuing Wrong Doctrine' (2005) 1 *Brigham Young University Law Review* 229.
- Romaniuk, P., Haber, J., and Murray, G., 'Suspicious Activity Reporting: Regulatory Change and the Role of Accountants' (2007) *The CPA Journal* 70.
- Ross, S., and Hannan, M., 'Money Laundering Regulation and Risk-Based Decision-Making' (2007) 10(1) *Journal of Money Laundering Control* 106.
- Russel, P.S., 'Money Laundering: A Global Challenge' (2004) 5(1/2) Journal of American Academy of Business 260.
- Serrano, M., and Kenny, P., 'The International Regulation of Money Laundering' (2003) 9(4) Global Governance 433.
- Simser, J., 'The Significance of Money Laundering: The Example of the Philippines' (2006) 9(3) *Journal of Money Laundering Control* 293.
- Spivack, P., and Raman, S., 'Regulating the 'New Regulators': Current Trends in Deferred Prosecution Agreements' (2008) 45(2) American Criminal Law Review 159.

- Stessens, G., Money Laundering: A New International Law Enforcement Model (2008).
- Tagoe, L., 'An Analysis of Banks' Liability for the Deposits of Proceeds of Criminal Activities in the U.K.' (2003) 4(4) *Journal of International Banking Regulation* 352.
- Thel, S., 'The Original Conception of Section 10(b) of the Securities Exchange Act' (1990) 42 Stanford Law Review 385.
- Thompson, D., 'Risk Management: A Brief History' (2003) *Journal of Banking and Financial Services* 30.
- Tucker Mann, T., 'Money Laundering' (2007) 44(2) American Criminal Law Review 769.
- Van Cleef, C.R., Silets, H.M., and Motz, P., 'Does the Punishment Fit the Crime?' (2004) 12(1) Journal of Financial Crime 56.
- Vartanian, T.P., 'Money Laundering Dominates Bank Enforcement Actions' (2004) 169(185) American Banker 10.
- World Bank, Analyzing and Managing Banking Risk: A Framework for Assessing Corporate Governance and Financial Risk (2nd ed, 2003).
- Wray, C.A., and Hur, R.K., 'Corporate Criminal Prosecution in a Post-Enron World: The Thompson Memo in Theory and Practice' (2006) 43(3) *American Criminal Law Review* 1095.
- Yeandle, M., Mainelli, M., Berendt, A., and Healy, B., Anti-Money Laundering Requirements: Costs Benefits and Perceptions (2005).

9.5 Official government reports and parliamentary testimony

- Aufhauser, D., 'Terrorism: Growing Wahhabi Influence in the United States' (Testimony before the United States Senate Committee on the Judiciary, 26 June 2003).
- Australian Transaction Reports and Analysis Centre, AUSTRAC Annual Report 2007-08 (AUSTRAC, Sydney, 2008).
- Baxter. T.C., 'Risk Management and Regulatory Failures at Riggs Bank and UBS: Lessons Learned' (Testimony before the Subcommittee on Oversight and Investigations, Committee on Financial Services, U.S. House of Representatives, 2 June 2004).

- Brown, K., (Written Statement before the Committee on Banking, Housing and Urban Affairs, United States Senate, 28 September 2004).
- Glaser, D., and Szubin, A.J., 'Isolating Proliferators and Sponsors of Terror: The Use of Sanctions and the International Financial System to Change Regime Behavior' (Joint Testimony before the Joint Hearing of the Terrorism, Non-proliferation & Trade Subcommittee of the House Foreign Affairs Committee & the Domestic and International Monetary Policy, Trade & Technology Subcommittee of the House Financial Services Committee, 110th Congress, 18 April 2007).
- New South Wales Law Reform Commission, Sentencing: Corporate Offenders (Report No 102, NSWLRC, Sydney, 2003).
- Riggs Bank N.A., (Written statement before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs of the United States Senate, Washington D.C., 15 July 2004).
- Schmidt Bies, S., 'Bank Secrecy Act Enforcement' (Testimony before the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, 3 June 2004).
- Small, R.A, 'Vulnerability of Private Banking to Money Laundering Activities' (Testimony before the Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate, 10 November 1999).
- United States Congress, Office of Technology Assessment, *Information Technologies for Control of Money Laundering*, OTA-ITC-630 (U.S. Government Printing Office, Washington D.C., 1995).
- United States Department of State, *U.S.-Macau Policy Act Report* (2004) http://www.state.gov/p/eap/rls/rpt/35706.htm at 27 January 2007.
- United States Senate Permanent Subcommittee on Investigations, Money Laundering and Foreign Corruption: Enforcement and Effectiveness of the Patriot Act (Supplemental Staff Report on U.S. Accounts used by Augusto Pinochet, Washington D.C., 16 March 2005).

9.6 Other reports and press releases

- Bank for International Settlements, 64th Annual Report (BIS, Switzerland, 1994).
- Black, J., The Development of Risk-Based Regulation in Financial Services: Canada, the U.K. and Australia (London School of Economics and Political Science, London, 2004).
- Corporate Crime Reporter, Crime without Conviction: The Rise of Deferred and Non Prosecution Agreements (CCR, New York, 2005).
- Delta Asia Financial Group, *Delta Asia Financial Group 2004 Annual Report* (DAFG, Hong Kong, 2005).
- Doerig, H., Operational Risks in Financial Services: An Old Challenge in a New Environment (Credit Suisse Group, Switzerland, 2001).
- Herring, R., International Financial Conglomerates: Implications for Bank Insolvency Regimes (Wharton School, Pennsylvania, 2003).
- Hutter, B.M., The Attractions of Risk-Based Regulation: Accounting for the Emergence of Risk Ideas in Regulation (Discussion Paper 33, London School of Economics and Political Science, London, 2005).
- Kaufman, G.G, and Scott, E.E., *Does Bank Regulation Retard or Contribute to Systemic Risk?* (Working Paper No. 211, Stanford Law School, California, 2000).
- Kerry, J., and Brown, H., *The BCCI Affair*, Report to the Committee on Foreign Relations, United States Senate, 102d Congress 2d Session Senate Print 102-140, 1992.
- National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (W.W. Norton & Company, New York, 2004).
- Prados, A.B., and Blanchard, C.M., Saudi Arabia: Terrorist Financing Issues (Congressional Research Service Report for Congress, Washington D.C., 2004).
- United Nations Development Programme, *Human Development Report 1999* (Oxford University Press, New York, 1999).
- United States Department of Justice, American Express Bank International enters into Deferred Prosecution Agreement and Forfeits \$55 million to Resolve Bank Secrecy Act Violations (Press Release, 6 August 2007).

