Anti-money laundering and counter-terrorism financing across the globe: A comparative study of regulatory action

Julie Walters, Carolyn Budd, Russell G Smith, Kim-Kwang Raymond Choo, Rob McCusker and David Rees

AIC Reports
Research and
Public Policy Series
113

www.aic.gov.au

ISSN 1836-2060 (Print)
1836-2079 (Online)
ISBN 978 1 921532 81 8 (Print)
978 1 921532 82 5 (Online)

Project no. 0140

Published by the Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601
Tel: (02) 6260 9200
Fax: (02) 6260 9299
Email: front.desk@aic.gov.au
Website: http://www.aic.gov.au

Please note: minor revisions are occasionally made to publications after release. The online versions available on the AIC website will always include any revisions.

Disclaimer: This research report does not necessarily reflect the policy position of the Australian Government.

Edited and typeset by the Australian Institute of Criminology

A full list of publications in the AIC Reports series can be found on the Australian Institute of Criminology website at **http://www.aic.gov.au**

Foreword

Most developed countries across the globe have enacted legislation to proscribe acts of money laundering and financing of terrorism, and to enable the proceeds of crime to be recovered from offenders. Such legislation reflects the principles developed by the Financial Action Task Force's (FATF-GAFI) 40 plus Nine Recommendations to combat money laundering and the financing of terrorism (FATF-GAFI 2004) to varying degrees. FATF-GAFI was established in 1989 as an international body to examine techniques employed by criminals to launder the proceeds of crime and the approaches taken internationally to counteract such activities, as well as to identify policies to impede money laundering and the financing of terrorism. FATF-GAFI issued 40 Recommendations to combat money laundering in 1990 and expanded these to deal with the problem of financing of terrorism after the 11 September 2001 attacks by adding a further Nine Special Recommendations on terrorism financing.

Despite the normative approach taken in the FATF-GAFI Recommendations, the specific legislative and procedural responses taken by individual countries have differed in many respects. Documenting these differences and comparing key aspects of the regimes in different countries is of considerable value to regulators and analysts for several reasons.

Law enforcement and prosecutorial agencies need to understand the differences that exist in criminal laws relating to money laundering between different countries when investigating and prosecuting illegal conduct, as conduct of this nature often entails cross-border activity requiring mutual assistance between agencies and extradition of suspects across jurisdictional borders.

Understanding the approaches taken by different countries to enhancing compliance with legislation and with soft regulatory measures can help policymakers develop best-practice mechanisms for increasing compliance with regulatory controls. Improved compliance has the potential to increase the quality of the financial intelligence gathered and the potential utility of regulatory regimes internationally.

Comparative research on the implementation of AML/CTF systems may illustrate the potential advantages of, and problems with, proposed changes to the regimes, such as extending the requirements to designated non-financial businesses and professions. Some countries have far greater experience with these approaches than others and it is important to make use of constructive lessons that have been learned.

The present research sought to compare the legal framework and compliance, and enforcement outcomes of the AML/CTF regimes across countries with disparate legal traditions. The countries included in the scope of the project were from the European Union (the United Kingdom, France, Germany and Belgium), Asia (the Republic of China (Taiwan), Hong Kong and Singapore), the United States and Australia. Within each of the selected countries, the structure of the criminal provisions proscribing money laundering and the financing of terrorism were reviewed and the judicial interpretation of these laws compared. Information is also presented on the number of businesses regulated within each country's AML/CTF system and the extent to which businesses outside the formal financial sector are regulated. The approach taken to financial intelligence reporting is also compared with the evidence presented on the nature and extent to which financial reports are required and undertaken in the selected countries as well as the circumstances

triggering reports. The extent to which entities comply with each country's AML/CTF regime is also considered and a number of quasi-indicators of compliance are presented, as well as the actions taken by regulators for non-compliance and the extent to which regulators and others have adopted non-punitive strategies to encourage or enhance compliance with the regimes.

One of the principal findings concerns the vast differences that exist between countries in the designation of crimes considered to be predicate offences for money laundering—that is, the types of serious crimes that can generate funds for laundering. These differences can have important implications where cross-border prosecutions are undertaken, as there may not be a corresponding degree to which conduct is proscribed in different countries, thus creating barriers to mutual legal assistance and extradition of suspects.

Another clear finding related to the extensive differences that exist between the countries examined is the extent to which specific regulated entities comply with their reporting obligations. Australia, for example, requires businesses to lodge a report in respect of all attempted transactions that raise suspicions of illegality, while Belgium requires businesses to undertake a degree of preliminary analysis of transactions prior to submitting a report to authorities. Belgium, France and Germany further limit the circumstances that trigger a reporting obligation to those associated with a list of specific crimes. The German system, for example, limits those crimes to either money laundering or the financing of terrorism. Other countries consider all serious crimes as potential predicate offences for money laundering reporting purposes.

As might be expected, the volume of reports of suspicious financial activity submitted by regulated entities each year has increased considerably, with entities both in Australia and the United States increasing the number of reports made to regulators by more than 300 percent between 2002–03 and 2008–09. Such increases are due to the increasing publicity of reporting obligations by regulators, increasing numbers of entities being subject to reporting obligations and potentially an increase in underlying criminality. Further research is required to understand the precise reasons behind the increase in reporting in the countries examined.

Interestingly, designated non-financial businesses and professions demonstrated similar levels of reporting to regulators across the countries examined. None of the countries that have included legal practitioners, accountants, real estate agents, dealers of precious metals and stones, and trust and company service providers, in their AML/CTF regimes reported receiving volumes of reports from these businesses by comparison with those from financial services businesses. Financial services businesses (particularly banks), continue to contribute the bulk of financial intelligence through reports of suspicious financial activities due to the large number of transactions dealt with on a daily basis.

Despite certain similarities, and the shared basis in FATF-GAFI's Recommendations, the elements of international AML/CTF regimes differ sufficiently to make direct comparisons between countries difficult. Care is needed in making direct comparisons between countries owing to their different legislative requirements, different cultures of compliance and differing patterns of financial crime and terrorism. The Australian Institute of Criminology has published a separate report that examines these different factors in some depth and such differences need to be considered in making any direct comparisons between countries. Prosecution, enforcement and reporting data can reveal interesting trends regarding the development of the AML/CTF regime over time within a specific country, or the impact changes to the regime have had on these measures. Using such measures as evaluative criteria between different countries can, however, be misleading unless local circumstances are considered in detail.

Future comparative studies of this nature would benefit from multilingual research, access to data held by regulators and other government agencies rather than reliance on publicly available information alone and from qualitative information held by financial intelligence units, regulated businesses and AML/CTF regulators. The present study does, however, provide a preliminary indication of how a number of countries from different legal traditions and continents have approached the challenges raised by money laundering and financing of terrorism in the twenty-first century.

Adam Tomison
Director

Contents

Tables

Acknowledgements

This report is based on research undertaken by current and former staff within the Global, Economic and Electronic Crime Research Program at the Australian Institute of Criminology. The authors are grateful to the many individuals who agreed to participate in consultations with the authors both within Australia and overseas between 2008 and 2010, and to the agency staff and the external referee who provided helpful feedback on earlier drafts.

The information contained in this report was current at 1 April 2011.

Acronyms and abbreviations

ADIs	authorised deposit taking institutions
AIC	Australian Institute of Criminology
AML/CTF	anti-money laundering/counter-terrorism financing
AML/CTF Act	*Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)
Annunzio-Wylie Act	*Annunzio-Wylie Anti-Money Laundering Act 1992*
APG	Asia/Pacific Group on Money Laundering
ARS	alternative remittance services
AUSTRAC	Australian Transaction Reports and Analysis Centre
BaFIN	German Financial Supervisory Authority
BKA	Federal Office of Criminal Investigation (Bundeskriminalamt)
Bank Secrecy Act	*Bank Records and Foreign Transaction Reporting Act 1970*
CAD	Commercial Affairs Department
CBFA	Banking, Finance and Insurance Commission
CCA	Court of Criminal Appeal
CDPP	Commonwealth Director of Public Prosecutions
CDSA	*Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act* (Cap 65A)
Consent order	Consent to the Assessment of Civil Money Penalty Order
COSC	Central Office for Seizure and Confiscation
CoTUNA	*Charter of the United Nations Act 1945* (Cth)
Criminal Code	*Criminal Code Act 1995* (Cth)
CTIF-CFI	Cellule de Traitement des Informations Financieres
CTR	Currency Transaction Reports
DNFBPs	designated non-financial businesses and professions
DTROP	Drug Trafficking (Recovery of Proceeds) Ordinance
EEA	European Economic Area
FATF-GAFI	Financial Action Task Force (Le Groupe d'action financière)

FDIC	Federal Deposit Insurance Corporation
FinCEN	Financial Crimes Enforcement Network
FIU	financial intelligence unit
FTR Act	*Financial Transaction Reports Act 1988* (Cth)
FSA	Financial Services Authority
Germany Money Laundering Act	Act on the Detection of Proceeds from Serious Crimes
HKICPA	Hong Kong Institute of Certified Public Accountants
HMRC	Her Majesty's Revenue and Customs
IFTIs	international funds transfer instructions
IMF	International Monetary Fund
INCSR	International Narcotics Control Strategy Report
JFIUHK	Joint Financial Intelligence Unit Hong Kong
MAS	Monetary Authority of Singapore
MLCA Taiwan	*Money Laundering Control Act*
MLPC	Money Laundering Prevention Centre
LPP	Legal Professional Privilege
LTTE	Liberation Tigers of Tamil Eelam
MLRO	money laundering reporting officer
Money Laundering Control Act	*Money Laundering Control Act 1986*
MSBs	money service businesses
MJIB	Investigation Bureau, Ministry of Justice, Republic of China
NatWest	National Westminster Plc
NCIS	National Criminal Intelligence Service
NCS	National Crime Squad
NCUA	National Credit Union Administration
OCC	Office of the Comptroller of the Currency
OSCO	Organised and Serious Crimes Ordinance
PATRIOT Act	*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 2001*
POBO	Prevention of Bribery Ordinance
POCA 2002	*Proceeds of Crime Act 2002* (Cth)
POCA 1987	*Proceeds of Crime Act 1987* (Cth)

POCA 2002 UK	*Proceeds of Crime Act 2002*
SARs	Suspicious Activity Reports
SEF	Singapore Exchange and Finance Pty Limited
SMRs	suspicious matter reports
SOCA	Serious Organised Crime Agency
SOCPA	*Serious Organised Crime and Police Act 2005* (UK)
STRs	Suspicious Transaction Reports
STRO	Suspicious Transaction Reporting Office
Terrorism Act	*Terrorism Act 2000*
Third Money Laundering Directive	Directive 2005/60/EC of the European Parliament and the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing
TRACFIN	Traitement du renseignement et action contre les circuits financiers clandestins
TSOFA	*Terrorism (Suppression of Financing) Act*
UKIS	UK Immigration Service
UNATMO	United Nations (Anti-Terrorism) Ordinance
UKFIU	UK Financial Intelligence Unit

Executive summary

This report presents a review of the different approaches taken by nine countries, including Australia, to the adoption of anti-money laundering and counter-terrorism financing (AML/CTF). In response to mounting international concern about money laundering in the late 1980s, countries around the world established the Financial Action Task Force (FATF-GAFI) to set international standards and develop policies to combat money laundering and terrorist financing. In 1990, the FATF-GAFI issued a set of 40 Recommendations to guide the fight against money laundering and these were expanded following 2001 to include nine additional Recommendations to respond to the financing of terrorism.

The FATF-GAFI's 40 plus nine Recommendations to combat money laundering and the financing of terrorism (FATF-GAFI 2004) have three primary objectives—to support the criminalisation of money laundering and the financing of terrorism, to ensure that assets linked to money laundering or the financing of terrorism can be frozen and confiscated and to ensure that financial institutions and other regulated businesses comply with the recommendations.

This report reviews the state of international responses to the FATF-GAFI Recommendations in order to assess how countries have applied the requirements, which sectors have been subject to regulation and how compliance and enforcement are undertaken.

Nine countries were chosen for review—Australia, the United States, the United Kingdom, France, Germany, Belgium and in Asia, Singapore, Hong Kong and the Republic of China (Taiwan). These were chosen to provide an indication of how diverse nations in separate continents have approached AML/CTF implementation. They were also chosen to be indicative of the measures taken in countries with different legal traditions and different types of risk in terms of money laundering and financing of terrorism.

The majority of the information used in this report came from publicly available documents published by regulatory bodies, financial intelligence units, law enforcement and other government agencies, industry bodies and FATF-GAFI itself. The authors also undertook a number of consultations with stakeholders in the countries in question in order to supplement the publicly available written material.

Regulatory regime

The regulatory regime in each country was examined by reviewing its criminal and regulatory legislation including assert recovery provisions, the nature of each country's government regulator (or financial intelligence unit), the extent of the regulated sector and the nature of the obligations cast upon reporting entities including laws against disclosing the fact of reporting to the business in question (tipping-off) and the nature of compliance and enforcement activities.

Overall, AML/CTF regimes across the countries in question share a common basis in FATFs Recommendations and accordingly, they were remarkably similar in their responses to, and implementation of, the Recommendations. A key area of difference between the nine countries is the extent and size of the regulated sector in each country. This affects not only the scale of reporting undertaken, but also the capacity to regulate and enforce compliance for large numbers of regulated businesses in some countries.

