Volume 8 Dec 2009 Number 2

JOURNAL OF LAW AND FINANCIAL MANAGEMENT

IN THIS ISSUE

JOURNAL OF LAW AND FINANCIAL MANAGEMENT

JOINT EDITORS

Tyrone M Carlin
and
Guy Ford
University of Sydney

The mode of citation of this volume is
(2009) 8(2) JLFM Page

ISSN 1446 - 6899

The Journal of Law and Financial Management is a refereed Journal. Every manuscript submitted to the journal is subject to review by at least one independent, expert referee.

CONTENTS

EDITORIAL

As 2009 draws to a close, we observe the dust settling over a business landscape startled by the impact of the global financial crisis. While commentators continue to reflect on and debate the causes and flow-on consequences from this unique confluence of events, many would agree that poor ethical behaviour, inadequate disclosure and an absence of appropriate risk measurement among banks were factors that contributed to the extreme erosion in value and unprecedented regulatory intervention.

In this issue, the Journal of Law & Financial Management provides a collection of timely articles examining business regulation issues in the wake of the global financial crises including ethics, banking disclosure and risk measurement among financial institutions.

Firstly, Barbara Mescher examines the role of ethics in contract performance and highlights critical issues associated with the application of ethical principles in business. Next, Nigel Finch examines the issues and trends in loan loss provisioning among Australasian banks. This study examines the practice of loan impairments and provisions over the period 2006 to 2009, a period designed to capture the impact of the global financial crises and interrogate the banks' response to this event. Finally, David Chaikin provides a commentary on the use and effectiveness of risk-based models in financial institutions. In response to many challenges such as money laundering and terrorism financing, financial institutions are expected to apply 'best practice' strategies designed to reduce the risk of being exposed to these financial crimes; however, as Chaikin illustrates, money laundering risks often remain even where financial institutions comply with regulatory requirements and best practices in risk management.

Tyrone M Carlin & Guy Ford

Sydney, December 2009.

Risk-Based Approaches to Combating Financial Crime

By Dr David Chaikin*
University of Sydney

Abstract

The traditional method of combating financial crimes such as money laundering is the use of prescriptive legislation. A new idea is that risk concepts may be applied to understanding the phenomenon of money laundering and in devising strategies to minimise money laundering. In Australia financial institutions have implemented a Risk-Based Approach to money laundering by devising Anti-Money Laundering/Counter-Terrorism Financing programs. Financial institutions are expected to identify the risks of money laundering arising from their customers, products/services, distribution/delivery systems and the countries/ jurisdictions in which they operate or do business. They are also required to analyse the risks in relation to their specific circumstances and apply a risk management strategy to reduce those risks. The challenge is that Risk-Based Approaches can only minimise the potential risks of money laundering at best; they cannot provide any guarantee that money launderers will not use the product or services of a financial institution. The money laundering risk remains even in circumstances where a financial institution complies with the regulatory requirements and applies best practice in risk management. Nevertheless, the Risk-Based Approach offers financial institutions the most efficient method of setting priorities and allocating resources to combat money laundering.

Keywords: Money laundering, Risk management, Compliance, Financial institutions

Introduction

It is well accepted that governments in democracies have a limited ability to combat financial crimes, given the difficulty in detecting such crimes, the lack of resources of investigatory agencies, and the obstacles in using the legal system to criminally prosecute or recover illicit monies. In the case of money laundering, there has been a massive change in government expectations regarding the responsibilities of financial institutions in dealing with this problem.

Since 9/11 the United States has initiated an aggressive 'war on terrorism' which has resulted in a wide range of legislative measures (such as the Patriot Act), new government institutions and enforcement actions. This has created new risks for any financial institution not embracing comprehensive Anti-Money Laundering and Counter-Financing of Terrorism (AMLCTF) strategies. Financial institutions are not only required to have robust compliance systems, but are also expected to be active participants in the 'war on terrorism and money laundering'. There is an increased risk that management will be held responsible for a money laundering incident or a money laundering compliance failure. In Australia, the A*nti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (*AML/CTF Act*) provides a comprehensive set of prescriptive rules to combat financial crime. At the same time, the legislation places emphasis on the role of the private sector in using Risk-Based Approaches (RBAs) to minimise their potential use by financial criminals. There is a continuing tension between the relative importance of prescriptive legislation and risk-based guidance.