- United States Department of Justice, Riggs Bank Enters Guilty Plea and Will Pay \$16

 Million Fine for Criminal Failure to Report Numerous Suspicious Transactions,

 Press Release (Press Release, 27 January 2005).
- United States Department of Justice, Union Bank of California enters into Deferred

 Prosecution Agreement and Forfeits \$21.6 million to Resolve Bank Secrecy Act

 Violations (Press Release, 17 September 2007).
- United States Department of Justice, U.S. Announces Agreement with United Bank of Africa (Press Release, 6 July 2007).
- United States Department of the Treasury, Statement by DAS Glaser on the Disposition of DPRK-Related Funds Frozen at Banco Delta Asia (Press Release, 19 March 2007).
- United States Department of the Treasury, *Treasury Designates Banco Delta Asia as*Primary Money Laundering Concern under USA PATRIOT Act (Press Release, 15

 September 2005).
- United States Department of the Treasury, *Treasury Finalizes Rule Against Banco Delta Asia: BDA Cut Off From U.S. Financial System* (Press Release, 14 March 2007).
- United States Department of the Treasury Office of Public Affairs, Treasury Department

 Designates Burma and Two Burmese Banks to be of "Primary Money Laundering

 Concern" and Announces Proposed Countermeasures Under Section 311 of the

 USA PATRIOT Act (Press Release, 19 November 2003).

9.7 Conference papers and speeches

- Braithewaite, J., 'Meta Risk Management and Responsive Governance' (Paper presented at the Risk Regulation, Accountability and Development Conference, Manchester, 26 June 2003).
- Bugg, D., 'Compliance through Prosecution (or Haunted by Kable)' (Speech delivered at the Australasian Law Teachers' Association Conference, Canberra, 3 July 2000).
- Byrne, J., 'How AML/CTF is Being Managed in the United States: The Impact of the Global Market Crisis on AML/CTF Including Information Sharing Between Jurisdictions

- and Institutions' (Paper presented at the Anti-Money Laundering and Counter-Terrorism Financing Conference 2009, Sydney, 2 April 2009).
- Caruana, J., 'Contemporary Issues in Credit Risk', (Speech delivered at the Credit Risk Summit USA 2003, New York, 27 October 2003).
- Cassella, S.D., 'The Case for Civil Forfeiture: Why In Rem Proceedings are an Essential Tool for Recovering the Proceeds of Crime' (Paper presented at the 25th Cambridge International Symposium on Economic Crime, Cambridge, 7 September 2007).
- Crockett, A., 'Introductory Remarks' (Speech delivered at the Third Joint Central Bank Research Conference on Risk Measurement and Systemic Risk, Basel, 7 March 2002).
- Davis, H., 'A New Regulator for the New Millenium' (Speech delivered at the Proceedings of Financial Services Authority Conference: A Radical New Approach to Regulation, London, 11 December 2000).
- Duke, J.R., 'Penalties Relating to Foreign Trusts for Failure to Report' (Speech delivered at Ashford Suites, High Point, North Carolina, 27 January 2006).
- Eatwell, J., 'International Regulation, Risk Management and the Creation of Instability' (Speech delivered at the International Monetary Fund, Washington, 1 October 2004).
- Fleming, T., 'OFAC and 311 Exposure Issues' (Paper presented at the 2006 ABA/ABA Money Laundering Enforcement Conference, Washington DC, 9 October 2006).
- Fox, W.J., (Untitled speech delivered at the Financial Services Roundtable, Washington D.C., 29 January 2004).
- lcard, A., 'Risk Measurement and Systemic Risk' (Speech delivered at the Fourth Joint Central Bank Research Conference on Risk Measurement and Systemic Risk, Frankfurt, 8 November 2005).
- Kuroda, H., 'The Importance of the Euro in a Rapidly Changing Environment: An Asian Perspective' (Speech delivered at the Brussels Economic Forum 2008: Economic and Monetary Union in Europe: 10 Years On, Brussels, 15 May 2008).

- McCarthy, C., 'Risk Based Regulation: The FSA's Experience' (Speech delivered via videolink to the Australian Securities & Investment Commission, Sydney, 13 February 2006).
- Manger, G., 'Commentary Part 2' (Speech delivered at the Anti-Money Laundering Symposium, Canberra, September/October 2002).
- Manger, G., 'Risk Management and Reputation, Commentary Part 3' (Speech delivered at the Anti-Money Laundering Symposium, Canberra, September/October 2002).
- Mitchell, S.L., 'The Implications of the USA Patriot Act on Foreign Banking Institutions' (Speech delivered at the National Anti-Money Laundering Training Seminar, St. Vincent and the Grenadines, 24 May 2002).
- Reuter. P., 'Assessing the Effects of the AML Regime: Identifying Success, the Relevant Outcomes and Metrics' (Speech delivered at the Anti-Money Laundering and Counter-Terrorism Financing Conference 2009, Sydney, 1 April 2009).
- Robinson, P., 'Effective AML the UK Story' (Speech delivered at the Asia-Pacific Financial Crime Conference & Exhibition, Singapore, July 27 2006).
- Rodrigues, A.G., 'The Prevention and the Combat of Money Laundering and Terrorist Financing: A Social Responsibility' (Speech delivered at the Anti-Money Laundering and Counter-Terrorism Financing Conference 2009, Managing Risk: Australian and International Perspectives, Sydney, 1 April 2009).
- Sassoon, J., 'Chairman's Address' (Paper delivered at the Financial Action Task Force, Paris Plenary, 12 October 2007) < http://www.fatf-gafi.org/dataoecd/0/23/39485130.pdf at 5 February 2008.
- Sharman, J.C., 'International Organisations, Blacklisting and Tax Haven Regulation' (Paper presented at the International Studies Association Meeting, Montreal, 18 March 2004).
- Thompson, L.D., (Untitled speech delivered at the Corporate Fraud Task Force Conference, Washington D.C., 26 September 2002).