All of the countries considered have made money laundering a criminal offence and one distinct from the crime that generated the funds in question. One of the key components of criminal money laundering offences that differs between each country is the consideration given to predicate offences, that is, the type of criminal conduct that generates funds which can then be laundered. Australia, the United States, Belgium, Germany, Hong Kong, Singapore and Taiwan all restrict money laundering predicate crimes to serious offences. Germany has included specific less serious offences as predicate offences, whereas Taiwan places a further restriction by adding a lower limit of NT$20m for the amount of funds in question. The definition of a serious, indictable, or felony offence differs between countries and is tied to minimum imprisonment periods in each country, generally a minimum period of 12 months imprisonment.

The real difference in the potential application of money laundering offences in these nine countries lies in the maximum prison sentences tied to potential predicate crimes. An offence can only become a predicate crime for a money laundering charge where the maximum sentence available for the predicate crime satisfies the conditions for money laundering in a specific jurisdiction. Illegal logging crimes, for example, do not carry the required sentences to meet the definition of a predicate offence for money laundering in Australia. The same offence in Indonesia, however, carries a maximum sentence that satisfies the severity condition of a money laundering charge in that jurisdiction.

Taiwan is the only country considered in this report that has not criminalised the financing of terrorism. Australia has criminalised financing individual terrorists, terrorist organisations and terrorist acts through providing funds and other resources. The United States and the United Kingdom have made illegal the funding of terrorist groups or acts, while Singapore has specifically mentioned individual terrorists and acts. Hong Kong has focused entirely on terrorist acts and purposes.

Reporting requirements

The reporting requirements within each country showed considerable variation. All of the countries required at least some sectors to submit reports of suspicious financial transactions, although the conditions of reporting were quite varied between countries.

In Australia, the systematic reporting requirements introduced under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) exceed those enacted in most of the other countries examined. While there were requirements in every country to submit a suspicious financial activity report in some form or other, Australia was the only country that required reports for each of the following—systematic reports for suspicious financial activity, high-value cash transactions, international movements of cash, international movements of value and international funds transfers—indicating the scope of the formal regime in Australia exceeds the others in this regard.

Australia, the United Kingdom and Taiwan require all regulated entities to submit reports of suspicious transactions. The remaining six countries have caveats, or additional guidelines, for when a report of suspicious activity is warranted.

The United States limits the transactions considered for reporting of this kind with a monetary threshold. Belgium, France and Germany also limit the transactions that might warrant a report but do so by considering the crimes they might be connected to. France's regulated entities must report transactions suspected to be connected to drug trafficking, organised crime, fraud against the European Communities, corruption, or terrorism financing. Belgium, like France, limits the reports received to those related to specific crimes which include terrorism or terrorist financing, organised crime, illicit trafficking, serious fraud and organised tax fraud, corruption, environment crime and counterfeiting. Belgium, however, only requires financial institutions to submit disclosures of suspicious transactions.

The approaches taken by Hong Kong and Singapore are somewhat different. Hong Kong and Singapore also limit the crimes that might trigger a transaction report to indictable offences in the case of Hong Kong and to drug trafficking or other criminal conduct in the case of Singapore. All individuals in Hong Kong, not just reporting entities, carry this obligation and an identical one to report suspicions of terrorist property. Singaporeans who come across transactions that might be connected to drug trafficking or criminal conduct in the course of business must submit a report. In addition, all persons in Singapore, and any Singaporean citizens overseas, must report any transactions suspected to be linked to the financing of terrorism.

Including a reporting requirement for cash transactions that exceed a threshold was less common among the nine countries considered. Australia and the United States require regulated entities to submit a report of transaction made using cash above a specific threshold set in legislation. The Australian threshold is AUD$10,000 and the United States threshold is US$10,000. Taiwan also requires regulated entities to submit a report of any cash transaction valued at NT$1m or over.

Singapore, rather than requiring a report for every cash transaction beyond a threshold, suggests to its regulated entities that large cash transactions are likely to be suspicious and warrant reporting. France and Germany have not required regulated entities to submit cash transaction reports. Germany, however, requires businesses to retain customer identification for cash transactions valued at €15,000 or more. French-regulated entities are similarly required to scrutinise cash transactions beyond a threshold limit and retain that information. Belgium prohibits cash payments of more than €15,000, rendering any reporting of this nature redundant. The United Kingdom and Hong Kong do not have any large cash transaction requirements.

Almost all of the nine countries have identical requirements to report the movements of cash across country borders, on entry and exit, but vary in the threshold amount required to trigger a report. Hong Kong is the only country considered that currently does not require reporting of international movements of cash.

Australia is one of two countries that have not mirrored the reporting requirements for cash for the movement of bearer negotiable instruments across international borders. The United States, United Kingdom, Belgium, France, Germany and Singapore subject movements of bearer negotiable instruments to the same reporting requirements, with the same thresholds, as cash movements.

Australia, instead, can require individuals moving bearer negotiable instruments across international borders to submit a report to a police or customs officer on request. There is no mandatory requirement to report all movements. Hong Kong similarly has no requirement for bearer negotiable instruments. Taiwan does not require reports for movements of instruments of value.

Australia is the only country under consideration that requires all regulated entities to report all electronic funds transfers (international funds transfer instructions—IFTIs) regardless of value.

Tipping-off clauses

Each of the nine countries currently has 'tipping-off' provisions that criminalise the revealing of details of a report about a suspicious transaction to those involved. The variations in tipping-off clauses come from the extent of the information encompassed and the exemptions made.

The United States and France have the simplest models for tipping-off and prohibit disclosing information connected to a report after it has been filed to those involved in the transaction. Belgium and Germany extend this to prohibit a disclosure connected to a report to any third party as well as the subject of a report. Both Hong Kong and Singapore prohibit the disclosure of any information related to reports to any person where the disclosure might prejudice an investigation.

Tipping-off in the United Kingdom applies to details of investigations as well as reports and extends to all third parties. The United Kingdom also has additional tipping-off provisions for civil recoveries, asset confiscations and money laundering offences. Taiwan's provisions are similar as they encompass both reports of suspect transactions and any suspected money laundering offence.

Australia specifically prohibits disclosing the details of reports of suspicious financial activity and any person or matter triggering a report to any third party. Australia also has one of the most extensive lists of persons exempt from tipping-off. Australia, like the United Kingdom, France and Singapore, exclude legal practitioners (in specific circumstances) from the requirements. Australia extends the exemptions beyond this to accountants, businesses with a joint anti-money laundering program and anyone trying to dissuade a customer from committing an offence under any law in Australia.

Judicial interpretation

The jurisprudence in the countries considered is continuing to evolve, with a number of cases having come before the courts in which questions of law have arisen. Courts have considered the meaning of 'structuring', 'concealing', 'profits' of crime and 'suspicion'. The Australian case of *R v Narayanan* addressed the definition of structuring under the *Financial Transaction Reports Act 1988* (Cth) (FTR Act) with the court defining *structuring* as *two or more non-reportable transactions conducted to ensure, or to attempt to ensure, that the transaction was not a significant cash transaction*. The court stated that multiple transactions that had been subjected to structuring could still, collectively, constitute a significant cash transaction.

In the United States, two cases have narrowed the scope of money laundering offences, one in terms of the process of laundering, the other in terms of what can be laundered. *Regalado Cuellar v United States* centred on the definition of *concealment*, finding that hiding currency for the purpose of transport was in itself not an act of laundering. The second case, *United States v Santos et al*, questioned what was meant by *proceeds of crime* and decided that it referred only to the profits generated.

Further cases have defined the actions that can constitute a conspiracy to commit money laundering. In Australia, *A Ansari v R, H Ansari v R* allowed a broad interpretation of conspiracy to launder money where the fault element for the laundering offence is recklessness. In the United States, the courts have ruled that the offence of conspiracy was to be treated the same as an actual act of money laundering.

In the United Kingdom, the definition of *suspicion* in relation to money laundering was examined in *R v DaSilva*, with the court requiring a suspicion that is more than fanciful in order for an offence of money laundering, or assisting, to be present. Cases have also questioned the extent to which proof of a predicate offence is necessary to establish money laundering.

The application of AML/CTF legislation to legal practitioners has also generated substantial debate. The decisions in the European Union and *Bowman v Fels* in the United Kingdom confirmed that legal practitioners are exempt from reporting requirements if they act in connection with giving legal advice to a client. Further issues debated in these cases were centred on the offence of making an 'arrangement' for money laundering.

The profile of the regulated sectors

Documenting the composition and size of the regulated sectors in each of the countries in question proved difficult owing to the limited data available in some countries. Difficulties were particularly encountered in obtaining information concerning industries without prudential regulation or other long-standing registration processes. Additional problems arose in obtaining information from some non English-speaking countries. Accordingly, the data located were somewhat incomplete, making comparisons across countries problematic.

Generally, the core financial institutions (the banking industry, finance companies and insurance industry) are regulated for AML/CTF purposes in all nine countries, although variations exist between the regulated sectors in relation to money service businesses (MSBs) and non-financial businesses including the professions.

The way in which AML/CTF requirements are applied to legal practitioners across the different countries gives rise to the greatest variations. Hong Kong and Singapore include legal practitioners in the full scope of their requirements, while legal practitioners in Germany, Belgium, the United Kingdom and France

have obligations only when dealing with customers in financial transactions or the settlement of real estate transactions. Legal practitioners in the United States and Taiwan are excluded from AML/CTF obligations. Australian legal practitioners, with the exception of those holding an Australian Financial Services Licence, are also excluded from AML/CTF responsibilities.

The requirements for legal practitioners in the United Kingdom, France, Belgium, Germany and Singapore are further complicated by legal professional privilege. Legal professionals in these countries, which would otherwise have AML/CTF obligations for at least some transactions, are exempt from the obligation to report suspicious transactions under some circumstances. Where the information was gained in circumstances protected by legal privilege, the lawyer involved is not required to submit a report.

Non-financial businesses in Australia, the United Kingdom and Singapore (3 countries with the most data available to estimate the size of the regulated sector) contributed the largest proportion of the regulated sectors in those countries. Undertaking a comparison between the numbers of businesses providing regulated services in all of the countries considered is a task complicated by the variations in the types of business providing services and the lack of available data for some countries. It can be concluded, however, in relation to the size of the regulated AML/CTF sector as a proportion of the entire business sector, that Australia and the United States have approximately one percent of businesses regulated for AML/CTF purposes, while the United Kingdom has almost 10 percent regulated. Complete comparative data is not available for other countries. The differences lie largely in the inclusion of the professional sectors in the United Kingdom, which account for very large numbers of businesses subject to regulation.

Compliance

Most of the countries considered in this report, with the exception of Germany and Taiwan, showed an increase in the volume of reports between the base year and the last year for which data were available.

The volume of reports submitted to authorities in Hong Kong, Singapore, France, the United Kingdom, the United States and Australia steadily increased over the period for which reporting data was available. Reporting entities in each country generally submitted a vastly increased volume of reports in 2008 or 2008–09 compared with the base year. Between 2004 and 2008, Singapore experienced an increase in reports of more than 580 percent. Reporting numbers in the United Kingdom and United States grew by 308 percent and 359 percent respectively. Singapore, unlike the United Kingdom and European Union countries, did not vastly expand the number of industries encompassed in the AML/CTF regime in that time.

Germany and Taiwan recorded a fall in the volume of reports over the period of available data. In 2007, Taiwan's Finance Intelligence Unit (FIU) received less than 40 percent of the reports filed in 2004; and Germany's FIU received 14 percent fewer reports in 2008 than in 2002.

The fluctuations in report volumes, particularly suspect transaction reports, are likely to have been influenced by factors outside of the level of suspicious activities. Any amendments made to the AML regimes, particularly any expansion in the reporting requirements or thresholds, were likely to have had an impact on the volume of reports. Also, as KPMG (2007) noted, the vast increases in reporting volumes in some countries may reflect an increased capacity to capture suspect transactions, rather than an increase in suspicious activities, in order to meet AML/CTF compliance requirements.

Including non-financial businesses in the AML/CTF regimes of these countries probably has not had a large impact on the volume of reports each FIU received within the timeframes considered in this report. Businesses in the financial services sector overwhelmingly submitted the largest proportion of reports in each of the countries considered, even in countries where non-financial businesses constituted a large percentage of the regulated sector. The non-financial businesses in the countries considered were still filing relatively low numbers of reports in the last year for which data was available. At best, the reports were low in volume and, at worst, were non-existent.

Professions with reporting requirements in the United Kingdom were responsible for only eight percent of suspicious reports in 2007, with the majority of these submitted by solicitors and accountants. In 2007, in Belgium, less than two percent of reports originated from non-financial businesses (excluding notaries), with legal practitioners and real estate agents submitting only three and two disclosures respectively. In Taiwan, only high-value dealers are required to submit reports; no businesses in this industry had submitted a report prior by 2007. The United States was the only country in this report to show comparable levels of reporting between the different sectors, with 48 percent of suspicious financial transaction reports in 2007 submitted by businesses outside of the financial sector.

The low levels of reporting from businesses outside of the financial sector cast doubt on the effectiveness of the regime in reaching these industries. Low levels of supervision have been suggested by the International Monetary Fund (IMF) as an explanation of the low numbers of reports by these industries in France. Recent changes to regulatory regimes in several countries, including Australia and those in the European Union, means that it is too early to adequately evaluate the level of compliance in this area.

Belgium had one of the highest percentages of reports leading to cases being forwarded to prosecution officials in 2007. Belgium's FIU received just over 12,000 reports and submitted 1,666 cases to the public prosecutor in that year. This represented 13 percent of all reports submitted and 23 percent of the total number of files opened. Taiwan's FIU also passed on a large proportion of cases to law enforcement in 2007. The Taiwanese FIU received fewer than 2,000 reports in that year and sent more than 20 percent of these onto law enforcement agencies. France, by contrast, passed on approximately 400 reports to law enforcement (3%) of the 12,000 reports received in 2007. The United Kingdom filed charges in 766 cases, resulting in 276 convictions, from more than 220,000 reports filed with the FIU.