In the first part of this paper, the concept and rationale of money laundering is explained from the perspective of financial criminals. The sequential three-stage process of money laundering, namely placement, layering and integration, is outlined. It is shown that money launderers exploit the financial system to hide their illicit gains from law enforcement and tax authorities. The international response to the money laundering problem has been developed over the past 20 years, with a common set of international standards accepted by more than 180 jurisdictions. The second part of the paper points out that the idea of risk concepts being applied to money laundering and anti-money laundering strategies is relatively new. It examines how the risk-based approach (RBA) applies to anti-money laundering laws, particularly in relation to the risks of not knowing your customer, inadequate monitoring mechanisms; failing to report suspicious transactions, and the criminal risk of becoming involved in a money laundering transaction. The third part details how managerial responsibilities in combating money laundering have been expanded from the Board level and senior management to junior employees. The final part examines the effectiveness of AML risk strategies in achieving AML objectives.

Money Laundering — Purposes and Responses

Money laundering is the process by which one conceals or disguises the true nature, source, disposition, movement or ownership of money. Money laundering usually occurs after a 'predicate offence' has brought money into the hands of criminals. Predicate offences such as robbing a bank, selling heroin or accepting a bribe are motivated by the criminals' desire for profit. But 'receipt of the illicit funds may leave the offenders with the problem of reintegrating large sums of money into the legitimate financial system without arousing the suspicions of law enforcement authorities' (Chaikin and Sharman 2009a, 29).

The purpose of money laundering is to create the appearance that illicit money or property has a legitimate

source, thereby preventing its seizure and confiscation, and to avoid detection by law enforcement agencies, thereby reducing the likelihood of prosecution for the predicate (or underlying) offence). Money laundering provides both the motive for many crimes, but also the means, in terms of working capital. Money laundering is used to break the paper trail by, for example, using cash or transferring funds overseas to a tax haven or bank secrecy haven. Laundering creates obstacles to government investigators, tax prosecutors and private detectives. If money cannot be traced, then prosecutions may be blocked, confiscation of assets may be avoided and debts may not be recovered (Chaikin and Sharman, 2009b, 10).

There are generally three sequential stages in the money laundering process. First, placement involves the physical disposal of proceeds of criminal activity, for example, the deposit of drug money into a bank account or the conversion of stolen cash into a property investment. The second stage is layering, which involves the separating of illicit funds from their source through transactions that disguise the audit trail and provide anonymity. Layering entails more complex concealment measures to disguise the illicit funds — for example, through the use of multiple electronic funds transfers through banks accounts in numerous countries or the transfer of funds through a series of corporate accounts where the beneficial ownership is hidden through trusts or shell corporations. The ultimate money laundering step is integration, in which the illicit funds are absorbed into the legitimate financial economy as normal funds, so that they may be 'used for investment, saving or expenditure without arousing any suspicion from government agencies' (AUSTRAC, 2008). For example, repatriation of monies from overseas jurisdictions through foreign credit or debit cards (a technique detected by Operation Wickenby in a major Australian offshore tax scam), phony foreign inheritances, or concealed foreign investments, are examples of the integration stage of the money laundering process.

The three-stage money laundering process is based on a drug trafficking, money laundering model. However, there are many money laundering transactions that do not adhere to the same pattern. One of the reasons for this is that the legal definition of money laundering may include money that is of legal origin, for example, monies earned in legitimate businesses hidden from the tax authorities. In countries such as Australia and the United States, tax evasion is a predicate offence for money laundering, so that there is the possibility that a tax offence may be conflated into a money laundering offence (Chaikin, 2009c). Also, a different money laundering process may be used in cases of terrorist financing, such as when monies from legal charities are used to support terrorist organisations or operations.

Anti-Money Laundering Responses

International standards of money laundering have developed since 1989 under the auspice of the Financial Action Task Force (FATF), which is a powerful inter-governmental policy body established under the auspice of G8. The FATF consists of 35 member countries, such as the United States, the United Kingdom and Australia. It has published a series of Recommendations on Anti-Money Laundering (AML) and Combating Terrorist Financing (CTF). The FATF standards have attained such authority that countries which do not adhere to them have been subject to a form of blacklisting or financial sanctions. More than 180 countries have agreed to implement the FATF standards. The FATF's international standards have been implemented by Australia through various legislation, including the Anti-Money Laundering and Terrorist Financing Act 2006 (Cth), the Proceeds of Crime Act 2002 (Cth), the Suppression of the Financing of Terrorism Act 2002 (Cth) and the Criminal Code Act 1995 (Cth). The AML regime contains various elements such as:

- Criminalisation of money laundering conduct and the financing of terrorism, as well as freezing and confiscation of the proceeds of crime;
- Know your customer (KYC) rules and procedures to prevent criminals or terrorists becoming customers of or dealing with private sector regulated entities;
- Monitoring procedures to detect unusual or suspicious transactions;
- Reporting by the private sector of transactions of suspicious matters, as well as other financial reports, such as significant cash reports and international funds transfer reports, and
- Analysis by government agencies of reports filed by regulated entities, and the dissemination of the analysed product to local law enforcement and regulatory agencies, as well as to foreign agencies.