9.8 News/magazine articles and media releases

- 'After Squabble, Riggs Agrees to \$643 million Buyout by PNC', *The Daily Item*(Pennsylvania) 14 February 2005

 http://archive.dailyitem.com/archive/2005/0214/biz/stories/06biz.htm at 12

 December 2006.
- Androphy, J., 'The Government's Dirty Laundry', Forbes, No. 7, 7 April 2008.
- Argenti, P.A., 'The Challenge of Protecting Reputation', Financial Times (London), 30

 September 2005 < http://news.ft.com/cms/s/7da92b26-3107-11da-ac1b-00000e2511c8.dwp_uuid=358e659a-2068-11da-b59e-00000e2511c8.html at 19

 April 2006.
- 'Bank of New York Wins the Dismissal of Shareholder Suit', *The Wall Street Journal* (New York) 29 November 2001, B14.
- Batchelor, M., 'Macau Gets Control of Banco Delta', *Bloomberg News*, 29 September 2005 http://www.iht.com/articles/2005/09/29/bloomberg/sxbanco.php at 1 January 2007.
- Blum, J., 'Equatorial Guinea, USA: US Oil Firms Entwined in Equatorial Guinea Deals', *The Washington Post* (Washington D.C.), 9 September 2004

 http://www.globalpolicy.org/nations/launder/regions/2004/09090ilfirms.htm at 15 April 2008.
- Boustany, N., and O'Hara, T., 'After Riggs, Embassy Accounts Can't Find a Home', *The Washington Post* (Washington D.C), 10 June 2004

 http://www.washingtonpost.com/wp-dyn/articles/A29674-2004Jun9.html at 8 December 2006.
- Butrin, D. et al, 'The Case of the Long Gone Cash', *Kommersant* (Moscow), 18 May 2007 http://commersant.com/p766368/r_1/money_laundering/ at 28 January 2008.
- 'China says it Regrets US Treasury Decision on N. Korea', *CNN News*, 15 March 2007 http://edition.cnn.com/2007/WORLD/asiapcf/03/15/china.macau.bank.reut/index.html at 20 March 2007.

- Chinoy, M., 'Macau Focus of Push on NK Activity', *CNN News*, 23 July 2006

 http://www.cnn.com/2006/WORLD/asiapcf/05/18/nkorea.Macau/index.html at 2 January 2007.
- Cody, E., 'U.S. Says Macau to Release \$25M in Frozen N. Korean Funds', *The Washington Post* (Washington D.C.), 10 April 2007 http://www.washingtonpost.com/wp-dyn/content/article/2007/04/10/AR2007041000165.html?hpid=moreheadlines at 17 April 2007.
- Coleman, Z., 'Banco Delta Board Yields Control', *The Standard* (Hong Kong), 29

 September 2005

 http://www.thestandard.com.hk/news_detail.asp?we_cat=4&art_id=2338&sid=47

 82658&con_type=1&d_str=20050929> at 23 January 2007.
- Cullison, A., 'Russia Sues Bank of New York Over 1990s Scandal', *The Wall Street Journal* (New York), 18 May 2007, A.3.
- 'FSA Says Demonstrating Controls Can Help Avoid Enforcement', *Compliance Reporter*, 4 July 2005, 1.
- Gardner, H., and Levitov, M., 'Russia Sues Bank of New York for \$22.5 Billion',

 **Bloomberg*, 17 May 2007

 **\frac{\text{http://www.bloomberg.com/apps/news?pid=20601087&sid=aiVrh6bgUcwk&ref}}{er=home} at 19 September 2007.
- Gertz, B., 'U.S. Sanctions Cost North Korea Millions', *The Washington Times* (Washington D.C.), 16 June 2006 http://www.washingtontimes.com/national/20060615-105145-9374r.htm at 18 January 2007.
- Gleckman, H., Borrus, A., and McNamee, M., 'Inside the KPMG Mess', *BusinessWeek*, 12 September 2005, 46.
- Greenless, D., 'Macau Inquiry Clears Bank of Money Laundering for N. Korea',

 International Herald Tribune Asia Pacific (New York), 12 March 2007

 http://www.iht.com/articles/2007/03/12/news/bank.php at 20 March 2007.
- Greenlees, D., and Lague, D., 'The Money Trail That Linked North Korea to Macao', *The New York Times* (New York), 11 April 2007

- http://www.nytimes.com/2007/04/11/world/asia/11cnd-macao.html at 5 July 2008.
- Greenless, D., and Lague, D., 'Trail Led to Macao as Focus of North Korean Corruption',

 The New York Times (New York), 13 April 2007

 http://www.nytimes.com/2007/04/13/world/asia/13macao.html?r=2&oref=slogin
 &oref=slogin> at 16 April 2007.
- Hall, K.G., 'Accounting Firm Finds No Evidence of Money Laundering', *McClatchy Newspapers* (Sacramento), 1 March 2007

 http://www.realcities.com/mld/krwashington/16812231.htm at 12 March 2007.
- Hall, K.G., 'Under Patriot Act, Treasury Casts a Wide Net', *McClatchy Newspapers* (Sacramento), 12 March 2007

 http://www.mcclatchydc.com/148/story/15754.html at 26 January 2009.
- Hamilton, W., 'KPMG Avoids Potential Collapse', *Los Angeles Times* (Los Angeles), 30 August 2005 < http://articles.latimes.com/2005/aug/30/business/fi-kpmg30 at 21 January 2009.
- 'HK PRESS: Macau's Banco Delta Asia Seeking Buyer', *The Standard* (Hong Kong), 27 February 2006 < http://asia.news.yahoo.com/060227/5/2ghrt.html at 4 January 2007.
- Isikoff, M., '9-11 Hijackers: A Saudi Money Trail?', *NewsWeek*, 22 November 2002 http://www.truthout.org/docs_02/11.26A.newswk.911.htm at 12 December 2006.
- 'Japan Closes Citibank Branches', *BBC News*, 17 September 2004

 http://news.bbc.co.uk/1/hi/business/3666828.stm at 30 April 2006.
- Johnson, T., 'Seizure of a Tiny Bank Linked to N. Korea May Soon End', *Monterey Herald* (Monterey), 8 March 2007

 http://www.montereyherald.com/mld/montereyherald/news/world/16862840.htm
 at 12 March 2007.
- Jopson, B., 'Is the Gamekeeper Tied Down by the Big Four?', *Financial Times* (London), 14 September 2006, 8.

- King, J., 'FBI Probes Possible Saudi, 9/11 Money Ties', CNN News, 23 November 2002 http://archives.cnn.com/2002/US/11/23/saudi.fbi.911/ at 11 December 2006.
- 'KPMG Pays \$456 million US Fine, 8 Former Execs Charged with Conspiracy', CBC

 News, 29 August 2005

 http://www.cbc.ca/money/story/2005/08/29/KPMG_fined20050829.html at 15 May 2008.
- Lague, D., 'Macao Set to Resolve North Korea Snag, U.S. Says', *The New York Times* (New York), 11 April 2007

 http://www.nytimes.com/2007/04/11/world/asia/11korea.html> at 17 April 2007.
- 'Laundering Charge Hits Macau Bank', *BBC News*, 19 September 2005 http://news.bbc.co.uk/1/hi/business/4261450.stm at 30 December 2006.
- Landay, J.S., and Hall, K.G., 'U.S. Claims about Macau Bank Questioned', *The Seattle Times* (Seattle), 2 March 2007 < http://archives.seattletimes.nwsource.com/cgi-bin/texis.cgi/web/vortex/display?slug=nkorea02&date=20070302 at 12 March 2007.
- Lawder, D., 'Macau Bank Struggles to Shake Off North Korea Links', *Reuters UK*, 21