Prosecution and enforcement

As with the levels of reporting suspicious financial activity, the number of people charged or prosecuted for money laundering has also generally increased within the nine countries analysed in this report. The approach to reporting enforcement figures also varied between countries.

Prosecution data in the Australian statistics show the number of charges dealt with by the public prosecutor, Germany reports the number of convictions, Taiwan measures prosecutions, the United Kingdom provides convictions and formal cautions and Hong Kong records convictions only. Statistics were not able to be gathered from France, Belgium and Singapore. Nevertheless, some general trend data can be extracted for the countries that published information in this area.

Most countries reported annual increases in the levels of enforcement activity in each country. By contrast, Germany reported a 40 percent decrease in the number of offences between 2002 and 2003. However, the number of recorded offences then increased between 2003 and 2007, with a 160 percent increase in the number of convictions in 2005 and 2006.

The United Kingdom demonstrated a dramatic increase from 16 offenders found guilty or cautioned in 2003 to 1,328 offenders in 2006. Convictions in Hong Kong increased from 49 convictions in 2004 to 179 in 2007. The volume of Australian offenders dealt with for criminal money laundering offences increased from five in the 2003–04 financial year, to 50 in 2009–10. Despite the increased volume of offenders dealt with during this period, Australia's volume of prosecutions is still low compared with other countries considered within this report. Statistics from the United States were obtained for the period 1994 to 2001 and it was found that the volume of money laundering charges remained constant during this period.

Best-practice strategies to enhance compliance

The strategies employed by the FIUs and AML/CTF regulators to enhance compliance fall into two principal categories—dialogue between the FIU and reporting entities, and increasing the ease of submission. The countries considered in this report have all adopted some aspects of both of these broad strategies for heightening compliance through non-punitive means.

Electronic report filing systems are common throughout all nine countries examined. Information available suggests that electronic filing has all but replaced paper disclosures in most cases.

In terms of feedback from FIUs to industry, it appears that the UK's FIU publishes more information on the volume and type of feedback provided to reporting entities than the Financial Crimes Enforcement Network (FinCEN) in the United States. A key feature of the feedback given to reporting entities in the United Kingdom is the systematic visits and seminars conducted within each sector. The Serious Organised Crime Agency (SOCA) also provides more general feedback to reporting businesses with website-based guidance on producing useful suspicious activity reports (SARs). Reporting entities also receive alerts to industry which detail information about the SARs regime. France has released less information on the feedback systems between Traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN) and reporting entities in English than other countries, making gauging the level of interaction less accurate. TRACFIN's annual report, however, contains some information intended for a reporting audience in the form of sanitised cases.

A number of FIUs reported providing or assisting in training key officers in reporting entities. The sector-specific seminars run by SOCA in the United Kingdom are conducted as an education tool for money laundering reporting officers. The United States, United Kingdom and Hong Kong all report formal processes for seeking feedback from reporting entities and others.

Future initiatives

Future comparative studies of this nature should aim to provide more complete information on the variables under consideration. This would entail undertaking qualitative research targeted at the regulators and industry associations in each country and, in the case of non-English-speaking locations, would require multilingual research and access to business and government statistical collections. Additional qualitative research would be likely to provide a more complete picture of the AML/CTF enforcement outcomes and the utility of the financial intelligence gathered by AML regimes. Additional qualitative information could inform regulators and others of the potential value of providing feedback to regulated businesses and highlight the effectiveness of other compliance-enhancing initiatives. This research may also inform regulators and policymakers of the practical implications for regulated businesses of the changes made to AML/CTF preventative systems in place.

As is apparent from this review, the challenges of conducting such research from open source documents are considerable, as public source material provides only a limited perspective. Problems also exist within individual nations where data are not being collected, or are collected in variable formats using different data fields, categories and definitions. The FATF-GAFI Mutual Evaluations provide a good deal of uniformly collected and comparable information, but often these reports are incomplete. Regulators and FIUs also collect considerable amounts of data from the regulated sectors in annual compliance reports, but these are not readily available or are collected using non-uniform categories across countries.

Ideally, a single repository of AML/CTF compliance and regulatory data should be established, although in practice, the resources required for this would be prohibitive. At present, the most that can be asked is that FIUs, law enforcement agencies and regulators maintain a dialogue to develop the use of harmonised data recording practices for the key variables of policy importance such as measures of enforcement outcomes and compliance statistics. The present report aimed to provide a basis for comparing the AML regimes by mapping the key components of the AML systems and identifying variables for tracking the use of those systems and has suggested areas for improving data collection in these areas. It is hoped that it provides an indication of the areas requiring most attention for dialogue and discussion in the years ahead.

Introduction

Background

The primary aims of those who commit economic crimes are to secure a financial advantage and to be able to make use of stolen funds without being detected by police and regulatory agencies. Many criminals, but by no means all, seek to disguise the origins of their criminally derived funds by engaging in a process of money laundering. Others, however, simply spend the money obtained with little attempt at concealment—which often leads to detection by police then prosecution and punishment. Organised criminals, in particular, see many benefits in money laundering, which include the ability to enhance their lifestyle and to enable the profits of their crimes to be re-invested in future criminal activities or in legitimate business operations.

There are three stages to laundering the proceeds of crime. In the initial or placement stage, the money launderer introduces illegal profits into the financial system. In some cases, illegally obtained funds may already lie within the financial system, such as where funds have been misappropriated electronically from the accounts of businesses. Placement can also entail splitting large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of financial instruments, such as cheques or money orders, that are then collected and deposited into accounts at other locations.

After the funds have entered the financial system, the launderer may engage in a series of transactions to distance the funds from their source. In this layering stage, the funds might be channelled through the purchase of investment instruments, or by transferring money electronically through a series of accounts at various banks. The launderer might also seek to disguise the transfers as payments for goods or services, thus giving them a legitimate appearance. Another device used at the layering stage is to use corporate and trust vehicles to disguise the true beneficial ownership of the tainted property.

Having successfully processed criminal proceeds through the first two phases, the money launderer then moves to the third or integration stage in which the funds re-enter the legitimate economy. The launderer might choose to invest the funds in real estate, luxury assets, or business ventures. It is at this stage that criminals seek to enjoy the benefits of their crimes, without risk of detection.

In response to mounting international concern about money laundering, FATF-GAFI was established in 1989. FATF-GAFI is an inter-governmental body which sets international standards and develops and promotes policies to combat money laundering and terrorist financing. In 1990, FATF-GAFI issued a set of 40 Recommendations to guide the fight against money laundering (FATF-GAFI 2004). The 40 Recommendations set out the framework for anti-money laundering efforts and provide a set

of counter-measures covering the criminal justice system and law enforcement, the financial system and its regulation, and measures to enhance international cooperation.

Following the attacks on the United States on 11 September 2001, FATF-GAFI expanded its mandate to deal with the financing of terrorism and created an additional nine Recommendations aimed at combating the funding of terrorist acts and terrorist organisations (FATF-GAFI 2008c). Financial transaction monitoring expanded considerably with the inclusion of counter-terrorism financing into the regime. The financing of terrorism often involves the use of legitimately derived funds, unlike money laundering which invariably involves the proceeds of criminal activities. As such, regulators have been required to examine a wide and ever-increasing number of transactions in an attempt to locate those which could show evidence of money laundering or financing of terrorism.

In June 2003, FATF-GAFI completed a major review of its Recommendations. The revised Recommendations were designed to combat increasingly sophisticated money laundering techniques, such as the use of corporate and trust entities to disguise the true ownership and control of illegal proceeds, and the increased use of professionals to advise and assist in money laundering. The Recommendations indicate the measures FATF considers necessary within criminal justice and regulatory systems, the preventive measures FATF-GAFI suggests are to be taken by financial institutions and certain other businesses and professions, and measures to facilitate international cooperation (FATF-GAFI 2004).

The FATF-GAFI 40 plus nine Recommendations to combat money laundering and the financing of terrorism have three primary objectives (FATF-GAFI 2004):

- to support the criminalisation of money laundering and the financing of terrorism;
- to ensure that assets linked to money laundering or the financing of terrorism can be frozen and confiscated; and
- to ensure that financial institutions and other regulated businesses comply with the Recommendations.

The strong emphasis that FATF-GAFI places on regulating financial institutions and other businesses aims to prevent money laundering and the financing of terrorism by making these activities more difficult for offenders to commit and facilitating the detection of offences by contributing information to law enforcement agencies. The removal of Burma (Myanmar) from FATF-GAFI's Non-Cooperative Countries and Territories list in October 2006 (FATF-GAFI 2007b) signified basic levels of compliance with the 40 plus nine Recommendations by the vast majority of countries globally.

There is, however, considerable disparity in the manner in which different countries across the globe have implemented the Recommendations and the scope and application of the Recommendations continues to evolve as local legislation and case law appears. Some countries have, for example, placed stringent limitations on the scope of the Recommendations through the enactment of local legislation, as interpreted by the courts. On occasions, this has limited greatly the application of the Recommendations to specific business sectors or types of transactions. By contrast, many countries, such as Australia, have recently introduced further legislation or amended existing legislation to implement FATF-GAFI's Recommendations more fully. The new legislation in these countries has yet to be tested, either before the courts in connection with prosecutions for non-compliance, by law enforcement organisations using the information gathered, or by the FATF-GAFI mutual evaluation process. It is timely, therefore, to review the state of international responses to the FATF-GAFI Recommendations to assess how countries have applied the requirements, what sectors have been subject to regulation and how compliance and enforcement are undertaken.

Aims and definitions

This report presents an environmental scan of the differing approaches taken by nine countries, including Australia, to adopting an AML/CTF regulatory regime and aims to make a meaningful comparison between those regimes in a number of key areas. It also seeks to document potential measures of the extent of the application of

regulatory requirements within each selected country and to assess and compare the extent of compliance and enforcement activities under each regime.

The aim of this report is to provide an intensive comparative review and analysis of some of the primary AML/CTF regulatory issues across the globe, not to reproduce the information contained in FATF-GAFI Mutual Evaluation Reports. Some commentators, such as Harvey (2005) and Sproat (2007), have sought to evaluate the performance of the AML/CTF regime using data on money laundering prosecutions, suspect transaction reporting, asset recoveries and other activity measures. Both Harvey (2008) and Sproat (2007) note the difficulty of evaluating the impact of AML/CTF regimes in the absence of clear evidence on the volume of money laundering prior to implementing enhanced AML/CTF systems. Accordingly, there is little base-line data upon which to undertake a rigorous evaluative assessment. The impact on less tangible goals such as maintaining or improving the integrity of financial systems is more difficult to gauge.

The present report does not seek to evaluate the effectiveness of the AML/CTF regimes of the countries examined as this research activity will be undertaken in another Australian Institute of Criminology (AIC) study. It is apparent, however, that the measures of AML/CTF activity provided in this report are insufficient to draw conclusions on the value of the AML/CTF system in any of the countries examined or to compare performance between them. Many of the core aspects of implementation of the regime globally, such as financial intelligence reporting volumes and conviction rates, cannot be considered proxy measures of the success of the AML/CTF system in the absence of a direct link between these indicia and a working definition of success for the regime. Arguably, the volume of items such as reports of suspicious financial activity could be evidence of either a large-scale money laundering problem or a small one. Simply relying on reporting activity levels is an inadequate measure of the success or otherwise of the regime, as reporting is influenced by a range of considerations in addition to levels of underlying laundering activity and predicate crime. The volume of reports of suspicious financial activities in any given year, for example, could reflect close to the total number of suspect transactions that took place or were attempted in a single country in a single year. The volume could also simply reflect the results of action by regulators in educating regulated businesses concerning their reporting obligations. The extent to which suspect and other transactions are reported is also dependent on the view taken by those in the regulated sectors concerning the necessity for, and effectiveness of, reporting. Some may take the view that reporting is unnecessary in most situations, while others may report even low-risk matters in order to avoid risk of enforcement action for regulatory non-compliance. The number of reports made also reflects the number of transactions that take place within a country each year. Many reports may reflect the presence of a large economy with an active financial services sector—the business sector likely to be responsible for the highest proportion of suspect matter reports.

Similar considerations apply to the use of money laundering convictions as a measure of money laundering that occurs in a given country (Reuter & Truman 2005). Few convictions may mean that there is little detected money laundering occurring, or that money laundering simply is not being detected, reported or dealt with by police and prosecutors. Further, it may also mean that prosecutors favour charging predicate offences or alternative changes rather than using offences of money laundering where these exist. Put simply, official crime statistics in this area often provide a poor measure of underlying money laundering activity. These and other problems of evaluation will be canvassed more fully in another AIC report.

As the countries discussed in this report share a common basis in having agreed to be bound by FATF-GAFI's Recommendations and other international AML/CTF standards, the central aspects of their AML/CTF regimes are similar. The legal definitions, however, of these common aspects are not uniform across all of the countries considered.