Applying Risk Concepts to Money Laundering and Anti-Money Laundering

The idea that risk concepts may be applied to money laundering and anti-money laundering strategies is relatively new. It is largely a by-product of the increased focus in the 1990s by regulators and management on operational risk, initially because of the complexity of internal systems leading to increased vulnerability and also the 'impact of deregulation and market volatility leading to increased risk-taking' (Raff, 2000, 12). The Basel Committee defined operational risk as 'the risk of loss resulting from inadequate or failed internal processes, people, or systems, or from external events' (Basel Committee, 2003). Whereas the Basel Committee considered that legal and compliance risks are a type of operational risk, it classified reputation risk and strategic risk as falling outside the concept of operational risk. The definitions of operational risk are 'fuzzy' because 'it is hard to make a clear-cut distinction between operational risk and the normal uncertainty that is faced in daily operations. By its nature, major operational risk occurs infrequently and is a discrete event(s). As a result, to measure the level of operational risk is equally hard as well as to define the operational risk' (Munn, 2003, 7, FSA, 2003).

Compliance risks have increased in the financial services industry because of new anti-terrorism financing laws, a global crackdown on money laundering, more stringent standards of corporate behaviour, corporate failure and fraud, and conflicts of interest scandals. The risks that may arise from compliance failure in the context of money laundering and terrorist financing include the risk of criminal prosecution (in effect, a 'corporate death sentence'), the risk of losing a license or being subject to a remedial direction by a regulator, the risk of a civil fine or pecuniary penalty order for breach of a regulatory requirement, and the risk of civil liability to third parties, such as under the doctrine of constructive trusts (Lester, 2010).

The application of risk concepts to money laundering involves a number of complex tasks carried out

by government policy makers, law enforcement agencies and private sector organisations and individuals. There is an initial difficulty in that 'there are currently no standard definitions used internationally within the AML/CFT context for the terms 'risk', 'threat' and 'vulnerability' (FATF, 2008, 2), nor is there any 'universally agreed and accepted methodology which prescribes the nature and extent of a risk-based approach' (Wolfsberg, 2008, 1). This is part of a larger policy challenge that there are competing international definitions, theories and models of risk and risk management, albeit national regulators have developed national standards on risk: see, for example, the joint Australian /New Zealand Risk Management Standard 4360: 2004. The most current risk management literature emphasises that risk should be considered not merely from a hazard or defensive perspective but also from an opportunity or positive perspective (Sharon, 2010, 1; Hillson, 2007, 6).

The government's role in the risk management process is to 'understand the sources and methods of money laundering and terrorist financing in its jurisdiction' so that it can develop and implement an effective anti-money laundering/counter-terrorist financing (AML/CFT) program. A national money laundering/terrorist financing (ML/TF) risk assessment should be considered the foundation for setting AML/CFT policy priorities and resource allocation (FATF, 2008, 2). A number of countries, such as Australia, Canada, Japan, United Kingdom and the United States have already conducted a national ML/TF risk assessment. Some agencies such as Australian Transaction Reports and Analysis Centre (AUSTRAC) have developed new software tools to assist it in its risk-based supervision of regulated entities. For example, the Compliance Risk Exposure Scoring Tool, known as CREST, allows AUSTRAC to prioritise its supervisory resources on entities with higher money laundering or terrorist financing risks.

The major challenge for national risk assessments is determining the size of money laundering in the local and national jurisdiction and the specific vulnerabilities of its financial and industrial sectors. There is the added complexity of how national money laundering inter-relates with international money laundering. Further, there is the challenge of working out the size of the illicit economy and the scale of money laundering (Unger, 2007, 6–10). One of the most commonly-quoted statistics is the IMF estimate that money laundering represents 2 per cent to 5 per cent of the world's GDP, that is, between $1.3 trillion to $3.2 trillion in 2009 figures. This estimate is imprecise because it is based on a series of national estimates, such as the amount of crime committed, the amount of profits made from crime and the amount of profits laundered. It is not merely the size of money laundering that is of interest to policy makers, but also its potential to destabilise governments, especially in poor, corrupt and undeveloped countries, and to undermine confidence in developed financial markets. There is also the destructive effect of money laundering on national tax bases, especially in the context of globalisation and the internet, and its corrupting influence on public institutions and law enforcement.

In June 2007, the FATF produced an important report, Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing (RBA paper) which has influenced national approaches to these problems. The RBA paper was generated as a result of a partnership between government agencies such as the UK Financial Services Authority and private sector representatives from the banking and corporate securities sectors. The RBA paper detailed a 'risk management process for dealing with money laundering and terrorist financing' that encompasses i) recognising the existence of risks; ii) undertaking an assessment of the risk(s); and iii) developing strategies to manage and mitigate the identified risks.