 December 2006

 http://uk.reuters.com/article/featuresNews/idUKSP15073620061222 at 25 April 2007.
- Lee, J., 'Macau Calls for Calm in Wake of U.S. Money-Laundering Charge', *Radio Free Asia*, 17 September 2005

 http://www.rfa.org/english/news/2005/09/17/Macau_bank/> at 10 January 2007.
- Lichtblau, E., 'Leniency for Big Corporations in the U.S.', *International Herald Tribune*(New York), 9 April 2008

 http://www.iht.com/articles/2008/04/09/business/justice.php at 16 May 2008.
- Lopez, J.C., 'Pinochet 'Used Wide Bank Network', *CNN News*, 16 March 2005

 http://edition.cnn.com/2005/WORLD/americas/03/16/pinochet.funds/ at 12

 December 2006.

- McGlynn, J., 'Banco Delta Asia, North Korea's Frozen Funds and US Undermining of the Six-Party Talks: Obstacles to a Solution', *Japan Focus*, 9 June 2007 http://japanfocus.org/products/details/2446 at 29 June 2008.
- 'Macau Bank drops North Korean Clients', *BBC News*, 16 February 2006 http://news.bbc.co.uk/1/hi/business/4718922.stm at 2 January 2007.
- Medetsky, A., and Elder, M., 'Bank of New York Sued by Russian Customs for \$22Bln for Money Laundering', *The Moscow Times* (Moscow), 18 May 2007, 2.
- Newman, R., 'Firms Tackle Money Laundering', *Knight Ridder Tribune Business News*, 5 October 2006, 1.
- 'No Sign of Thaw for Delta Asia', *Macau Business*, 1 January 2006

 http://www.Macaubusiness.com/index.php?id=367> at 3 January 2007.
- O'Brien, T.L., 'At Riggs Bank, a Tangled Path Led to Scandal', *The New York Times* (New York), 19 July 2004

 http://www.nytimes.com/2004/07/19/business/19BANK.final.html?ex=124797600
 0&en=cb5f669d9fc948cd&ei=5088&partner=rssnyt> at 15 December 2006.
- O'Hara, T., 'Allbrittons, Riggs to Pay Victims of Pinochet', *The Washington Post* (Washington D.C.), 26 February 2005 http://www.washingtonpost.com/wp-dyn/articles/A53805-2005Feb25.html at 18 December 2006.
- O'Hara, T., 'In Cultivating International Clients, Riggs Went Down a Perilous Path', *The Washington Post* (Washington D.C.), 21 March 2005

 http://www.washingtonpost.com/ac2/wp-dyn/A52084-2005Mar20?language=printer at 24 December 2006.
- O'Hara, T., 'Judge Backs Riggs's \$16 Million Plea Deal', *The Washington Post* (Washington D.C.), 30 March 2005 http://www.washingtonpost.com/wp-dyn/articles/A11383-2005Mar29.html at 23 December 2006.
- O'Hara, T., 'Riggs Bank Agrees to Guilty Plea and Fine', *The Washington Post* (Washington D.C.), 28 January 2005, A01.
- O'Hara, T., Riggs, 'PNC Reach New Merger Agreement', *The Washington Post* (Washington D.C.), 11 February 2005 http://www.washingtonpost.com/wp-dyn/articles/A13829-2005Feb10.html at 3 December 2006.

- O'Hara, T., 'PNC Settles Last Riggs Shareholder Suit', *The Washington Post* (Washington D.C.), 13 October 2005 http://www.washingtonpost.com/wp-dyn/content/article/2005/10/12/AR2005101202163_pf.html at 23 December 2006.
- O'Hara. T., and Day, K., 'Riggs Bank Hid Assets of Pinochet, Report Says', *The Washington Post* (Washington D.C.), 15 July 2004 < http://www.washingtonpost.com/wp-dyn/articles/A50222-2004Jul14.html at 24 December 2006.
- 'Owning Up: Delta Asia Admits Selling Pyongyang Gold', *Macau Business*, 1 January 2007 http://www.macaubusiness.com/index.php?id=672 at 28 April 2007.
- Pacelle, M., 'Riggs Sues PNC as Deal Collapses', *The Wall Street Journal* (New York), 8 February 2005, A.3.
- Parloff, R., 'Bank of New York's \$22.5 Billion Headache', Fortune, 24 September 2008

 http://money.cnn.com/2008/09/23/news/companies/parloff_bank_new_york.fortune/index.htm at 14 January 2008.
- Paulson, M., 'History of U.S. Sanctions Shows Most Haven't Worked', *Seattle Post-Intelligencer*, 11 May 1999 < http://seattlepi.nwsource.com/iraq/sanction.shtml at 30 December 2008.
- 'PBC Fines BTMU CNY1.2mn for Violation of Anti-Money Laundering', SinoCast China Business Daily News (Beijing), 5 April 2006, 1.
- 'Pinochet's Web of Bank Accounts Exposed', *Guardian Unlimited*, 16 March 2005 http://www.guardian.co.uk/pinochet/Story/0,.1488929,00.html at 17 December 2006.
- 'Riggs National Accepts Reduced PNC Merger Deal', Finfacts Ireland, 11 February 2005

 http://www.finfacts.com/cgi-bin/irelandbusinessnews/exec/view.cgi?archive=2&num=424 at 20 December 2006.
- Simpson, G.R., 'ABN Amro to Pay \$80 Million Fine Over Iran, Libya', *The Wall Street Journal* (New York), 20 December 2005, A.3.
- Simpson, G.R., 'Riggs Bank Is Sued over 9/11 Attacks', *The Wall Street Journal* (New York), 13 September 2004, B.3.