The following are definitions of key aspects of AML/CTF regimes discussed in this report that will be used throughout the report:

- *alternative remittance services (ARS)*—transmission of money or value, including informal systems or networks, outside of the formal banking sector;

- *regulated entities*—businesses, including financial institutions, MSBs and designated non-financial businesses and professions with AML/CTF obligations under respective regulatory regimes;
- *regulated sector*—all businesses providing a financial, money service, or non-financial designated service currently regulated for AML/CTF purposes in each country;
- *financial institution*—a person or entity conducting, as a business, one or more of the following activities or operations on behalf of a customer:
  - accepting deposits and other repayable funds from the public;
  - lending and financing commercial transactions;
  - financial leasing;
  - transferring money or value;
  - issuing and managing means of payment such as stored value cards;
  - providing financial guarantees and commitments;
  - trading in money market instruments, foreign exchange, exchange, interest rate and index instruments, transferable securities or commodities;
  - participating in securities issues;
  - portfolio management;
  - otherwise investing, administering, or managing funds on behalf of another person;
  - underwriting and placing life insurance and other investment-related insurance products; and
  - money and currency exchanging;
- *designated non-financial businesses and professions (DNFBPs)*—businesses, outside of financial institutions, identified by AML/CTF legislation as exposed to risks of money laundering and the financing of terrorism. The DNFBPs identified by FATF-GAFI are:
  - casinos;
  - real estate agents;
  - dealers in precious metals;
  - dealers in precious stones;
  - legal practitioners, notaries, other legal professionals and accountants providing services to external clients; and
  - trust and company service providers.
- *reports of suspicious financial activity*—reports lodged by financial institutions and other regulated entities to the financial intelligence unit of any transaction suspected of being the proceeds of criminal activity or involved in the financing of terrorism.
- *reports of high-value cash transactions*—reports lodged by financial institutions and other regulated entities to the financial intelligence unit of any transaction in cash greater than a nominated value threshold.
- *reports of international movements of cash*—reports lodged to the financial intelligence unit of the movement of physical currency across national borders, usually above a nominated threshold.
- *reports of international electronic transactions*—reports lodged by financial institutions and other regulated entities to the financial intelligence unit of the electronic transfer of funds overseas, usually above a nominated threshold;
- *FIU*—a central agency responsible for receiving (and as permitted, requesting), analysing and disseminating disclosures of financial information:
  - concerning suspected proceeds of crime and potential financing of terrorism; or
  - required by national legislation or regulation in order to combat money laundering and terrorist financing;
- *tipping-off provisions*—requirements for entities filing reports of suspicious financial activity to avoid disclosing information about the details or the report, or the existence of a report, to the subject of the report or another prohibited party;
- *criminal penalties*—penalties imposed following a criminal conviction for an offence;
- *civil penalties*—penalties imposed following civil proceedings rather than proving an offence to a criminal standard or with criminal court procedures;
- *predicate offences*—financially motivated offences generating funds to be laundered;
- *criminal asset recovery*—freezing or confiscating the assets generated by a crime after a conviction for that offence; the required standard of proof is usually beyond a reasonable doubt;

- *civil asset recovery*—freezing or confiscating assets that are believed to be generated by a crime in a process held independently from criminal proceedings or not reliant on a conviction for an offence; the required standard of proof is usually on the balance of probabilities and not beyond a reasonable doubt; and
- *unexplained wealth*—requiring persons possessing suspect assets to demonstrate their lawful acquisition to a court; this process reverses the onus of proof.

The scope and application of each of these terms and concepts is governed by the precise terms of local legislation, as interpreted by the courts. The above definitions are used, in a general sense, for discussion purposes across all jurisdictions.

Geographical scope

This report compares data from eight countries that demonstrate diverse experiences of implementing AML/CTF measures from the position adopted in Australia. The jurisdictions were selected from North America (United States), Europe (United Kingdom, France, Germany, Belgium) and Asia (Singapore, Hong Kong, Republic of China (Taiwan)) in order to provide an indication of how diverse nations in separate continents have approached AML/CTF implementation. They were also chosen to be indicative of the measures taken in countries with different legal traditions; and of those that experience different types of risk in terms of money laundering and financing of terrorism.

Methodology

The majority of the information used in this report has been sourced from publicly available documents produced by regulatory bodies, financial intelligence units, law enforcement and other government agencies, industry bodies and FATF-GAFI itself.

The authors undertook a number of consultations with stakeholders in order to supplement the publicly available information. Consultations with the Australian Transaction Reports and Analysis Centre (AUSTRAC)—the Australian financial intelligence unit—provided additional estimates of the number of businesses currently regulated for AML/CTF in Australia. A Roundtable discussion was also held in Canberra in 2007 with 25 law enforcement and industry stakeholders.

Additional consultations held in the eight countries of interest expanded on the available information on the regulatory environment in those countries and on law enforcement responses to money laundering and the financing of terrorism offences.

- In London, the British Bankers' Association, the Law Society of England and Wales, the Solicitors Regulation Authority, selected legal practices, the Institute of Chartered Accountants in England and Wales, the Fraud Advisory Panel, the Financial Services Authority, the Organised and Financial Crime Unit, UK Home Office, the Serious and Organised Crime Agency, HM Treasury, the Foreign and Commonwealth Office, Counter Terrorism Policy Department, the International Association of Money Transfer Networks Ltd and the Economic and Specialist Crime Operational Command Unit, Specialist Crime Directorate of the Metropolitan Police Service all provided information on the United Kingdom.
- Consultations with the Ministry of Justice, FIU Germany and Dr Thomas Spies contributed additional statistics and regulatory information for Germany.
- The Banking Commission, situated within the International Chamber of Commerce, and the FATF-GAFI Secretariat in Paris also participated in consultations as part of this project.
- In Belgium, information was provided by the Belgian Financial Intelligence Processing Unit in Brussels.
- In the United States, consultations were held with the Peterson Institute for International Economics, Professor Peter Reuter, Maryland School of Public Policy, the Terrorist Financing Operations Section of the Federal Bureau of Investigation, US Treasury Executive Office for Asset Forfeiture, FinCEN, IMF and Mr Bruce Zagaris, Partner, Berliner, Corcoran and Rowe LLP.
- In Singapore, consultations were held with representatives of the International Centre for Political Violence and Terrorism Research/ Nanyang Technological University, Deutsche Bank AG, DBS Bank Ltd, Commercial Affairs Department, OCBC Bank, United Overseas Bank Limited, Citibank Singapore Ltd, BNP Paribas Singapore Branch and the Association of Banks in Singapore.

- In Hong Kong, consultations were conducted with HK Customs & Excise, Joint Financial Intelligence Unit, Department of Justice, Independent Commission Against Corruption, Hong Kong Monetary Authority, Commercial Crime Bureau, Hong Kong Police Service, Hong Kong Association of Banks and University of Hong Kong.
- In Taiwan, the Money Laundering Prevention Centre (MLPC), Central Bank of the Republic of China, Banking Bureau, Financial Supervisory Commission, Financial Examination Bureau, Criminal Investigation Bureau, National Police Administration, Ministry of the Interior, Interpol Taipei, Office of Homeland Security (Counter Terrorism Office), Crime Research Centre/National Chung-Cheng University, and SinoPac Bank in Taipei also contributed information during consultations.

Regulatory regime and case law

The details on the regulatory regime for each country were sourced from the following publicly available documents:

- legislation;
- guidance notes released by regulatory and industry bodies for specific sectors;
- annual reports from financial intelligence units and government agencies and departments; and
- Mutual Evaluation Reports conducted by FATF-GAFI, IMF and the Asia/Pacific Group on Money Laundering (APG).

The cases discussed for each country have been sourced from published case transcripts and other court documents, legal industry body websites, regulatory compliance agency publications and some media reports.

Evaluating the size of the regulated sector

The estimates of the size of the regulated sectors in each of the countries were drawn extensively from publicly available information from regulatory and supervisory agencies. Information from industry bodies without compliance or enforcement powers was used to estimate the number of businesses with AML/CTF obligations where official figures from regulatory agencies were not available. Mutual Evaluation reports published by FATF-GAFI, IMF, or APG were also employed to estimate the number of businesses in industries with AML/CTF requirements for some countries.

Compliance and enforcement

Compliance and enforcement data were derived from several years of financial intelligence unit and government agency annual reports, activity reviews and the Mutual Evaluation reports. English language translations were not available from some agencies; data were also gathered from agency websites in these instances.

Structure of this report

This report provides a summary of the regulatory regime and key cases in each country, the estimated size of the regulated sector and the extent of compliance and enforcement activity in each jurisdiction.

The second section describes the AML/CTF legislative regime in each of the nine countries. It includes the criminal provisions for money laundering and the financing of terrorism, as well as the basis of the preventative regulatory measures in place for each country. The structure of the financial intelligence unit, the scope of the regulated sector, the obligations to submit financial intelligence reports, the inclusion of tipping-off provisions and the basis of the required compliance programs are discussed. Less focus is placed on specific customer identification requirements, record keeping provisions and ongoing customer due diligence. A detailed discussion of emerging areas of concern, such as the use of informal banking systems and charities for money laundering and terrorism financing activities, is also beyond the scope of this report. These areas, however, are noted where countries regulate them for AML/CTF purposes.

The second section also provides some consideration of case law arising from money laundering convictions and sanctions applied for non-compliance with AML/CTF regulations. The focus is on prosecutions and other events specifically

involving regulated businesses in the jurisdictions where this information is available. Discussion of criminal prosecutions of individuals for money laundering in some countries has also been included where this has challenged the perception of the money laundering offence in some way.

The third section attempts to describe and compare the size of the regulated sector in each country considered in the scope of the report. The contribution of businesses from the financial, money service and DNFB industries are compared for each country where the information is available. This section also documents the extent of regulation of key non-financial businesses such as legal practitioners, accountants, the gambling industry and dealers in precious metals and stones.

The fourth section surveys the extent of compliance and enforcement activity in the nine countries.

A range of measures have been used in an attempt to gauge the degree of compliance and enforcement in each jurisdiction. The countries considered within the scope of this report have not adopted and reported uniform measurements of compliance of enforcement activity and as a result, the information presented for each country is a combination of financial intelligence report statistics, prosecutions statistics and asset freezing and recovery figures.

The final section documents some of the strategies adopted by financial intelligence units and regulators to promote compliance in the selected jurisdictions. The use of electronic report filing, the provision of timely feedback to industry, the extent of training provided to the regulated sectors and the degree to which financial intelligence units have sought feedback from the regulated sectors are methods for boosting compliance are discussed in this section.

Regulatory regime

This section presents information on a sample of international AML/CTF regulatory regimes and aims to compare the scope of the regime in Australia with that in the United States and selected countries in the European Union and Asia. The comparison of the AML/CTF regulatory regimes in this section is centred on the key legislation, extent of the regulated sector, the key obligations under the AML/CTF legislation and the financial intelligence unit. This section also addresses case law as it relates to AML/CTF and its implementations in the selected countries.

Financial intelligence units

FIUs were first established in the late 1980s and early 1990s in response to a need to centralise money laundering information. The scope of FIU responsibilities was subsequently widened to include the financing of terrorism following the increased risks of the twenty-first century. This represented new challenges as the methods of the financing of terrorism are different from those normally associated with money laundering (Schott 2004).

All FIUs share three core functions, which are to receive, analyse and disseminate information in order to combat money laundering and terrorist financing domestically and as Schott (2004) argues, internationally. Aside from these common core functions, however, the design of FIUs can differ dramatically. Schott (2004) identifies four types of FIU. These are based on an administrative model, a law enforcement model, a judicial (prosecutorial) model and a hybrid model.

The administrative model FIU may be either independent or attached to a regulatory or supervisory authority. The role of the administrative FIU as an intermediary between law enforcement and reporting entities allows this type of FIU to remain neutral. The information channelled through administrative model FIUs is also more easily exchanged between the FIUs of other countries. The drawback of the administrative model is that the separation of the FIU from law enforcement organisations limits its powers to obtain evidence and assert measures based on suspicious transactions. This style of FIU may also be subject to more stringent supervision by political authorities (Schott 2004).

The law enforcement model solves the issue of accessing evidence and obtaining outcomes from suspicious transaction reports (STRs), as this type of FIU has the maximum law enforcement use of disclosure information and access to criminal information. Law enforcement model FIUs, however,

tend to be more focused on investigation than on prevention and may be treated with suspicion by reporting entities who may view the FIU as an extension of the police (Schott 2004).

Judicial or prosecutorial FIUs are affiliated with a judicial or prosecutors office. These are often relatively free from political influence and the intelligence obtained by the FIU can be given directly to the prosecutor. The disadvantages of judicial model FIUs can be the same as law enforcement models. A fourth approach to FIU structures is a hybrid of the above models (Schott 2004).

The countries in this report represent two different FIU types. The FIUs of Australia, Belgium, France and the United States are administrative FIUs. The FIUs of Germany, the United Kingdom, Hong Kong and Singapore are law enforcement examples.

FIUs also vary in the degree of autonomy experienced and this is often influenced by the placement of the FIU in the government and law enforcement structures. FIUs established outside of a government agency are likely to have the greatest level of autonomy, while those that are part of the central bank are likely to be more autonomous than one within a ministry (Schott 2004). FIUs may also serve as a regulator or supervising body over regulated entities.

Australia

Anti-money laundering and counter-terrorism financing legislation

Criminal money laundering offences

Australia has a complex legislative regime for detecting, prosecuting and deterring money laundering activities. Commentators have divided this legislation into three categories (Deitz & Buttle 2008):

- criminal offences for money laundering at both a Commonwealth and a state and territory level;
- asset recovery legislation, also present at both a Commonwealth and a state and territory level; and
- prevention and detection measures, legislated at a Commonwealth level.

Money laundering offences are criminalised at a Commonwealth level in Division 400 of the *Criminal Code Act 1995* (Cth) (Criminal Code). The definition of money laundering in the Criminal Code is broad. The Criminal Code does not limit predicate offences with a specific list. Predicate offences are, instead, those with a minimum sentence of at least one year's imprisonment. Australia's money laundering offences are distinguished from each other according to the amount of money involved in the activity and the level of intent of the accused.

The Australian states and territories have also enacted legislation creating offences for money laundering. The offences at a state and territory level differ according to areas such as relevant predicate offences, the intent of the defendant and penalties attached to the offences.