The FATF has issued guidance on the risk-based approach to a range of industries and professions, including:

Life Insurance Sector (October 2009);
Money Service Businesses (July 2009);
Legal Professionals (October 2008);
Casinos (October 2008);
Real Estate Agents (August 2008);
Accountants (August 2008);
Trust and Company Service Providers (August 2008); and
Dealers in Precious Metals and Dealers in Precious Stones (July 2008).

In examining how the RBA applies to anti-money laundering laws, several topics may be discussed. In the case of the provision of financial services, such as banking and asset management, there are significant compliance risks. These risks include the risks of not knowing your customer, inadequate monitoring mechanisms, failing to report suspicious transactions and the criminal risk of becoming involved in a money laundering transaction.

Know Your Customer (KYC)/Customer Due Diligence (CDD)

One of the pillars of the anti money laundering regime is the concept of 'Knowing Your Customer' (KYC) which is related to the idea of 'Customer Due Diligence' (CDD).

KYC has a long history in securities and investment regulation, originating in the early 1960s in rules developed by self regulatory organisations, such as New York Stock Exchange Rule 405. For example, a stock broker which is recommending an investment to an unsophisticated client is required to assess the suitability of that investment for that customer. In making a judgment, the broker is required to obtain facts from the customer concerning his/her investment objectives or goals, risk preferences, financial position, income and assets. The reason for requiring brokers to know their clients is that brokers should only recommend investments suitable to the needs of their retail clients and that it is in the financial interests of brokers to know their customer for credit risk purposes (IOSCO 2004).

With the introduction of anti-money laundering laws, the KYC requirement has acquired a broader significance. KYC is essential so that a financial institution does not unwittingly or unknowingly assist in the laundering of illicit funds or the financing of terrorism. A financial institution must know one's customer to minimise the risk of criminal, civil or regulatory liability for money laundering, and avoid any reputation risk that may arise from a money laundering scandal. As the Basel Committee has pointed out: 'Without (adequate) due diligence, banks can become subject to reputational, operational, legal and concentration risks, which can result in significant financial cost' (Basel, 2001).

According to the FATF, financial institutions are expected to take the following due diligence measures to ensure that they know their customers:

- Identify and verify the identity of each customer on

a timely basis;
- Take reasonable risk-based measures to identify and verify the identity of any beneficial owner; and
- Obtain appropriate additional information to understand the customer's circumstances and business, including the expected nature and level of transactions

(FATF 2007, 27).

There is a requirement that all customers will be classified according to their AML/CTF risk, with additional Customer Due Diligence (CDD) measures applied to higher risk customers, such as Politically Exposed Persons (PEPs) or Senior Public Figures, Higher Net Worth Individuals, and Correspondent Banking Relationships. The application of the Risk-Based Approach to customer risk in the context of money laundering has been problematical. The theory is that by introducing CDD procedures, which includes knowing one's customer, there are reduced risks of attracting criminal clients and their illicit monies. The reliability of the identification system is based on three generous assumptions. First, in countries such as the United States and Australia, the identification requirements are based on Western naming systems which are inadequate for the purpose of identifying persons from ethnic groups which have a different naming system. Second, there is an assumption that it is difficult to forge identity documents and that this can be detected by bank officers. This assumption sits uncomfortably with the extensive problem of forged identification in the Asia/Pacific region. Third, there is an element of self-voluntarism in that customers are required to disclose all the names that they commonly use or names in which they have opened bank accounts at other financial institutions. Further, there has been a marked failure by many countries to impose legislative requirements for disclosure of beneficial ownership and control of corporate entities. This lacunae undermines not only AML/CTF systems but the processes of regulation generally (US Senate, 2008).

Monitoring of Customers and Transactions

Implementing reasonable CDD processes and procedures in respect of new and existing customers is only the first step in creating an effective AML system. Financial institutions are also required to monitor customers and transactions as part of an ongoing customer and transaction management. As the FATF has observed: 'The degree and nature of monitoring … will depend on the size of the financial institution, the AML/CTF risks that the institution has, the monitoring method being used (manual, automated or some combination) and the types of activities under scrutiny' (FATF, 2007, 26).

Under the RBA approach, not all customers, accounts or transactions will be subject to the same level of monitoring. The financial institution's knowledge of the customer is an important consideration in determining the level and type of monitoring. The monitoring of transactions against a customer's profile, the monitoring of account activity to determine whether a customer's risk profile should be reclassified to a higher level, and the monitoring of incoming and outgoing transactions against a customer's profile are important AML measures. Thus, as a vital prerequisite, in the case of higher risk customers, financial institutions must acquire knowledge of the provenance of the source of funds (for example, bank loans or customer's own funds), knowledge of the nature of proposed transactions, and knowledge of 'red signals' or warning signs in relation to a customer's accounts or transactions. The monitoring of accounts may lead to the decision to report a suspicious transaction which is discussed below.