- Simpson, G.R., 'Senate Panel Blasts Riggs Bank; Scathing Report Claims Corruption Flourished Amid Inadequate Oversight', *The Wall Street Journal* (New York), 15 July 2004, A.3.
- Simpson, G.R., Fairclough, G., and Solomon, J., 'U.S. Probes Banks' North Korea Ties', *The Wall Street Journal* (New York), 8 September 2005, A.3.
- 'Some Shareholders Sue Bank of New York', *The New York Times* (New York), 25
 September 1999
 http://query.nytimes.com/gst/fullpage.html?res=9E06E4D7133FF936A1575AC
 0A96F958260> at 3 November 2007.
- Suparno, R., 'The Euro: A Viable Alternative to the U.S. Dollar', *The Jakarta Post* (Jakarta), 18 July 2005 http://www.thejakartapost.com/news/2005/07/18/euro-viable-alternative-us-dollar.html at 24 January 2009.
- 'Treasury Bars Deals with Macau's Banco Delta', *CNN News*, 14 March 2007

 http://money.cnn.com/2007/03/14/news/international/macau.reut/index.htm?postversion=2007031417 at 20 March 2007.
- 'U.S. Money Laundering Accusation Ignites Resentment in Macau', *People's Daily Online* (Beijing), 17 September 2005

 http://english.peopledaily.com.cn/200509/17/eng20050917_209027.html at 9

 January 2007.
- Ustinova, T., and Stempel, J., 'Russia Sues Bank of New York for \$22.5 Billion', *Reuters*, 17 May 2007

 http://www.reuters.com/article/businessNews/idUSL175611720070517?pageNumber=2&sp=true at 20 September 2007.
- Wilke, J.R., and Pacelle, M., 'Riggs Is Set to Plead Guilty to Crime', *The Wall Street Journal* (New York), 26 January 2005 http://tania.blythe-systems.com/pipermail/nytr/Week-of-Mon-20050124/012447.html at 13 December 2006.
- Wright, T., 'UBS Sells 3 Private Banks to Another Unit of a Rival', *The New York Times* (New York), 6 September 2005, C2.

9.9 Other materials

- Abramson, L., and Godoy, M., *The Patriot Act: Key Controversies* (2006) NPR http://www.npr.org/news/specials/patriotact/patriotactprovisions.html at 1 May 2008.
- ACI and TowerGroup, Money Laundering: Preserving the Integrity of Financial Institutions (2002) < http://www.aciworldwide.com/pdfs/aci_trends_frauddetect2.pdf at 1 April 2006.
- Advisen, Shareholder Derivative Suits: A Growing Concern for Corporate Directors and Officers (2005)

 http://www.cnapro.com/pdf/ShareholderDeriviativeSuits_Advisen.pdf at 25 June 2006.
- Ainslie, E.K., Indicting Corporations Revisited: Lessons of the Arthur Andersen Prosecution (2004) American College of Trial Lawyers

 http://www.actl.com/AM/Template.cfm?Section=All_Publications&Template=/C

 M/ContentDisplay.cfm&ContentFileID=51> at 4 August 2008.
- Allens Arthur Robinson, Civil Penalty Provisions in Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (2006) http://www.aar.com.au/pubs/fmres/foamldec06.htm at 24 August 2007.
- Allens Arthur Robinson, 'Corporate Culture' as a Basis for the Criminal Liability of Corporations (2008) < http://198.170.85.29/Allens-Arthur-Robinson-Corporate-Culture-paper-for-Ruggie-Feb-2008.pdf at 2 January 2009.
- American Bar Association, *Director Oversight Duties after Caremark* (2001) http://www.abanet.org/buslaw/committees/CL996000pub/newsletter/200703/ at 24 November 2007.
- Aon Corporation, *Corporate Reputation: Not Worth Risking* (2003)

 http://www.aon.com/about/publications/pdf/issues/wharton_corp_rep_r040303.pd
 at 19 April 2006">f> at 19 April 2006.
- Asia-Pacific Group on Money Laundering, Summaries of Mutual Evaluation Reports

 Adopted in 2002 2003 (2003)

- http://www.apgml.org/documents/docs/8/Summary%20ME%20Reports%20200 2-03.pdf> at 28 January 2008.
- Australian Institute of Criminology, *The Global Response to Money Laundering: How Global Politics Shaped the Result* (2002)

 http://www.aic.gov.au/conferences/2002-ml/broome.pdf> at 17 February 2008.
- Australian Transaction Reports and Analysis Centre, AUSTRAC Information Circular No. 45

 U.S. Department of the Treasury Financial Crimes Enforcement Network

 (FinCEN) Advisory Regarding North Korea (2006)

 http://www.austrac.gov.au/files/aic_45_fincen_advisory_regarding_north_korea.p
 df> at 27 January 2009.
- Australian Transaction Reports and Analysis Centre, *Introduction to AML/CTF*http://www.austrac.gov.au/elearning/mod1/mod_1_money_laundering_3.html at 27 July 2008.
- Australian Transaction Reports and Analysis Centre, *Introduction to AML/CTF: Terrorism Financing*http://www.austrac.gov.au/elearning/pdf/mod_terrorism_financing.pdf> at 18
 February 2008.
- Australian Transaction Reports and Analysis Centre, *Risk Management: A Tool for Small-to-Medium Sized Businesses* http://www.austrac.gov.au/risk_management.html at 6 October 2009.
- Bakerplatt, Riggs Bank the fall of an Institution A Salutary Lesson for All? (2005) http://www.bakerplatt.com/upload/public/Files/1/artriggsbank.pdf at 15 May 2007.
- Binnington, A., Constructive Trusts And All Crimes Money Laundering Legislation: Is

 There a Problem? (1998) Jersey Legal Information Board

 http://www.jerseylegalinfo.je/publications/jerseylawreview/Oct98/constructive_t
 rusts.aspx> at 10 October 2006.
- Blank Rome LLP, Riggs Bank, N.A. Agrees to Plead Guilty to Bank Secrecy Act Violations and Pay \$16 Million Fine (2005)

- http://www.blankrome.com/index.cfm?contentID=37&itemID=382 at 12 December 2006.
- Borchersen-Keto, S., OCC says Mistakes Made in Oversight of Riggs Bank's Compliance with BSA (2004) Compliance Headquarters

 http://www.complianceheadquarters.com/AML/AML_Articles/6_4_04.html at 28 December 2006.
- Bosworth-Davies, R., How Do I Know When I am Suspicious? (2004) SAS http://www.sas.com/news/feature/fsi/dec04aml.html at 1 June 2008.
- Carey Olsen, Latest Developments in Anti-Money Laundering Provisions (2006)

 http://www.careyolsen.com/downloads/co100453.pdf> at 13 December 2007.
- Cassella, S.D., Recovering the Proceeds of Crime from the Correspondent Account of a Foreign Bank (2005).

 http://works.bepress.com/cgi/viewcontent.cgi?article=1015&context=stefan_cassella at 22 May 2008.
- Chalmers, R., *Risk-based Approach to AML/CTF*, United Kingdom Financial Services
 Authority < http://www.fscey.gov.tw/public/Attachment/7103115302771.pdf at 30 September 2008.
- Cohen, Milstein, Hausfeld & Toll P.L.L.C., *PNC Settles Last Riggs Shareholder Suit* (2005) http://www.cmht.com/cases riggsarticle.php> at 12 December 2006.
- Economist Intelligence Unit and PricewaterhouseCoopers, *Taming Uncertainty: Risk*Management for the Entire Enterprise (2002) PricewaterhouseCoopers

 http://www.pwc.com/images/gx/eng/fs/111802taming.pdf> at 11 August 2006.
- Elliott, K.A., Hufbauer, G.C., and Oegg, B., The Concise Encyclopaedia of Economics (2nd ed, undated) < http://www.econlib.org/library/Enc/Sanctions.html at 30 December 2008.
- Fagg, S., \$4.5 Billion Laundering Estimate (2007) Lawyers Weekly http://www.lawyersweekly.com.au/articles/4-5-billion-laundering-estimate-z137203.htm at 9 June 2008.