Asset recovery mechanisms

The bulk of the Commonwealth asset recovery provisions are contained in the *Proceeds of Crime Act 2002* (Cth) (POCA 2002). POCA 2002 repealed the previous *Proceeds of Crime Act 1987* (Cth) (POCA 1987). POCA 1987 allowed law enforcement to pursue the recovery of assets linked to offences after a conviction. POCA 2002 added the ability to use civil recovery to the Commonwealth's asset recovery mechanisms.

Each Australian state and territory also has asset recovery legislation for funds generated by offences at state level. All Australian states and territories, with the exception of Tasmania, have replaced criminal-based asset recovery schemes with those that also enable the recovery of assets using civil procedures.

Key preventative legislation

Australian anti-money laundering legislation developed as a direct response to two Royal Commissions in the 1980s exposing the links between money laundering, major tax evasion, fraud and organised crime. The Costigan and Stewart Royal Commissions identified the need for legislative strategies to address these issues. While initially focusing largely on suspect transactions and large cash transactions, Australia's anti-money laundering legislation was later extended to include

the reporting and monitoring of certain international transactions. Australia's primary anti-money laundering legislation, the FTR Act, was enacted to erect barriers in Australia's wider financial and gambling sectors to discourage financially motivated criminals and to provide financial intelligence to revenue and law enforcement agencies. It applied to a wide range of businesses within the financial services industry, including banks, building societies, credit unions, the insurance industry, the travel industry and the gambling industry.

The FTR Act was the first piece of legislation related to the prevention and detection of money laundering and the financing of terrorism in Australia. The AML/CTF Act replaced the FTR Act as the primary AML/CTF legislation in Australia in 2006. The AML/CTF Act was subsequently amended in April 2007. Currently, there are 71 services with AML/CTF obligations identified in the Act. The AML/CTF regime is also comprised of supporting regulations and by legally binding Anti-Money Laundering and Counter-Terrorism Financing Rules Instruments issued by the AUSTRAC Chief Executive Officer.

The provisions of the AML/CTF Act encompass all sectors and entities that provide the services designated within the Act as carrying a risk of money laundering or of terrorism financing. The focus is on the nature of the service rather than on the nature of entity that supplies it. The Act applies to financial institutions and designated non-financial businesses including MSBs and some professions.

The AML/CTF regime is a risk-based system in which businesses supplying designated services have the discretion to assess the risks associated with specific customers and transactions and, to an extent, determine how to mitigate that risk by meeting the obligations under the Act.

Terrorism financing legislation

Australia also has a number of pieces of legislation prohibiting the financing of terrorism and aimed at preventing it. The current Australian legislation for terrorism financing offences can also be classified into similar categories as those of money laundering offences:

- Criminal offences for the financing of terrorism in ss 102–103 of the Criminal Code—the *Suppression of the Financing of Terrorism Act 2002* (Cth) amended the Criminal Code to include these provisions. The terrorism financing offences were later amended by the *Anti-Terrorism Act* (no. 2) 2005 (Cth).
- Additional asset freezing legislation is also contained in the *Charter of the United Nations Act 1945* (Cth) (CoTUNA)—this Act contains provisions related to Australia's obligation, as a member state of the United Nations, to freeze the assets of nominated terrorists. The CoTUNA's provisions (s 20) criminalise dealing with the assets linked to any individual or entity on the Consolidated List maintained by the Department of Foreign Affairs and Trade, in addition to criminalising the provision of assets (s 21) to individuals or entities on the list.
- The AML/CTF Act, and the associated regulations, is targeted at the financing of terrorism as well as money laundering offences.

Financial intelligence unit

AUSTRAC acts as both the FIU and central AML/CTF regulatory body in Australia. AUSTRAC was originally established under the FTR Act in 1988.

AUSTRAC is a statutory authority within the Attorney-General's portfolio (AUSTRAC 2007). While AUSTRAC is the AML/CTF regulator in Australia, it does not have any law enforcement powers or prosecutorial powers and is an administrative style FIU. AUSTRAC employed 311 full-time equivalent staff, on average, in 2008–09 (AUSTRAC 2009a).

Regulated sector

The AML/CTF regime currently applies to:

- financial services (banks, credit unions, building societies, lending, leasing and hire purchase companies, stored value card issuers, asset management companies, financial planners (who arrange for the issue of financial products), life insurers, superannuation funds, custodial services companies and security dealers);

- MSBs (remittance dealers, issuers of traveller's cheques, foreign exchange dealers and cash couriers);
- the gambling sector (casinos, bookmakers, TABs, clubs and pubs, internet and electronic gaming service providers); and
- bullion dealers.

The AML/CTF Act does not encompass DNFBPs outside of providers of the above services, although the implementation of reforms to include legal practitioners and accountants providing specific services, real estate agents, trust and company service providers, and dealers in precious metals and stones are being considered by the Australian Government.

Obligations

The obligations contained in the AML/CTF Act were introduced in stages of six months, 12 months and 24 months after Royal Assent. The customer identification and verification obligations came into effect 12 months after Royal Assent (12 December 2006), as did the obligation to establish and maintain an AML/CTF program. Record keeping and other aspects came into effect the day after Royal Assent.

Financial intelligence reports

The AML/CTF Act currently requires regulated entities to provide the following financial intelligence reports to AUSTRAC:

- Reports of suspicious financial activity—all entities in the regulated sector are obligated to submit SMRs to AUSTRAC. SMRs are discretionary reports that may be triggered by transactions of any value or at any stage of a transaction.
- Reports of high-value cash transactions—all entities in the regulated sector must submit a threshold transaction report for any transaction in physical currency, or e-currency, of $10,000 or more (or foreign currency equivalent). SMRs can be lodged in connection with a threshold transaction report.
- Reports of international electronic transactions—reporting entities are obligated to report all IFTIs, regardless of value, to AUSTRAC. A report of IFTIs can also be the subject of an SMR or of a threshold transaction report.

The AML/CTF Act also contains the reporting requirements for individuals moving physical currency, or bearer negotiable instruments into or out of Australia:

- Reports of international movements of cash—individuals moving AUD$10,000 or more, or the equivalent in foreign currency, into or out of Australia must submit an international currency transfer report under the AML/CTF Act. A previous obligation to report movements of cash existed under the FTR Act.
- Reports of international movements of instruments of value—individuals moving instruments of value into or out of Australia may be required to submit a report of bearer negotiable instruments by a police or Australian Customs Service officer.

Tipping-off

The AML/CTF Act has tipping-off provisions for regulated entities that have filed a suspicious matter report. Entities are prohibited from disclosing information about the submission of a suspicious matter report, or any person or matter that leads to a reporting obligation, to anyone other than an AUSTRAC staff member or the AUSTRAC chief executive officer.

There are exceptions to the tipping-off provisions in the AML/CTF Act. Businesses performing the following services are exempt from the tipping-off provisions if a disclosure is made to dissuade a customer from engaging in conduct that constitutes an offence against either Commonwealth or state or territory law:

- legal practitioners, partnerships or companies supplying legal services;
- qualified accountants, partnerships or companies supplying professional accountancy services; and
- another person specified in the AML/CTF Rules.

Reporting entities are also exempt from the tipping-off provisions if a disclosure is made to a legal practitioner in order to gain legal advice. Any person to whom a disclosure is made under these circumstances is prohibited from further disclosing the information.

Matters reported under Part 4 of CoTUNA are also exempt from the tipping-off provisions, as are disclosures made in the following circumstances:

- businesses with a joint anti-money laundering program within a designated business group are able to disclose information to other businesses within the group to inform them of the risks of dealing with a specific customer;
- reporting entities that are authorised deposit taking institutions (ADIs) may disclose information to owner–manager branches of that ADI.
- disclosures made in compliance with a Commonwealth, state, or territory law or those made to a law enforcement body.

Disclosures made contrary to the tipping-off provisions constitute a criminal offence for the individual, and not a civil penalty offence for the reporting entity, in Australia.

Anti-money laundering/counter-terrorism financing compliance programs

The AML/CTF Act requires all reporting entities to establish an AML/CTF program. This obligation came into effect on 12 December 2007. Reporting entities are required to assess their own levels of money laundering and terrorism financing risks and develop their own programs.

There are three types of programs—standard programs for individual businesses, joint programs for businesses that form part of a designated business group and special programs that apply only to Australian Financial Services Licence holders that offer a specific designated service under the AML/CTF Act.

The vast majority of reporting entities must develop either standard or joint programs. Each program type has two components. Part A of the program refers to identifying, managing and reducing the risk of money laundering and terrorism financing faced by the reporting entity. Part B of the program centres on customer identification measures and includes the minimum 'know your customer' information requirements.

All reporting entities must report their compliance with the AML/CTF Act to AUSTRAC. The AUSTRAC chief executive officer defines the compliance reporting timeframe and submission date by issuing a Rules instrument.

United States

Other countries have imitated the AML/CTF regime of the United States because of its pioneering status and because of the centrality of the United States to international finance (Levi & Reuter 2006).

Anti-money laundering and counter-terrorism financing legislation

Money laundering legislation

The current AML regulations in the United States are a composite of a number of legislative acts and regulations which have evolved over time (Aggarwal & Raghavan 2006). The development and amendment of these acts has often been a response to concerns over specific incidents.

The *Bank Records and Foreign Transaction Reporting Act 1970* (Bank Secrecy Act) was the first legislation introduced in the United States specifically targeting money laundering and was aimed primarily at the use of foreign banks for money laundering (Gup 2006). The *Money Laundering Control Act 1986* (Money Laundering Control Act) was introduced as a component of the 'war on drugs' in the 1980s. The *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 2001* (the PATRIOT Act) was a response to terrorism drafted after the 11 September 2001 attacks (Levi & Reuter 2006). Dividing the US legislation into criminal measures, asset freezing and prevention is complicated by the extended history of money laundering legislation in the United States.

The Bank Secrecy Act did not initially criminalise money laundering as an offence. The Bank Secrecy Act focused instead on tracking the secret use of foreign bank accounts by US customers. The criminalisation of money laundering occurred when the Money Laundering Control Act amended the Bank Secrecy Act to introduce criminal provisions. The Money Laundering Control Act amendments also increased the potential liabilities for legal persons. It extended the criminal offences beyond natural persons to financial institutions.

Criminal money laundering offences in the United States vary according to the circumstances of the laundering activity and not according to the amount of money involved or the level of intent of the launderer. The Money Laundering Control Act specifies the predicate crimes for money laundering offences in the United States. There are currently approximately 250 listed potential predicate offences (FATF-GAFI 2006), although felony offences under US federal or state law, or foreign felony offences, may be predicate crimes.

The United States has both criminal and civil asset recovery legislation. Criminal assets recovery provisions, requiring a conviction for an offence, are contained in 18 USC 982. The civil assets recovery provisions are contained in 18 USC 981.

The Bank Secrecy Act is the central legislation for the money laundering regulatory system in the United States. The PATRIOT Act amended the Bank Secrecy Act in 2001 and substantially increased the regulatory requirements intended to prevent and detect money laundering in the United States. The PATRIOT Act, in addition to expanding the regulatory regime, also increased the penalties for money laundering offences.

Other significant Acts have shaped the regulatory regime in the United States. The *Annunzio-Wylie Anti-Money Laundering Act 1992* (Annunzio-Wylie Act) permitted the Secretary of the Treasury to require any financial institution to file a report of a suspicious transaction. This Act also required all businesses to keep customer identification records for all currency transactions between US$3,000 and US$10,000. The *Money Laundering Suppression Act 1994*, implemented in 1996, set out the requirement for banks, thrifts and credit unions to file reports of suspicious transactions to the FIU.

The Annunzio-Wylie Act criminalised the operation or ownership of an unlicensed money transmitting business. This provision is contained in 18 USC 1960 and also criminalises operating or owning of a business that knowingly transports or transmits funds derived from a criminal offence or funds intended to promote an unlawful activity.

US Sentencing Guidelines state that the fine imposed on regulated entities implicated in money laundering offences can be influenced by both the seriousness of the offence and organisation's culpability. Culpability can be diminished by a compliance program in accordance with the Bank Secrecy Act.

Terrorism financing legislation

There are four federal criminal offences that deal directly with the financing of terrorism or terrorist organisations:

- 18 USC 2339A—providing material support for the commission of offences specified;
- 18 USC 2339B—providing material support or resources to designated foreign terrorist organisations;
- 18 USC 2339C(a)—providing or collecting terrorist funds for a specified act; and
- 18 USC 2339C(c)—concealing or disguising either material support to foreign terrorist organisations or funds used, or intended to be used, for terrorist acts.

The United States, like Australia, has additional asset freezing legislation. Executive Order 13224, issued after the 11 September 2001 attacks, prohibits dealing with the assets of individuals and entities identified in the Order or those added to the Order by the Secretary of State, Secretary of Treasury, or the Attorney-General.

The PATRIOT Act, as noted above, was passed in the aftermath of the 11 September 2001 attacks. The amendments made to the Bank Secrecy Act by the PATRIOT Act, and the regulatory regime as a whole, is targeted jointly at the financing of terrorism and money laundering activities. The United States has focused some specific measures on the financing of terrorism in response to the 11 September 2001 attacks. The requirement to register all value transfer businesses with FinCEN is one such measure.

Financial intelligence unit

FinCEN, established in 1990 by the Department of Treasury, is the FIU in the United States. FinCEN receives reports from regulated entities and works on combining this information with other government and public information. The intelligence reports generated from this process are passed onto law enforcement agencies. FinCEN is an administrative

style FIU and does not have any law enforcement or prosecutorial powers. Like AUSTRAC in Australia, FinCEN is both an anti-money laundering regulator and the FIU in the United States. FinCEN employed 327 staff members in 2009 (FinCEN 2009b).