Suspicious Matters Reports

The system of reporting suspicious matters to a governmental authority is a fundamental feature of AML regimes. For example, s 41 of the *AML/CTF Act* imposes a duty on reporting entities to give a report to the Chief Executive Officer of AUSTRAC where they suspect on reasonable grounds any of the following:

(a) the customer is not who he/she claims to be,
(b) information they have concerning the provision of

Potential Cases of Suspicion

Identity of client and/or underlying beneficiary	False address; forged identity documents; refusal to provide identification information or documents; different ID documents for different transactions; doubts about the real beneficiary of the account.
Suspicious background	Positive match of person's name and date of birth with person on UN or national watch list; accounts of persons identified as known criminals or associates of criminals.
Cash transactions	Cash deposits are packaged in an unusual way by the customer; cash deposits just under threshold ($10,000) so as to avoid reporting requirement; unusually large cash deposits by a client with personal or business links to an area associated with drug trafficking.
Multiple accounts	Large number of accounts having a common account holder, introducer or authorised signatory with no rational or bona fide purpose; inexplicable transfers between accounts with no rational purpose.
Transactions involving accounts	Deposit of monies into several accounts which are consolidated into one and transferred to another country; inexplicable reactivation of a dormant account with deposits followed by frequent cash withdrawals; inexplicable transfers between the client's accounts.
Nature and value of transactions	Frequent purchase of traveller's cheques when this is outside normal customer's activities; multiple cash deposits into an account at multiple locations by third parties; inexplicable large value transactions which are not consistent with customer's financial standing or business activities.
Transactions involving foreign countries	Frequent use of a credit card issued by a foreign bank that does not operate in Australia by a customer that does not live and work in the country of issue; inexplicable accumulation of large deposit balances and subsequent transfers to overseas jurisdictions; deposits followed shortly by international funds transfers to or through jurisdictions that require enhanced due diligence, for example, FATF-listed countries, money laundering havens or tax havens.
Transactions related to offshore business activities	Loans to or from offshore companies that have no public profile and may be shell companies or 'shell banks'; use of letter-of-credit to move money between countries when such trade is inconsistent with the client's business; inexplicable large international funds transfers into account from an offshore account owned by the customer.

the designated service
- i) may be relevant to the investigation of a person for tax evasion or attempted tax evasion,
- ii) may be relevant to the investigation or prosecution of a person for an offence against the Commonwealth, State or Territory laws,
- iii) may assist the enforcement of a Commonwealth, State or Territory proceeds of crime law,
- iv) may be relevant to the investigation or prosecution of a money laundering or terrorism-financing offence, or

(c) the provision of the designated service is preparatory to the commission of a money-laundering or terrorism-financing offence.

The suspicious matter reporting obligation arises regardless of the amount of money involved, the nature and seriousness of the criminal offence, or whether the reporting entity accepts the business or transactions of the actual/potential customer. The reporting obligation is not subject to any risk threshold. In order to assist reporting entities to comply with their suspicious matter reporting obligation, AUSTRAC has issued various publications, including the AUSTRAC Regulatory Guide, and Public Legal Interpretation No 6 of 2008 concerning suspect transactions and suspicious matter reports.

A suspicious transaction will be one where it is inconsistent with the known legitimate business or personal activities of the customer, or where there is a series of transactions that are unusual or large compared with the history of the account and which have no apparent genuine financial or lawful purpose. The potential cases of suspicion are illustrated in the table below which has been adapted from reports by Financial Intelligence Units from Australia, Canada and India.

The potential cases of suspicion set out above are based largely on past cases which government agencies have summarised, anonymised and published on their websites. Indeed, the determination of the meaning of the term 'suspicion' has been heavily influenced by government agencies which in turn have relied on typologies produced by international expert groups, such as the FATF, the Asia/Pacific Group on Money Laundering and the Egmont Group. National financial intelligence agencies and AML regulators, such as AUSTRAC, have also produced typologies and case studies on money laundering and financial crimes, which are updated on the basis of new cases and perceived new risks. The purpose of the government-generated typologies is to facilitate regulated entities in the making of informed decisions concerning AML systems and processes, as well as in training employees. This is necessary because the private sector does not have sufficient knowledge about illicit activity. However, current typologies may have little predictive value except for unimaginative and unsophisticated criminals and terrorists. Further, since the 'red flags' of suspicious conduct are well-publicised, it is not too difficult for a reasonably astute money launderer to evade detection. Since the money laundering profession is one that is founded on deception, it is extremely difficult for financial institutions to close all possible avenues of money laundering. Indeed, since every instrument or facility provided by financial institutions may be potentially used for money laundering, there is virtually an unlimited range of possible vehicles for money laundering (Chaikin, 1992, 467).