- Fagg, S., Laundering Causing Recruiting Woes (2006) Human Resources Magazine http://www.humanresourcesmagazine.com.au/articles/a0/0c043fa0.asp at 20 September 2006.
- Fagg, S., Risk-based Laundering Approach Yields Little Fruit (2007) Lawyers Weekly http://www.lawyersweekly.com.au/articles/Risk-based-laundering-approach-yields-little-fruit_z70171.htm at 29 April 2008.
- Financial Action Task Force, Guidance on the Risk-Based Approach to Combating Money

 Laundering and Terrorist Financing High Level Principles and Procedures

 (2007) Organisation for Economic Cooperation and Development

 http://www.oecd.org/dataoecd/43/46/38960576.pdf> at 29 April 2008.
- Financial Action Task Force, *Risk-Based Approach: Guidance for Money Services***Businesses* (2009) < http://www.fatf-gafi.org/dataoecd/45/1/43249256.pdf> at 7

 October 2009.
- Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Combating the Financing of Terrorism Australia* (2005) Organisation for Economic Cooperation and Development http://www.oecd.org/dataoecd/60/33/35528955.pdf at 3 May 2008.
- Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Combating the Financing of Terrorism Summary: Switzerland* (2005) http://www.fatf-gafi.org/dataoecd/60/30/35529139.pdf at 19 November 2007.
- Financial Action Task Force Secretariat, Interpretative Note to Special Recommendation II:

 Criminalising the Financing of Terrorism and Associated Money Laundering

 (2004) Asia-Pacific Group on Money Laundering

 http://apgml.org/issues/docs/14/FATF%20Interpretative%20Note%20to%20Sp%20Rec%20II.doc at 26 July 2007.
- Financial Crimes Enforcement Network, Advisory: Guidance to Financial Institutions on the Provision of Banking Services to North Korean Government Agencies and Associated Front Companies Engaged in Illicit Activities (2005)

 http://www.fincen.gov/advisory.pdf at 14 March 2007.

- Financial Crimes Enforcement Network, Assessment of Civil Money Penalty in the Matter of Riggs Bank N.A., No. 2004-01 (2004)
 http://www.fincen.gov/riggsassessment3.pdf> at 2 January 2007.
- Financial Crimes Enforcement Network, FinCEN Withdraws Finding on Latvia's Multibanka and Issues Final Rule against Latvia's VEF Banka (2006)

 http://www.fincen.gov/latvia 311 withdraw.html> at 5 December 2006.
- Financial Crimes Enforcement Network, Treasury Issues Final Rule against Commercial

 Bank of Syria U.S. Financial Institutions Must Terminate Correspondent Accounts

 (2006) U.D. Department of the Treasury

 http://www.ustreas.gov/press/releases/js4105.htm at 5 December 2006.
- Financial Services Commission Mauritius, Code on the Prevention of Money Laundering and Terrorist Financing (Intended for Management Companies) (2003)

 at 26 August 2007.
- Fisher, B., *Money Laundering What You Don't Know Can Hurt You*, ACI Worldwide, http://www.aciworldwide.com/pdfs/aci_trends_frauddetect.pdf at 13 March 2006.
- Gallo, P.A., *The Writing on the Bank of Scotland's Wall* (2002) Pacific Risk Ltd http://www.asiamaze.com/asiamaze%20-%20BoS%20ABC%20Case.pdf at 20 November 2007.
- Godse, V., *Anti-Money Laundering*, L&T Infotech Confidential 2

 http://202.81.207.25/Intinfotech/WhitePapers/AML%20Whitepaper.pdf at 15

 June 2007.
- Harris, R., *Picking Up the Pieces* (2004) CFO Magazine http://www.cfo.com/printable/article.cfm/3015379?f=options at 19 April 2006.
- Hasnas, J., Rethinking Vicarious Criminal Liability: Corporate Culpability for White-Collar Crime (2006) The Heritage Foundation

 http://www.heritage.org/Research/LegalIssues/wm1195.cfm at 30 December 2008.

- Hauben, R., North Korea's \$25 Million and Banco Delta Asia: Another Abuse under the U.S. Patriot Act (2001) (2007) NewsGroups

 http://newsgroups.derkeiler.com/pdf/Archive/Soc/soc.culture.korean/2007-03/msg00027.pdf at 26 January 2009.
- Heir, K., *Encyclopaedia of Management*, Reference for Business http://www.referenceforbusiness.com/management/Pr-Sa/Risk-Management.html at 14 August 2006.
- Heller Ehrman LLP, Banco Delta Asia has Terminated its North Korean Business and Will Implement a New Anti-Money Laundering Program (2006)

 http://www.hellerehrman.com/en/news/press/press 3289.html> at 3 January 2007.
- Herbert, C., Five Ways to Manage Operational Risk in an Even Riskier World, IBM

 Australia http://www-8.ibm.com/nz/media/downloads/IBMarticles/Operational_risk.pdf at 23 May 2006.
- Herbert-Smith, *The Effect of the Risk Based Approach on Civil Liability* (2006) http://www.herbertsmith.com/NR/rdonlyres/F9AC5EB7-8A64-43C2-AA40-650B320155F4/2275/TheeffectofriskbasedapproachJune2806.html at 2 November 2006.
- HM Treasury, *Money Laundering Regulations 2007: An Information Sheet for Firms* (2007) http://www.hm-treasury.gov.uk/media/2/6/moneylaundering_guide150807.pdf at 26 July 2008.
- HM Treasury, The UK's Anti-Money Laundering Legislation and the Data Protection Act 1998: Guidance Notes for the Financial Sector (2002) http://www.hm-treasury.gov.uk/mediastore/otherfiles/money_laundering.pdf at 22 November 2007.
- Hogan & Hartson, The Long Arm (and Tight Grip) of Deposit Forfeiture Under the USA PATRIOT Act (2007)

 http://www.hoganandhartson.com/files/Publication/dd5bbfdc-e2a2-466e-a9e3-f3609bb82b63/Presentation/PublicationAttachment/b608bc68-2e17-4fd8-ab7b-ffab2baca6ca/FinSvcRegUpdate.pdf at 22 May 2008.