Regulated sector

The regulated sector in the United States is very large. Levi & Reuter (2006) describe the current United States prevention regime as having four areas. These are core financial institutions, non-core financial institutions, non-financial businesses and professions. As discussed above, the PATRIOT Act substantially expanded the AML/CTF requirements and one aspect of the expansion was to increase the industries covered by AML/CTF legislation.

The PATRIOT Act expanded the anti-money laundering program requirements to include broker-dealers, casinos, futures commission merchants, introducing brokers, commodity pool operators and commodity trading advisors. Informal value transfer systems (providers of remittance services) were also included in the definition of financial institutions (Gup 2006). The regime also includes dealers in precious metals, stones, or jewels.

The service providers identified as financial institutions under the Bank Secrecy Act are:

- banks (commercial banks, savings and loan associations, credit unions);
- federally regulated securities brokers;
- currency and exchange houses;
- funds transmitters;
- cheque-cashing businesses;
- persons subject to state or federal bank supervisory authorities;
- casinos and card clubs; and
- insurance companies offering selected products, such as life insurance, annuity contracts, property and casualty insurance, and health insurance.

Professions in the United States, such as legal practitioners, are not subject to preventive AML/CTF requirements. Members of the professions, however, may of course be prosecuted for any criminal involvement in the financing of terrorism and for assisting money laundering activities (Levi & Reuter 2006).

The third section of this report considers the regulated sector in a slightly different way to Levi and Reuter (2006) by dividing businesses with AML/CTF obligations into three categories—financial institutions, MSBs and non-financial businesses.

Obligations

Financial intelligence reports

The financial intelligence reports system of the United States is more complex than the Australian model. Different types of reporting entities are subject to different reporting requirements and different thresholds for each report type.

- Reports of suspicious financial activity—compulsory SARs are subject to a minimum threshold for the value of the transaction. The threshold for SARs for MSBs is US$2,000. For financial institutions, casinos and the futures and securities sector, the threshold is US$5,000. The transaction threshold increases to US$25,000 where a suspect cannot be identified.
- Reports of high-value cash transactions—financial institutions, casinos, trades and businesses must file Currency Transaction Reports (CTR) after engaging in a currency transaction of more than US$10,000. Some institutions, such as banks, can seek exceptions for filing CTRs for transactions with cash-intensive businesses for stated amounts and for specific time periods. Casinos are excluded from reporting payouts from slot machine jackpots and video lottery terminals.
- Reports of international movements of cash—businesses and individuals transporting, or arranging to transport, more than US$10,000 into or out of the United States must file a Report of International Transportation of Currency or Monetary Instruments.
- Reports of international movements of instruments of value—the transportation of more than US$10,000 in instruments of value into or out of the United States is subject to the same report as transporting cash.
- Reports of international electronic transactions—the United States does not require this kind of report.
- Additions—individuals with financial interests held overseas with an aggregate value of more than US$10,000 must submit a Report of Foreign Bank and Financial Accounts.

Tipping-off

Section 31 USC 5318 prohibits financial institutions, their employees, directors, officers and agents that have filed a SAR from disclosing this information to any person involved in the transaction. All government employees are also subject to the tipping-off provision, except where disclosure is part of their official duties. The Code of Federal Regulations (Chapter 12) states that SARs filed by banks are confidential and that any individual subpoenaed or otherwise requested to disclose any information about a SAR should refer to 31 USC 5318.

Compliance programs

The Bank Secrecy Act requires regulated entities to establish anti-money laundering programs that encompass, at a minimum:

- internal policies, procedures and controls;
- a compliance officer;
- ongoing training for staff; and
- independent auditing systems.

Different types of entities are subject to different specific anti-money laundering program requirements. The most stringent regulations apply to core financial institutions. Core financial institutions are required to have full anti-money laundering programs and are subject to additional regulations governing specific areas such as customer identification.

Non-core financial institutions have been progressively added to the anti-money laundering regime. MSBs are the largest sub-category of non-core financial institutions. MSBs must register with FinCEN before operating. The anti-money laundering program regulations for non-core financial service businesses, including money service providers, are less stringent than those for core financial services. MSBs are tasked with self-assessing their level of risk depending on their location and the specific services they provide.

The elements of an anti-money laundering program required by non-financial businesses are less specific although non-financial businesses do have some requirements such as identification checks and record-keeping. Compliance supervision and any practical use of sanctions is limited because most non-financial businesses are registered in state or local jurisdictions. Authorities have little leverage to punish non-compliance by non-financial businesses.

European Union

Money laundering legislation

The Directive 2005/60/EC of the European Parliament and the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (the Third Money Laundering Directive) is now the core of the EU's AML/CTF preventative measures. The purpose of the Third Money Laundering Directive is to ensure that European legislation complies with the revised FATF-GAFI 40 plus nine Recommendations. The current Directive replaces the 2001 Second Money Laundering Directive and amends the requirements to more fully comply with the revised FATF-GAFI Recommendations.

The Third Money Laundering Directive outlines the AML/CTF requirements for member states, although members must implement the Directive into domestic legislation. The expanded requirements include extending the AML/CTF regime to DNFBPs and targeting the financing of terrorism. The Third Money Laundering Directive also introduced significant change by requiring member states to implement a risk-based approach to money laundering prevention. Some countries, such as the United Kingdom, had risk-based systems in place prior to the Directive. The Directive was, however, the first attempt to allow regulated entities flexibility in assessing their own levels of risk (KPMG 2007).

The European Union's deadline for implementation was December 2007. The large changes many countries needed to instigate meant that implementation was realistically expected to be uneven (KPMG 2007).

The introduction of the Third Money Laundering Directive was met with heavy criticism. The European Union released the Directive in a climate where some member states had not fully implemented the reforms contained in the Second Money Laundering Directive of 2001. Criticism was also levelled at the European Union's release of the Third Money Laundering Directive ahead of evaluating the impact of the Second Money Laundering Directive reforms.

Further concerns arose from the Directive's inclusion of DNFBPs. Critics suggested that the regulated sector would comply with the reforms solely to avoid the costly legal consequences of non-compliance rather than to mitigate money laundering or the financing of terrorism. The consequences of approaching AML/CTF in this way was anticipated to result in defensive reporting, marked by a substantial increase in the number of financial intelligence reports submitted, but no gains in the quality of reports or information. Defensive reporting generates a backlog of intelligence, an increased workload for FIUs and other agencies created by superfluous reports, as well as less effective FIUs.

It is difficult to gauge the motivation for regulated businesses to comply with AML/CTF requirements from the data available in this report. Some Australian businesses, however, conceded that their compliance was to avoid penalties rather than from any perceived threats of money laundering or terrorism financing taking place in their businesses (Walters et al. forthcoming). The DNFBPs included in the regimes of the EU countries considered within this sample did not appear to engage in defensive reporting. Very few DNFBPs from within the sample filed any reports with the FIU or with regulators. The volume of reports the FIUs received overall did increase in most countries, although the number of reports in most cases had begun to increase years before the introduction of the Third Money Laundering Directive. The fourth section of this report considers compliance and report numbers in more detail.

In 2005, the Council of the European Union released Regulation (EC) No. 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the community. The Regulation requires member states to enact legislation to require any persons entering or leaving the European Union to declare movements of cash, currency, or bearer negotiable instruments valued at €10,000 or more. The regulation came into force on 15 June 2007.

The Regulation (EC) No. 1781/2006 on information on the payer accompanying the transfer of funds sets out the minimum payer identity information that must be sent with international funds transfers from member states.

Terrorism financing legislation

Alongside the Third Money Laundering Directive, the Council Regulation (EC) No. 881/2002 (United Nations Al Qaida and Taliban list) and Council Regulation (EC) No. 2580/2001 (European Union terrorism list) are also directly applicable in law in all member states (Howell 2007). The EU terrorism list was published at the end of 2001 and incorporated individuals are to be subjected to asset freezing mechanisms and prevented from engaging in business transactions (Neve et al. 2006). This list operates alongside the UN's Al Qaida and Taliban list.

United Kingdom

Anti-money laundering and counter-terrorism financing legislation

Recent estimates of the cost of all serious organised crime to the United Kingdom approximate £15b per year (SOCA 2008a). Trafficking Class A drugs was perceived to be the greatest threat in terms of organised crime and money laundering in 2008 (SOCA 2008a, 2008b). The United Kingdom was believed to be one of the most lucrative markets in the world for Class A drug smugglers (SOCA 2006).

Property purchases, cash-intensive businesses and front companies were the methods that SOCA believed to be the most commonly used to launder money in the United Kingdom (SOCA 2006). SOCA identified cash as the mainstay of serious criminal activity due to its flexibility and because it does not leave an audit trail.

Money laundering legislation

Money laundering is criminalised in the United Kingdom by the *Proceeds of Crime Act 2002* (UK) (POCA 2002 UK) as amended by the *Serious Organised Crime and Police Act 2005* (UK).

POCA 2002 UK states that a person commits an offence by concealing, disguising, converting, or transferring criminal property, or by removing criminal property from the United Kingdom. Entering into, or becoming concerned with, an arrangement known or suspected to facilitate the acquisition, retention, use, or control of criminal property by or on behalf

of another person is a separate offence in the United Kingdom. It is also an offence under this Act to acquire, use, or possess criminal property. Natural and legal persons may be convicted of a money laundering offence in the United Kingdom (FATF-GAFI 2007a).

The offences in POCA 2002 UK may apply to the perpetrator of a predicate offence or third parties. A money laundering conviction is not dependant on gaining a conviction for the predicate crime that generated the funds to be laundered.

The potential predicate offences for money laundering in the United Kingdom are not restricted to a list of specific crimes. All crimes committed in the United Kingdom, or acts committed in other jurisdictions considered criminal offence if they had occurred in the United Kingdom, are potentially predicate crimes. Criminal property is that constituting or representing any benefits derived from criminal conduct, in whole or part, either directly or indirectly (s 340 POCA 2002 UK).

Sections 330–332 create offences for persons failing to submit suspicious activity reports if the suspicion came about in the course of business in the regulated sector. Sections 330–331 apply to persons and nominated officers (individuals nominated to receive disclosures within a business) within the regulated sector. Section 332 applies to nominated officers in the non-regulated sectors who have an internal disclosure system under the risk-based approach. There are slightly different requirements with ss 331 and 332, where the first is suspicion based on reasonable grounds, whereas the second is a suspicion based in fact (Law Society UK 2008).

The United Kingdom also regulates money laundering through the Money Laundering Regulations. The 2003 regulations were recently amended in favour of the Money Laundering Regulations 2007 which were created to implement the EU's Third Money Laundering Directive (Law Society UK 2008). These regulations took effect in December 2007.

The United Kingdom has provisions for confiscating laundered property under POCA 2002 UK, the *Terrorism Act 2000* (UK) (Terrorism Act) and the *Anti-terrorism, Crime and Security Act 2001* (UK).

The confiscation regime includes both civil and criminal provisions. Criminal confiscation provisions are contained in POCA 2002 UK and the Terrorism Act.

The provisions in POCA 2002 UK allow for asset recovery providing the court shows the defendant is either:

- guilty of a lifestyle offence;
- has received a total of at least £5,000 in the course of criminal conduct; or
- has received a total of at least £5,000 from an offence occurring over at least six months.

The provisions for civil recovery are located in the *Anti-terrorism, Crime and Security Act 2001* (UK) and POCA 2002 UK. Assets can be seized under the *Anti-terrorism, Crime and Security Act 2001 (UK)* where there are reasonable grounds for suspecting they are linked to terrorist organisations or terrorist acts. POCA 2002 UK allows the civil recovery of assets of £10,000 or more without a conviction if prosecution has been attempted first and proven unsuccessful. Cash can only be recovered with this method if there are also other types of property involved.

The United Kingdom employs a risk-based approach to money laundering regulation for customer due diligence and ongoing monitoring of clients. The risk-based approach does not extend to suspicious activity reporting where specific obligations are defined (Law Society UK 2008). The Financial Services Authority (FSA) is the AML/CFT regulator for financial institutions. Ongoing regulation of the reporting entities in the United Kingdom is carried out under a risk-based approach based that employs an impact assessment based on the size of the entity and the number of customers (FATF-GAFI 2007a).

Terrorism financing legislation

Terrorism financing is criminalised under the Terrorism Act in Part III, ss 15–18 (FATF-GAFI 2007a). The offences are for raising funds, using and possessing terrorist property or money, creating funds arrangements and for money laundering. The *Anti-terrorism, Crime and Security Act 2001* (UK) amended the Terrorism Act provisions for freezing assets linked to terrorism activities.

The Al Qaida and Taliban (United Nations Measures) Order 2006 (UK) and the Terrorism (United Nations Measures) Order 2006 (UK) create offences for providing funds or economic resources to terrorists. A case in April 2008 (*A, K, M, Q and G v HM Treasury* [2008] EWHC 869 (Admin)) raised doubts about the lawfulness of asset freezing under these Orders. The case has gone to appeal to the House of Lords (Jones & Zgonec-Rože 2009).

Financial intelligence unit

The UK FIU is part of SOCA (SOCA 2008b). SOCA was established in April 2006 under the *Serious Organised Crime and Police Act 2005* (UK) (SOCPA) which amended POCA 2002 UK (SOCA 2007). SOCA replaced the National Criminal Intelligence Service (NCIS), the National Crime Squad (NCS), parts of Her Majesty's Revenue and Customs (HMRC) and the UK Immigration Service (UKIS) (SOCA 2006). SOCA is sponsored by the Home Office but operates independently.