The detection of potential suspicious matters or transactions is one of the most difficult compliance responsibilities of reporting entities. The legislative assumption is that reporting entities are in the best position to know their business, including their products, customers and distribution systems, and so are best placed to evaluate their vulnerabilities to crime and money laundering. The idea is that the private sector has the knowledge and means to evaluate facts and patterns of conduct which are unusual or indicative of illegality. It may seem odd that reporting entities, such as financial institutions, are required to apply behavioural theory and the policeman's proclivity for suspicion to their dealings with existing and prospective customers. However, the argument that financial institutions do not have the knowledge, experience or information systems to identify suspicious transactions has been rejected by all governments that have implemented suspicious-based reporting schemes. The fact is that reporting entities in Australia and elsewhere have increased the number of suspicious matters/transactions reports in response to increased regulatory pressure and new AML laws.

There is a strong incentive for reporting entities to comply with the government's view of suspicion. For example, under s 235 of the *AML/CTF Act*, reporting entities are given protection against legal suits by customers whenever they comply with their obligation to report suspicious matters. A customer of a financial institution who is injured by a suspicious matters report cannot sue the financial institution for breach of contract or under tort law even if a court subsequently holds that there were no reasonable grounds of suspicion for filing the suspicious matters report.

Criminal Offence of Money Laundering

A major risk for reporting entities is that they may become embroiled in an actual money laundering criminal case because their services or products are exploited by criminals. The federal criminal offences of money laundering in Australia are found in Part 10.2, Division 400 of the Criminal Code Act 1995 (Cth), as well as in a range of state legislation. In a criminal case, the prosecution must prove beyond reasonable doubt that a crime actually happened (physical acts or omissions) and that the accused intended the crime to happen (mental element or state of mind). Sections 400.3-400.8 of the Criminal Code sets out 18 offences. The more serious offences are defined according to the mens reaof the accused. For example, intentional money laundering is where the accused believes the money or property is proceeds of crime or intends that money or property will become an instrument of crime, reckless money laundering is where the accused is reckless of this fact, while negligent money laundering is where the accused is negligent of this fact.

In many money laundering cases, the success of the prosecution will depend on whether the mental element of the offence is proved by circumstantial evidence. There is usually little dispute about whether the conduct constituting the offence occurred, because the offences are extremely wide, encompassing normal financial transactions and business deals carried out by banks, commercial entities and professional advisers. The acceptance of a deposit, the making of a loan, and the receipt of money in a property or business transaction are examples of conduct which may constitute the actus reus of money laundering. Under the Criminal Code, it is sufficient if the accused deals with money or property which is the proceeds of crime. 'Deals with money or other property' is

defined as where a person receives, possesses, conceals or disposes of money or other property, imports or exports money or other property, or engages in a banking transaction, and the money or other property is proceeds of crime. 'Money or other property' includes financial instruments, cards and other objects which represent money or can be exchanged for money, whether or not they have intrinsic value. 'Proceeds of crime' is defined as any money or property derived from an offence attracting a prison sentence of 12 months or more.

Section 400.9 creates a distinct offence of receiving, possessing, concealing, disposing or importing/ exporting any money or other property that it is reasonable to suspect that the money or property is proceeds of crime in relation to an indictable offence. Reasonable suspicion is deemed to exist where conduct involves structured transactions to avoid the reporting requirements, or where the account is held with a bank under a false name. It is a defence if the accused proves that he/she had no reasonable grounds for suspecting that the money or property was derived or realised, directly or indirectly, from some form of unlawful activity: s 400.9.5)

Managerial Responsibilities and Anti-Money Laundering

Under Australian law, all organisations which provide designated services are prohibited from supplying such services until they have developed and implemented an appropriate AML/CTF program. A reporting entity's AML/CTF program is one that identifies, mitigates and manages the risks of its products or services that may facilitate money laundering or terrorist financing. The main requirements of the programs are set out in the Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No 1). In developing a program, a reporting entity should also apply AUSTRAC's Guidance Note Risk Management and AML/CTF programs, and consider all relevant risks, including customer risk, product/service risk, delivery risk, and jurisdiction/country risk.

AUSTRAC considers that AML/CTF programs are a fundamental element of the risk-based approach:

> AML/CTF programs are risk based. This means reporting entities can develop their own programs with minimal cost, tailored to their situation and money laundering and terrorism financing risks. This approach recognises that the reporting entity is in the best position to assess the risk of their customers, products and services and to allocate resources to counter those risks. The risk-based approach also ensures there is minimum impact on customers (AUSTRAC, 2009).