- International Monetary Fund, Offshore Financial Centers: The Role of the IMF (2000) http://www.imf.org/external/np/mae/oshore/2000/eng/role.htm at 13 May 2006.
- International Monetary Fund, The IMF and the Fight against Money Laundering and the Financing of Terrorism: A Factsheet (2005)

 http://www.imf.org/external/np/exr/facts/aml.htm at 17 May 2006.
- International Organization for Standardization, Committee Draft of ISO 31000 Risk Management (2009) http://www.npc-se.co.th/pdf/iso31000/ISO FDIS 31000 (E).pdf> at 6 October 2009.
- International Organization for Standardization, *Risk Management Vocabulary Guidelines for Use in Standards* (2002).
- Jones Day, Shareholder Derivative Actions Overview http://www.jonesday.com/shareholder_derivative_actions/ at 24 June 2007.
- Kaplan, L.A., Some Reflections on Corporate Criminal Responsibility (2007) The Antitrust Source http://www.abanet.org/antitrust/at-source/07/10/Oct07-Kaplan10-18f.pdf at 31 December 2008.
- Khoury, P.F., *DOJ's "Thompson Memo" Is Unconstitutional* (2006) Wiley Rein LLP http://www.wileyrein.com/publication.cfm?publication_id=12690> at 3 August 2008.
- KPMG, Global Anti-Money Laundering Survey: How Banks Are Facing up to the Challenge (2004)

 http://www.kpmg.ca/en/industries/fs/banking/documents/globalAntiMoneyLaunderingSurvey.pdf> at 1 September 2006.
- KPMG, Global Anti-Money Laundering Survey 2007 (2007)

 http://www.kpmg.com/SiteCollectionDocuments/Global%20Anti-money%20laundering%20survey%202007.pdf at 9 June 2008.
- Landau, S., and Anderson, S., *Blood Deposits and the Riggs Bank: Pinochet's Bank Finally Pays Up* (2005) Counterpunch

 http://www.counterpunch.org/landau03122005.html at 7 December 2006.

- Law Society of England and Wales, *Guide Online*http://www.lawsociety.org.uk/professional/conduct/guideonline/view=page.law?
 POLICYID=225074> at 12 November 2006.
- Levi, M., and Reuter, P., *Money Laundering* (2006) The University of Chicago http://www.publicpolicy.umd.edu/faculty/reuter/Working%20Papers/Levi_and_R euter.pdf> at 16 October 2008.
- Levitt, M., Pulling Tehran's Purse Stings: Leveraging Sanctions and Market Forces to Alter Iranian Behavior (2007) The Washington Institute

 http://www.washingtoninstitute.org/templateC07.php?CID=333 at 8 April 2007.
- McGlynn, J., Banco Delta Asia, North Korea's Frozen Funds and US Undermining of the Six-Party Talks: Obstacles to a Solution. Part III (2007) Japan Focus http://www.japanfocus.org/-John-McGlynn/2446 at 5 May 2009.
- McNeil, C., Laundering Lessons from the UK (2006) Risk Management Magazine

 http://www.riskmanagementmagazine.com.au/articles/1D/0C047E1D.asp?Type

 =125&Category=1241> at 29 July 2007.
- Mantas Inc. and Celent Communications, White Paper: Using Behaviour Detection to

 Identify Operational Risk (2003)

 http://www.mantas.com/GlobalAssets/PDF/WhitePapers/CelentOperationalRisk.p

 df> at 1 April 2006.
- Memorandum from Larry D. Thompson, Deputy Attorney General, to Heads of Department Components and United States Attorneys, 20 January 2003

 http://www.usdoj.gov/dag/cftf/corporate_guidelines.htm> at 1 August 2008.
- Memorandum from Paul J. McNulty, Deputy Attorney General, to Heads of Department Components and United States Attorneys, 12 December 2006. http://www.usdoj.gov/dag/speeches/2006/mcnulty_memo.pdf at 1 March 2009.
- Mercator Advisory Group, *Anti-Money Laundering Technology* (2005)

 http://mercatoradvisorygroup.com/index.php?doc=news&action=view_item&type

 =2&id=156> at 16 October 2006.
- MorrisJames, Supreme Court Interprets the "Duty" to Act in Good Faith (2006) Delaware Business Litigation Report

- http://www.delawarebusinesslitigation.com/archives/case-summaries-supreme-court-interprets-the-duty-to-act-in-good-faith.html at 19 November 2007.
- New York State Society of CPA's, *Riggs Bank is Sued over 9/11 Attacks* (2004) http://www.nysscpa.org/home/2004/904/2week/article4.htm at 14 April 2007.
- O'Callaghan, T., and Alfano, J., *Money Laundering and the Financing of Terrorism: Back to Basics* (2007) Money Management

 http://www.moneymanagement.com.au/Article.aspx?ArticleID=215380> on 23

 March 2008.
- Office of the Comptroller of the Currency, Consent Order of Civil Money Penalty in the Matter of Riggs Bank N.A. (2004) http://www.occ.treas.gov/ftp/eas/EA2004-44.pdf> at 5 January 2007.
- Office of the Comptroller of the Currency, *Interagency Statement of Civil Monetary*Penalties (1998) < http://www.occ.treas.gov/ftp/bulletin/98-32.txt at 23 August 2008.
- Office of the Comptroller of the Currency, *Money Laundering: A Banker's Guide to Avoiding Problems* (2002) http://www.occ.treas.gov/moneylaundering2002.pdf at 18 June 2007.
- Office of the Comptroller of the Currency, OCC Assesses \$25 Million Penalty against Riggs

 Bank N.A. (2004)

 http://www.occ.treas.gov/toolkit/newsrelease.aspx?Doc=5AOFP8K.xml at 20

 December 2006.
- Office of Foreign Assets Control, OFAC Compliance Mandatory; Penalties for Non-Compliance Staggering

 http://216.70.94.10/legupdates/officeofforeignassetscontrol.pdf at 18 November 2006.
- Office of Foreign Assets Control, Cuba: What You Need to Know about the U.S. Embargo (2004) http://www.treas.gov/offices/enforcement/ofac/programs/cuba/cuba.pdf at 19 October 2007.
- Office of the Superintendent of Financial Institutions, Guidelines on Deterring and Detecting