The aim of SOCA is to prevent, detect and contribute to a reduction in serious organised crime and to gather, store, analyse and disseminate information on crime (SOCA 2008b). The top three priorities of SOCA are Class A drug trafficking, people smuggling and people trafficking, in that order (SOCA 2008b). SOCA employed over 4,000 staff in 2008–09 (SOCA 2009a).

Regulated sector

The United Kingdom employed over one million people in the financial services industry in 2007, which made it one of the largest commercial banking sectors in the world. The insurance industry was the largest in Europe and third largest in the world that year (FATF-GAFI 2007a).

POCA 2002 UK defines the regulated sector by services and not by types of businesses. The United Kingdom's regulated financial sector contains all of the financial activities defined by FATF-GAFI (FATF-GAFI 2007a). The Money Laundering Regulations 2007 expanded the boundaries of the regulated sector for DNFBPs to include auditors, accountants and tax advisors, independent legal practitioners, trust or company service providers, estate agents, high-value dealers and casinos (Law Society UK 2008). Legal practitioners are covered in POCA 2002 UK when they participate in selected financial and real estate transactions.

Obligations

Financial intelligence reports

The key difference between the financial intelligence reports required in the United Kingdom and those required in Australia is the absence of any requirement to report international electronic funds transfers.

- Reports of suspicious financial activity—all regulated entities are required to report all suspicions of money laundering. The requirement applies to transactions of any amount, as well as attempted transactions (FATF-GAFI 2007a). An exception applies to professional legal advisors if the information or suspicion arose in privileged circumstances. Privileged circumstances apply to information communicated in connection with providing legal advice to a client or in connection with legal proceedings. The exemption does not occur if the interaction is intended to further a criminal purpose (Law Society UK 2008).
- Reports of high-value cash transactions—the United Kingdom does not require reports of high-value cash transactions above a specific threshold. Businesses accepting €15,000 or more in physical currency, either as a single transaction or linked transactions, need to register with the Commissioners of HMRC but do not need to file cash transaction reports. A feasibility study conducted in 2006 concluded that the UK's anti-money laundering regime would remain suspicion-based rather than threshold-based (FATF-GAFI 2007a).
- Reports of international movements of cash—the United Kingdom has applied EU Council Regulation No. 1889/2005 (the European Union cash controls regulation) since June 2007. This regulation complements the previous disclosure rules that required all travellers entering and exiting the European Union to declare any currency and bearer negotiable instruments of €10,000 or more. The previous disclosure system required a verbal disclosure to customs officers rather than a formal written declaration. Those travelling within the European Union are still bound by the verbal disclosure system. The EU cash control regulation extends only to travel into or out of the European Union (FATF-GAFI 2007a).

- Reports of international movements of instruments of value—instruments of value are covered by the EU cash controls regulation outlined above.
- Reports of international electronic transactions—there is no specific requirement to submit a report to the FIU about electronic transactions. The transaction will only be the subject of a report if it fulfils the requirements for an STR.

Tipping-off

The United Kingdom has recently amended the tipping-off requirements and offences that apply to the regulated sector. Section 333 of POCA 2002 UK criminalises making a disclosure that might prejudice an investigation stemming from a report of a suspicious transaction. The maximum penalty for a conviction on indictment is 14 years imprisonment and a fine.

The defences to disclosing are also laid out in s 333 and apply to:

- disclosures within an undertaking or group, such as employees of the same firm;
- disclosures between institutions such as professional legal advisors;
- disclosures to supervisory authorities; and
- disclosures made by legal professionals to clients for the purpose of dissuading criminal conduct (Law Society UK 2008).

Section 342 contains further offences for making a disclosure that may prejudice criminal or civil confiscation proceedings or a money laundering investigation. The maximum penalty for this offence is imprisonment for five years and a fine. Legal practitioners have an exemption if the disclosure is in the process of giving legal advice or in connection to legal proceedings (Law Society UK 2008).

Anti-money laundering/counter-terrorism financing compliance programs

The Money Laundering Regulations 2007 require regulated entities to establish appropriate risk-sensitive policies and procedures for customer due diligence and ongoing monitoring, record-keeping, reporting, internal controls, risk assessment and management, and for monitoring compliance with these policies.

The Regulations require regulated businesses to train all relevant employees about money laundering and terrorism financing laws. Regulated entities must also provide regular training on recognising and responding to transactions that may be implicated in money laundering or the financing of terrorism.

Belgium

Belgium has a comprehensive anti-money laundering regime and a high rate of compliance with FATF-GAFI Recommendations. Forty-one out of 48 applicable Recommendations were marked as compliant or above in the most recent evaluation (FATF-GAFI 2005a). Belgium, despite its high level of compliance with the Recommendations, was identified as potentially vulnerable to money laundering through the informal financial sector due to the use of alternative remittance and the large diamond trade in the country used by the United States (US Department of State 2008).

The European Commission identified Belgium as one of 15 countries non-compliant with the Third Money Laundering Directive and initiated infringement measures in 2008 (Europa 2008). Belgium anticipated fully transposing the Third Money Laundering Directive into domestic law by November 2009 (European Commission 2009a, 2009b). The following information is based on the Belgian AML/CTF requirements prior to the full implementation of the Third Money Laundering Directive.

Anti-money laundering and counter-terrorism financing legislation

Money laundering legislation

Money laundering is criminalised in Belgium under Article 505 of the Penal Code. The offence is for laundering the proceeds of any crime.

The Law of 11 January 1993 is the central anti-money laundering legislation. The preventative requirements for regulated entities relating to specific predicate offences are contained in this Law. The legislation was most recently amended in 2007 and is expected to be amended again in line with the Third Money Laundering Directive.

This legislation focuses only on serious predicate offences, including terrorism or terrorist financing, organised crime, illicit trafficking, serious fraud and organised tax fraud, corruption, environmental crime and counterfeiting. The serious predicate crimes also extend to stockmarket-related offences, providing foreign exchange or fund transfer services without a licence, breach of trust, abuse of corporate assets, hostage taking, theft or extortion using violence or threats, or an offence related to the state of bankruptcy.

The Central Office for Seizure and Confiscation (COSC) monitors all asset freezing and confiscation in Belgium. FATF-GAFI (2005a) described Belgium's existing asset confiscation regime as sophisticated, although lacking clarity in some areas. Belgium was in the process of drafting new legislation at the time of the FATF-GAFI evaluation in 2005.

Counter-terrorism financing

Articles 140 and 141 of the Penal code criminalise participating in and financing terrorist groups (FATF-GAFI 2005a). The Penal Code defines participation in a terrorist group to include providing information, material resources or financing for an activity with the knowledge that participation contributes to the commission of a crime. Article 141 penalises the provision of material resources and includes financial aid (FATF-GAFI 2005a). The penalties for these offences range from five years to 10 years in prison. The Law of 11 January 1993 combines AML/CTF requirements for regulated entities.

Financial intelligence unit

The Cellule de Traitement des Informations Financieres (CTIF-CFI) was created in June 2003. It is classed as an administrative FIU (Schott 2004) that is independent and supervised by the Ministries of Justice and Finance. CTIF-CFI's main role is to receive, analyse and disseminate all disclosures from regulated entities. It operates as a filter between regulated entities and judicial authorities, reporting any possible money laundering to the public prosecutor.

CTIF-CFI, alongside its duties as FIU, also acts as the supervisory body for entities and professions not supervised by the Banking, Finance and Insurance Commission (CBFA) or other authorities (FATF-GAFI 2005a). Areas within the regulated sector are regulated by those agencies with the appropriate specialist knowledge of the respective sectors (eg the CBFA is responsible for financial institutions and the Gaming Commission is responsible for casinos) but CTIF-CFI nevertheless maintains a close relationship with all regulators. CTIF-CFI is an independent organisation with its own budget provided by the regulated sector.

The Belgian regime requires reporting entities to perform some analysis prior to submitting a disclosure to the FIU. This reduces the number of disclosures. CTIF-CFI argue the disclosures that are made are of a higher quality than if all matters were reported uncritically (CTIF-CFI 2006). Belgium has had an online disclosure system since 2006. As an additional power, CTIF-CFI has the authority to freeze bank accounts on a case-by-case basis, if there is sufficient evidence that money laundering has been committed. The FIU can suspend a transaction for up to two working days to complete analysis (FATF-GAFI 2005a).

Regulated sector

Belgium has a comprehensive list of regulated financial entities including the National Bank of Belgium and the Public Trustee Office (Caisse des Dépôts et Consignations). Entities and businesses engaged in banking, credit, investment, insurance, mortgage, lease-financing, currency exchange, derivatives, funds transport, real estate and dealing in diamonds are also covered. Professionals are also included in Belgium's anti-money laundering regime, including notaries, bailiffs, auditors, approved accountants, tax advisors and tax specialist-accountants, and gambling establishments and gaming halls (casinos). The regulations also apply to legal practitioners, but only when performing certain transactions to do with finances and real estate.

Major objections were lodged by the legal profession to the Third Money Laundering Directive. Indeed, the profession has a history of litigation in relation to both the Second and Third Directives. In 2005, the then Court of Arbitration in Belgium (now the Constitutional Court of Belgium) heard arguments promulgated by the French and German-speaking

Bar Association, Association of Flemish Bars and the French and Dutch Bar Association of Brussels to the effect that the duty to report imposed by the anti-money laundering legislation infringed the duty to maintain professional secrecy and impacted upon lawyers' independence. Such principles, the combined professional bodies maintained, were safeguarded by the Belgian Constitution and the Convention for the Protection of Human Rights and Fundamental Freedoms. In 2005, the Court of Arbitration referred to the European Court of Justice the question of whether the Second EU Directive, in including reporting obligations on lawyers, violated the right to a fair trial. The European Court of Justice issued its opinion on 26 June 2007 and held that the reporting obligations under the Directive applied to lawyers only insofar as they advised a client in the preparation or execution of certain transactions—essentially those of a financial nature or concerning real estate—or when they acted on behalf of and for a client in any financial or real estate transaction. Given that such activities generally occurred outside of judicial proceedings, there could be no impact upon whether the client received a fair trial. Undeterred, the Belgian Bar Associations launched a second challenge to the implementation of the Second Money Laundering Directive in November 2007 in the Belgian Constitutional Court.

The CTIF-CFI believes that there is active involvement of the legal profession in criminal activity in Belgium. Interestingly, the 2007 International Narcotics Control Strategy Report (INCSR) noted that in 2005 there were no suspicious transaction reports filed by the legal profession and in 2006 CTIF-CFI recorded (in its 2006 annual report) just two such reports. Although the legal profession in many jurisdictions has tended to fall behind other reporting entities, the rate in Belgium should give cause for concern. Interestingly, CTIF-CFI also notes that the real estate sector claims not to be aware of any significant money laundering issues pertaining to its sector, which might explain the fact that it posted only two suspicious transaction reports in 2006 (L Umans, CTIF-CFI personal communication 11 January 2008). Belgium requires regulated entities to obtain customer identification and verification based on a risk-profile.

Obligations

Financial intelligence reports

Belgium legislation requires the following approaches to financial intelligence reporting:

- Reports of suspicious financial activity—regulated financial entities are required to submit disclosures of any suspicious transactions to the FIU prior to conducting the transaction, or if this is not possible, the disclosure should be made immediately afterwards (Law of 11 January 1993 Article 12). The information may be provided by telephone but must be followed up by a written lodgement. Failure to report carries an administrative fine of between €250 and €1,250,000.
- Financial institutions, professions and casinos are also required to disclose any facts which they know or suspect to be linked to money laundering or terrorism financing (Law of 11 January 1993 Article 14, 14bis). Legal practitioners must also adhere to this requirement. Legal practitioners make reports to the President of the bar association of which they belong and not directly to the FIU. The President of the bar association can pass the information to the FIU. Legal practitioners are exempt from the requirement to submit reports if the information came to them in the course of ascertaining the legal position of their client, defending the client, or providing advice on instituting or avoiding legal proceedings (Article 14bis).
- An interesting addition to the regime in Belgium is the requirement for internal analysis to be conducted by the anti-money laundering compliance officer prior to submitting a disclosure (CTIF-CFI 2008).
- Reports of high-value cash transactions—Belgium law prohibits cash payments for real estate that are in excess of 10 percent of the total price of the sale or greater than €15,000. Cash payments are also illegal for any goods over €15,000 (The Law of 11 January 1993, chapter IIbis, Article 10bis and 10ter). While Belgium does not include high-value dealers (except diamond dealers) in the list of reporting entities, the illegality of cash payments over €15,000 makes their explicit

inclusion unnecessary. Regulated entities connected to the real estate sector who form a belief that this requirement is not being upheld must inform the FIU (The Law of 11 January 1993, article 10bis).

- Reports of international movements of cash—the regime in Belgium also covers transporting cash in and out of the European Union. On 15 June 2007, Belgium enacted the Royal Decree of 5 October 2006 which requires any currency coming into or out of the European Union worth more than €10,000 to be declared (CTIF-CFI 2006). If sums above this amount are not declared and the money is suspected to have illicit origins, a report is filed and the money may be confiscated for up to 14 days (CTIF-CFI 2006).
- Reports of international movements of instruments of value—bearer negotiable instruments are subjected to the same reporting requirements as cash in Belgium.
- Belgium has committed to cease issuing bearer bonds from 1 January 2008 as an additional preventative measure targeting bearer negotiable instruments. Bonds issued before this date will still be accepted along with foreign issued bonds (US Department of State 2008).
- Reports of international electronic transactions—The regulation (EC) No. 1781/2006 requires complete payer information to be sent with any transfers of funds outside the European community. Similarly, financial institutions conducting international electronic transfers of funds must retain information on the identity of the client (CTIF-CFI 2009). Under the regulation, transfers within the European Union only require account information unless they are deemed suspicious, when further information can be requested. There is no requirement to submit a specific report to the FIU with these regulations.