Reporting entities that implement the risk-based approach 'must take into account the nature, size and complexity of the business and the risk that business might reasonably face of money laundering and terrorism financing. The program must also be applicable to all areas of a business which provide designated services' (Jensen, 2008).

A key employee in developing and implementing the AML/CTF regime, especially the AML/CTF program, is the AML/CTF compliance officer (AMLCO). The AMLCO's responsibilities include the development of AML/CTF processes and procedures, as well as monitoring enterprise-wide AML/CTF performance. The AMLCO must have 'appropriate seniority' in the management structure, 'appropriate reporting lines' and 'access to the executive and Board of the reporting entity' (AUSTRAC, 2007). The AMLCO must provide not only appropriate reports to senior management and the Board, but also an awareness within the firm of AML/CTF policies, processes, issues and techniques. It is the AML/CTF office who assumes day-to-day responsibility for compliance decisions, which are often complex and difficult especially since hitherto there has been little organisational or individual experience in dealing with AML/CTF risks.

The Board has the overall responsibility of 'considering and approving AML/CTF Policy', any proposed amendments, and receiving and reviewing reports on the implementation of AML/CTF Policy. In the case of larger financial services organisations, it is best practice for one of the committees of the Board, such as the Business Risk/Audit and Compliance Committee to oversee the AML/CTF Program and report to the Board. For example, the Business Risk Committee may review the AML/CTF Policy, as well as AML/CTF reports received from management, 'monitor the organisation's AML/CTF performance and compliance with the AML/CTF Policy', and review breaches of the AML/CTF Policy and remedial actions taken. The Business Risk Committee would then make appropriate recommendations to the Board.

In major financial services companies, the managing director would also have AML/CTF responsibilities such as 'managing the AML/CTF regime across the entire business', assigning responsibilities to ensure 'effective management of the identified risks', ensuring that all parts of the business, including all lines of business, implement AML/CTF, and promoting an AML/CTF culture so that it becomes 'embedded throughout the organisation' (MSL 2009). Senior managers in large organisations would 'ensure that the requirements of AML/CTF Policy are incorporated into Divisional processes', 'be accountable for delivering the outcome of AML/CTF processes and procedures in their particular area of responsibility' and 'support the AML/CTF Compliance Officer in the execution of the responsibilities of that position' (MSL 2009). The managing director and senior management must ensure that there is a system so that employees are aware that they are individually responsible for complying with the firm's AML/CTF program and the *AML/CTF Act*. Not only must employees be aware of their responsibilities but they must be given appropriate training on an ongoing basis. This is a significant compliance responsibility because of the frequent turnover of staff in financial institutions.

Effectiveness of AML Risk Strategies

Although Australia enacted one of the world's first AML laws in 1988 and has become a leader in encouraging the spread of global AML standards, in October 2005, the FATF criticised Australia's lack of criminal prosecutions for money laundering (FATF 2005, 6). As a direct result, in December 2006, the Australian Parliament passed the Anti-Money Laundering and Counter-Terrorism Financing Act to ensure that Australia complied with FATF standards and to improve the detection and prevention of money laundering. Other legislative and administrative measures have been implemented so as to improve Australia's compliance with international AML/CTF standards.

The original aim of Australia's AML regime was to disrupt illicit finance by making predicate offences less

profitable, and thus less attractive, as well as reducing the availability of working capital to criminals . By countering money laundering as an offence distinct from the underlying crime it was hoped that the number of predicate offences would fall. However, there is little empirical evidence to show that AML strategies have had any significant impact on the underlying predicate crimes, a problem exacerbated by the lack of performance criteria in assessing AML systems (Chaikin 2009d, 239). This does not mean that the AML strategies do not serve any useful purpose. Indeed, AML laws are often the only mechanism to prosecute the higher echelons of organised crime, who insulate themselves from the underlying crime. Further, one of the central purposes of the *AML/CTF Act* is to 'minimise the potential that designated services may be useful for money laundering or terrorism financing purposes' (AUSTRAC 2007, 3).

Perhaps the greatest impact of intelligence produced by the AML process is on tax enforcement in Australia. This may be explained by the huge volume of reports produced by the AML process, which includes reporting of suspected tax offences. For example, in 2008–2009, AUSTRAC received '19,771,903 transaction reports from regulated entities, equating to an average of 76,000 reports per business day (a 10.15 per cent increase on the total number received in 2007–08)' (AUSTRAC 2009, 3). This is a massive intelligence base which has been exploited by the Australian Taxation Office (ATO) in its investigations and recovery of tax monies (Jensen 2009, 51–55). The ATO has used the data collected by AUSTRAC to 'monitor money movements into and out of Australia, profile individuals, industries, occupations and geographical areas, identify potential high-risk transactions, identify and quantify compliance risks and develop compliance strategies, and assist in the selection of compliance cases for further investigation' (Auditor General, 2004).