 Money Laundering and Terrorist Financing: Sound Business and Financial

- Practices (2003) < http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/guidelines/sound/guidelines/B8_e.pdf at 29 April 2008.
- Oliver, P., Reputation and Risk on the Line (2006) Lawyers Weekly http://www.lawyersweekly.com.au/articles/50/0C045650.asp?Type=55&Category=1325> at 3 November 2006.
- People's Bank of China, China Became a Full Member of Financial Action Task Force on Anti-Money Laundering (2007)

 http://www.pbc.gov.cn/english//detail.asp?col=6400&ID=872 at 17 July 2007.
- Perry, J., and de Fontnouvelle, P., Measuring Reputational Risk: The Market Reaction to Operational Loss Announcements (2005) Federal Reserve Bank of Boston http://www.bos.frb.org/bankinfo/qau/jppd1005.pdf> at 30 March 2006.
- Proceedings Summary 19/1997 C, Separate Proceeding III. Operation Condor for the crimes of terrorism and genocide, in the Central Investigative Court N° 5, Madrid, before Garcia Gutierrez S/N on 16 September 2004.
- SAS Institute and Lepus, Anti-Money Laundering Reappraised: The Benefits of a Holistic,
 Risk Based Approach (2006) West Coast Anti-Money Laundering Forum
 http://www.wcamlforum.org/pdf/Anti-Money%20Laundering%20Reappraised%20-%20SAS%20-%202006-05.pdf at 30 April 2008.
- Schott, P.A., Comprehensive Reference Guide to AML/CTF, World Bank
 http://www1.worldbank.org/finance/html/amlcft/docs/Ref_Guide_EN/v2/01-Ch01_EN_v2.pdf> at 20 December 2008.
- Suresha, R., and Karthik, K.V., *Mitigating Operational Risk An Approach to Countering Money Laundering*, Iflex Consulting http://www.iflexconsulting.com/Expertise/mitigate.pdf> at 2 June 2006.

- Swedish Regulator Fines Forex AB Over \$7 Million for AML Deficiencies (2008)

 Moneylaundering.com

 http://www.moneylaundering.com/NewsBriefDisplay.aspx?id=1794-at-16 March 2009.
- Trzaskowski, J., *Legal Risk Management Some Reflections* (2005) Legal Risk Management http://www.legalriskmanagement.com/PUBLICATIONS/2005_LRM.pdf at 28 March 2006.
- UBS, UBS Statement on Regulatory Actions by the U.S. Federal Reserve and the Swiss

 Federal Banking Commission (2004)

 http://www.ubs.com/1/e/media_overview/media_global/search1/search10?newsId

 =59058> at 24 January 2009.
- United Kingdom Financial Services Authority, A Risk-Based Approach to Anti-Money

 Laundering Supervision in the U.K. (2008)

 http://www.fsa.gov.uk/pages/About/What/financial_crime/pdf/amlsf_mar08.pdf
 at 20 January 2009.
- United Kingdom Financial Services Authority, *Enforcement Handbook* http://fsahandbook.info/FSA/extra/4755.pdf> at 12 July 2008.
- United Nations Information Service, Countries Invited to Sign, Ratify or Accede to

 Multilateral Treaties During the Treaty Event 23-25 and 29 September and 1

 October 2008, UNIS/INF/281, 22 September 2008.
- United States Customs and Border Protection, Manhattan Bank Pleads Guilty to U.S.

 Criminal Charges for Failure to Report \$123 Million in Suspicious Cash Deposits
 (2002)

 http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/legacy/2002/1120
 02/11272002.xml> at 25 July 2007.
- United States Department of Justice, Field Guidance on New Authorities (Redacted) Enacted in the 2001 Anti-Terrorism Legislation (2001)

 http://usacm.acm.org/usacm/DOJ_Terrorism_Law.htm at 1 November 2007.

- United States Department of the Treasury, BSA/AML Getting it Right: OTS Formal and Informal Enforcement Actions (2006)

 http://www.ots.treas.gov/docs/4/480250.pdf> at 6 January 2008.
- United States Department of the Treasury, 'Finding That Banco Delta Asia SARL is a Financial Institution of Primary Money Laundering Concern', *Federal Register*, Vol. 70, No. 181, 20 September 2005, 55215.
- United States Federal Reserve, *The PNC Financial Services Group, Inc., Pittsburgh,*Pennsylvania: Order Approving the Merger of Bank Holding Companies (2005)

 http://www.federalreserve.gov/boarddocs/press/orders/2005/200504262/attachment.pdf> at 14 December 2006.
- United States Government, *U.S. Federal Register*, Vol. 73, No. 174, 8 September 2008, 51933-51941.
- United States Government, U.S. Federal Register Proposed Rules, Vol. 71, No. 134, 13 July 2006, 39606.
- United States Sentencing Commission, Federal Sentencing Guideline Manual (2006) http://www.ussc.gov/2006guid/tabcon06 1.htm> at 10 October 2007.
- United States Sentencing Commission, Federal Sentencing Guideline Manual (2008) http://www.ussc.gov/2008guid/tabcon08_1.htm> at 3 October 2009.
- United States Sentencing Commission, *Sourcebook of Federal Sentencing Statistics* (2006) http://www.ussc.gov/ANNRPT/2006/SBTOC06.htm at 10 October 2007.
- United States Sentencing Commission, *Sourcebook of Federal Sentencing Statistics* (2008) http://www.ussc.gov/ANNRPT/2006/SBTOC08.htm at 3 October 2009.
- Wells, C., Criminal Responsibility of Legal Persons in Common Law Jurisdictions, Paper prepared for OECD Anti-Corruption Unit, Paris, 4 October 2000.
- Wessing, T., Money Laundering: Changes to the UK's Money Laundering Regime (2005)

 http://www.taylorwessing.com/website/generator/taylorwessing/content/publications/items/UK/MondeyLaundering_TWUK_english.de,property=file.pdf at 20 October 2006.

- Wolfsberg Group, Anti-Money Laundering Principles for Correspondent Banking (2002) http://www.wolfsberg-principles.com/faq-correspondent-banking.html at 3 September 2006.
- Wolfsberg Group, Wolfsberg Statement Guidance on a Risk Based Approach for Managing Money Laundering Risks (2006) http://www.wolfsberg-principles.com/risk-based-approach.html at 24 May 2006.
- World Bank, *Money Laundering Impacts Development*http://www1.worldbank.org/finance/html/amlCTF/docs/Ref_Guide_EN/v2/02-Ch02_EN_v2.pdf at 1 April 2006.
- World-Check, Reputation Damage: The Price Riggs Paid < http://www.world-check.com/media/d/content_whitepaper_reference/whitepaper-3.pdf at 14 December 2006.
- Zarate, J.C., Financial Power and International Security: Reflections on the Evolution of the Global Anti-Money Laundering and Counter-Terrorist Financing Regime since 9/11, UBS Money Laundering Prevention Newsletter, Spring 2009, 15.

RARE BOOKS LIB.

- ^ MAR 2000