Conclusions

This paper has sought to examine how Risk-Based Approaches (RBA) have been applied in the context of financial crimes, particularly money laundering. Financial institutions are expected to identify the risks of money laundering arising from their customers, products/services, distribution/delivery systems and the countries/ jurisdictions in which they operate or do business. They are also required to analyse the risks in relation to their specific circumstances and apply a risk management strategy to reduce those risks. The challenge in applying RBAs is that such approaches can only minimise the potential risks of money laundering at best; they cannot provide any guarantee that money launderers will not use the product or services of a regulated entity. The money laundering risk remains even in circumstances where a financial institution complies with the regulatory requirements and applies best practice in risk management. Nevertheless, the RBA offers regulated entities the most efficient method of setting priorities and allocating resources to combat financial crimes, including money laundering.

References

Auditor-General, *The Australian Taxation Office's Use of AUSTRAC Data Follow-up Audit*, Audit Report No 18 (2004).

AUSTRAC, *Introduction to Money Laundering* (2008).

AUSTRAC, *Guidance Note: Risk Management and AML/CTF Programs* (2007) http://www.austrac.gov.au/files/risk_man_and_amlctf_programs.pdf .

Basel Committee, *Customer Due Diligence for Banks* (October 2001).

Basel Committee, *The New Basel Capital Accord* (April 2003)

David Chaikin, 'Money Laundering: An Investigatory Perspective' (1992) 2 *Criminal Law Forum* 467–510.

David Chaikin and J C Sharman, 'Corruption and Anti-Money Laundering Systems: Putting a Luxury Good to Work' (2009) 22 (1) *Governance: An International Journal of Policy, Administration, and Institutions* 27–45 (2009a).

David Chaikin and J C Sharman, *Corruption and Money Laundering: A Symbiotic Relationship* (Palgrave Macmillan, New York, 2009) (2009b).

David Chaikin (ed), *Money Laundering, Tax Evasion & Tax Havens* (Australian Scholarly Publishing, Melbourne, 2009) (2009c).

David Chaikin, 'How Effective are Suspicious Transaction Reporting Systems?' (2009) 12 (3) *Journal of Money Laundering Control* 238–253 (2009d).

Financial Action Task Force, *Third Mutual Evaluation Report on Anti-Money Laundering and Combating the Financing of Terrorism: Australia* (October 2005).

Financial Action Task Force, *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing* (2007).

Financial Action Task Force, *Money Laundering and Terrorist Financing: Risk Assessment Strategies* (June 2008).

Financial Services Authority United Kingdom, *Building a Framework for Operational Risk Management: the FSA's Observations* (July 2003) <http://www.fsa.gov.uk/Pages/Library/Policy/Policy/2003/PS142_2.shtml>.

David Hillson and Ruth Murray, *Understanding and Managing Risk Attitude* (2nd ed, Gower, 2007).

International Organisation of Securities Commissions (IOSCO),
Principles on Client Identification and Beneficial Ownership for the Securities Industry (May 2004).

Neil Jensen, 'Creating an Environment in Australia Hostile to Money Laundering and Terrorism Financing: A Changing Role for AUSTRAC' (2008) 5 *Macquarie Journal of Business Law* 93.

Zoe Lester, *Anti-Money Laundering: A Risk Perspective* (PhD

Thesis, University of Sydney, 2010).

CC Mun, 'New Proposal for Operational Risk Measurement of Small/Medium Size Banks'(Research Paper, FSS Financial Forum, Seoul, 2003).

Mystate Limited, *Anti-Money Laundering/Counter-Terrorism Financing Policy* (February 2009).

Daniel MG Raff, *Risk Management in an Age of Change* (The Wharton School, Philadelphia, 30 June 2000).

Bill Sharon, *Risk Management: Beyond Compliance*, QFinance.com

Brigitte Unger, *The Scale and Impacts of Money Laundering* (2007).

US Senate Committee on Homeland Security and Governmental Affairs, *Levin-Coleman-Obama Bill Introduced to Stop Misuse of US Companies* (May 1, 2008).

* Author Contact Details
Dr David Chaikin
Senior Lecturer
Discipline of Business Law
Faculty of Economics and Business
University of Sydney, Australia.
E: david.chaikin@sydney.edu.au
T: 61 2 9036 7132

The Risk-Based Approach offers financial institutions the most efficient method of setting priorities and allocating resources to combat money laundering.