Tipping-off

Article 19 of the Law of 11 January 1993 contains the provisions for tipping-off. The law states that regulated entities may not inform their client or third parties that information has been transferred to the FIU or that an investigation is in progress. The offence carries an administrative fine of between €250 and €1,250,000.

Anti-money laundering/counter-terrorism financing compliance programs

Article 9 of the Law of 11 January 1993 directs regulated entities to train staff in money laundering preventative measures. Article 10 requires specified entities to appoint an individual responsible for implementing the preventative measures. In April 2007, CTIF-CFI produced a list of money laundering indicators, that is, a set of generic issues of which the relevant reporting entities ought to be aware. Thus, for example, financial professionals were advised to be wary of clients '...opening an account that is credited exclusively by cash deposits' (CTIF-CFI 2007b: 1), insurance companies were advised to be wary of '…a client concluding an insurance contract who is particularly interested in its early surrender and in the amount that he will then have at his disposal' (CTIF-CFI 2007b: 4) and real estate agents were advised to be wary of a client who '…buys real estate without having seen the property' (CTIF-CFI 2007b: 7). CTIF-CFI also sends relevant sections of the Belgian AML/CTF legislation (Law of 11 January 1993 on Preventing Use of the Financial System for Purposes of Laundering Money and Terrorism Financing [as amended] and Article 505 of the Penal Code) that apply to a specific sector. CTIF-CFI provides other guidance and undertakes training activities with the professional bodies (L Umans, CTIF-CFI personal communication 11 January 2008).

France

IMF (2005) considers France to be attractive to money launderers because of its stable economy and strong currency. It describes France's main vulnerabilities to money laundering as arising from the layering and integration stages rather than during the placement phases (IMF 2005).

France, like Belgium, has attracted infringement measures from the European Commission for failing to fully implement the Third Money Laundering Directive (Europa 2009). France had initiated full implementation of the Third Money Laundering Directive but not finalised doing so by October 2009 (European Commission 2009b).

Ordinance no. 2009–104 of 30 January 2009 implements the Third Money Laundering Directive into domestic French law. Full implementation of the Third Money Laundering Directive in France will be completed by a series of Decrees (IBA 2009).

Two administrative decrees expanded on the French AML/CTF requirements—Decree no. 2009–1087 on customer due diligence and reporting obligations for the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and the Order of the Minister of economy on the application of Article R. 561–12 of the Code Monétaire et Financier (Monetary and Financial Code)—were enacted in September 2009 (Financial Standards Foundation 2011). Decree no 2009–1087 further defines the know your customer requirements for beneficial owners, exempt clients and transactions, high-risk transactions and customers included an expanded definition of politically exposed persons and using identity information collected by third parties (Ashurst 2009).

Anti-money laundering and counter-terrorism financing legislation

Money laundering legislation

France has been a leader in the development and promotion of the FATF-GAFI 40 plus nine Recommendations since money laundering, tied to narcotics, was first criminalised in 1987 (IMF 2005). In 1997, France expanded the scope of predicate offences to include the proceeds of all crimes. The offences are laid out in articles 222–38 and 324–1 of the Criminal Code and Article 415 of the Customs Code and the law does not require the conviction of a predicate offence for a money laundering conviction (IMF 2005). The penalties for money laundering are laid out in article 324 of the Penal Code. Convictions for laundering the proceeds of drug trafficking crimes carry much larger penalties than those for laundering the proceeds of other types of predicate offences. Both natural persons and legal entities may be convicted of money laundering offences (IMF 2005).

The requirements for regulated entities to perform anti-money laundering measures are laid out in the Title VI of Book V of the Code Monétaire et Financier (Monetary and Financial Code) (Articles L561–1 to L–565–3). Entities are required to disclose all transactions and facts suspected to derive from drug trafficking, organised crime, defrauding the financial interests of the European community or corruption, or those that might be linked to terrorism financing (L562–2).

The Act of 11 February 2004 extended mandatory reporting to all legal counsel and created a new disciplinary authority for legal practitioners (Chevrier 2004). There was considerable debate surrounding the mandatory reporting for legal practitioners as required in the European Union Second Money Laundering Directive. The legal profession was opposed to the requirement and the possible breach of legal security (Chevrier 2004). Legal entities therefore have some unique requirements and leniencies in France.

The regime in France allows for, in theory, all seized assets to be confiscated. The measures generally apply only to those assets seized in the course of judicial procedure (IMF 2005). The measures are contained in the Code of Criminal procedure (IMF 2005).

Counter-terrorism financing

Terrorism financing is criminalised in Article 421–2–2 of the Criminal Code (IMF 2005). The terrorism financing preventative measures are contained in the Monetary and Financial Code (Articles L564–1 to L564–6).

Financial intelligence unit

France was one of the first countries to establish an FIU (IMF 2005) with TRACFIN created by the Act of 9 May 1990 (Chevrier 2004). It is a service of the French Ministry of Finance and is responsible for analysing the suspicious transaction reports received from reporting entities (IMF 2005).

In cases of non-compliance with AML obligations, sanctions are imposed by the supervisory authorities (Commission Bancaire, Commission de Contrôle des Assurances, Autorité des Marchés Financiers) and not by TRACFIN. A number of entities, however, including gaming houses and high-value dealers do not have a competent supervisory authority. The IMF, as such, considers anti-money laundering supervision to be underdeveloped in France.

Regulated sector

France has a comprehensive legal and institutional framework for regulated entities. Alongside financial institutions, reporting entities include real estate professionals, casinos and gaming houses, high-value dealers including precious stones and metals, art and antiques dealers, and legal and accounting professionals (IMF 2005; Article L562–1 of the Financial and Monetary Code). Legal practitioners and notaries have been required to report suspicious transactions since 1998 whenever they intervene in financial and real estate transactions (Chevrier 2004).

Obligations

Financial intelligence reports

French legislation requires regulated businesses and international travellers to take the following approaches to financial intelligence reporting:

- Reports of suspicious financial activity—French law requires reporting entities to submit two types of reports to the FIU. The first is an STR. The second type of report must be lodged when the identity of a beneficiary remains unknown after customer due diligence measures have been completed (IMF 2005; L562–2, L562–2–1). There are no size threshold limits for submitting either report. The reporting entity must submit the STR where there is a suspicion that the transaction is tied to drug trafficking, organised crime, fraud against the European Communities, corruption, or terrorism financing (IMF 2005). The reporting entity must submit the STR before the reportable transaction is completed unless the transaction cannot be prevented.
- There has been some disagreement over which suspected crimes must be reported. The French legislation creates a disparity between the predicate crimes criminalised for money laundering and those triggering a financial intelligence report. Suspicions of transactions tied to the more serious crimes, such as drug trafficking, terrorism and organised crime are widely accepted. The requirement to report transactions linked to less serious offences of lower level misappropriation of funds and tax evasion is sometimes disputed (Favarel-Garrigues, Godefroy & Lascoumes 2008).
- Legal practitioners are only required to submit reports when intervening in financial or real estate transactions for their clients. Legal practitioners must report all suspicious transactions to the Bar and the Bar determines whether there is cause to pass the investigation to the FIU (Chevrier 2004; IMF 2005). Legal practitioners are not required to make a report about a transaction if the practitioner came across the information in the course of representing the client in judicial proceedings, or in the course of giving legal advice, unless the contact serves money laundering purposes.
- Reports of high-value cash transactions—there is no requirement to systematically report large cash transactions, however, Article L–563–3 allows transactions above a threshold to be subjected to scrutiny and for the reporting entity to retain a record of this. At the time of the last IMF evaluation the threshold was €150,000 (IMF 2005).
- Reports of international movements of cash—under Regulation (EC) No. 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community and Articles 464 and 465 of the French Customs code, all persons entering and leaving the European Union must declare any sums, securities and assets valued at €10,000 or more. This includes cash, cheques, bearer cheques, travellers' cheques, bearer debt notes, growth bonds and transferrable securities.
- Reports of international movements of instruments of value—instruments of value are covered by the regulation described above.
- Reports of international electronic transactions—the Regulation (EC) No. 1781/2006 requires complete payer information to be sent with any transfers of funds outside the European community. This, however, is not a direct requirement to submit a report to the FIU. Under this regulation, transfers within the European Union only require account information, unless they are deemed suspicious, and then further information can be requested. Article L562–2 allows the authority to require reports of transaction over a specified threshold if they involve countries deemed to be inadequate in the fight against money laundering.

Tipping-off

Executives and agents of regulated entities are not permitted to advise the party to a transaction of the existence of a declaration under article L574–1 of the Monetary and Financial Code. A breach of this provision carries a penalty of a fine of €22,500. An important exemption to this applies to legal practitioners who are permitted to reveal the existence of a report on their activities to a client.

Anti-money laundering and counter-terrorism financing compliance programs

The Article 6 of Decree 91–160 of 13 February 1991 requires all financial entities to adopt written rules defining the procedures for anti-money laundering and for all staff involved in anti-money laundering to be kept informed and to receive training (IMF 2005).

Germany

The European Union initiated infringement procedures against Germany for its failure to meet the 15 December 2007 implementation deadline for the Third Money Laundering Directive (Europa 2008). Germany narrowly avoided attending the European Court of Justice for the late implementation.

Anti-money laundering and counter-terrorism financing legislation

Money laundering legislation

Germany's money laundering criminal offences were added to the German Criminal Code (Article 261) by the Act on Suppression of Illegal Drug Trafficking and other Manifestations of Organised Crime. Article 261 of the German Criminal Code has been amended several times to increase the scope of predicate offences. Predicate crimes for money laundering offences in Germany are listed in Article 261. German predicate crimes encompass all serious criminal offences, defined as those with a minimum sentence of one year's imprisonment and specified less serious offences. The less serious offences included come from the German Criminal Code, Narcotics Law and Precursors Law, and the Fiscal Code and other financial regulation. Specific offences from the Residence Act and Asylum Procedure Law, where committed by a terrorist or criminal organisation, and others from the Fiscal Code, where committed by a gang or on a commercial basis, are also predicate crimes.

The available penalty for money laundering convictions is three months to five years imprisonment. Money laundering offences tied to tax evasion (predicate crimes specified from the Fiscal Code) may carry penalties from six months to 10 years imprisonment if the perpetrator acts professionally or as a member of a gang that has formed to continually commit money laundering offences.

Germany's forfeiture and confiscation provisions apply to property used in, or derived from, criminal offences and property intended for the commission or preparation of a criminal offence (IMF 2004). The provisions extend to all property belonging to criminal organisations and not just to property directly connected to criminal offences. The confiscation regime applies, in principle, to all criminal profits belonging to criminal organisations even if individual acts cannot be identified (IMF 2004).

The *Act on the Detection of Proceeds from Serious Crimes* (the Germany Money Laundering Act) is the central preventative legislation in Germany.

Counter-terrorism financing legislation

Terrorism financing is criminalised under ss 129a–129b of the German Criminal Code. The offences are termed as providing support to a terrorist group rather than a specific offence for the financing of terrorism (Neve et al. 2006). A conviction for providing support to a terrorist organisation carries penalties from between six months and 10 years imprisonment.

Germany, unlike Australia, does not predefine or list terrorist organisations. In each case, the organisation in question must be demonstrated, at trial, to fit the definition of a terrorist organisation. Section 129a also defines a terrorist organisation as one with activities directed towards murder in aggravated circumstances, genocide, crimes against humanity, war crimes, or crimes against personal liberty. Organisations that aim to cause physical or

psychological harm to individuals, to commit offences endangering the public, to commit some specific environmental offences, or to commit offences under the *Weapons Act* or the *Weapons of War (Control) Act* are also terrorist organisations in Germany.

Financial intelligence unit

FIU Germany is a single, centralised body within the Federal Office of Criminal Investigation (BKA; US Department of State 2008). BKA is the central office for police information and a subordinate agency of the Federal Ministry of the Interior (BKA 2006b). FIU Germany was established in August 2002 and later moved into BKA. The functions of FIU Germany are set out in the Germany Money Laundering Act.

FIU Germany is a law enforcement style FIU and is staffed by law enforcement personnel. The role of the FIU is to collect and analyse suspicious transaction reports and check these against the data stored by other offices and report these to prosecuting authorities. The FIU's position within BKA means the FIU has access to numerous sources of information for analysis (IMF 2004). FIU Germany also provides information and resources to reporting entities in Germany.

BKA, in additional to housing FIU Germany, also contains a joint financial investigation task force. BKA can carry out investigations and law enforcement operations for money laundering and international terrorism offences. The Landerkriminalamt (state police forces) also conduct investigations and prosecute money laundering offences in Germany (Peters nd).

Regulated sector

Several financial regulators merged into the German Financial Supervisory Authority (BaFIN) in 2002 (IMF 2004). BaFin is responsible for implementing the MLA with regard to most credit and financial services institutions and insurance companies. Alongside these, BaFin supervises money remittance services, currency exchange and credit card businesses. The supervision of these additional businesses represents a unique component of the German anti-money laundering system (IMF 2004).

Aside from credit institutions, financial services with AML/CTF obligations also include investment, trading and portfolio companies and brokers, as well as money transmitters and currency dealers and non-European Economic Area deposit brokers.

The Germany Money Laundering Act (s 3) includes auditors, accountants, tax advisors, tax agents, real estate agents, casinos and persons trading in goods in the regulated sector in Germany. Legal advisors, and other registered persons in the Legal Services Act (Rechtsdienstleistungsgesetz), have AML/CTF obligations when assisting in the planning or execution of transactions for clients that encompass:

- buying and selling real property or business entities;
- managing client money, securities, or other assets;
- opening or managing bank, savings, or securities accounts;
- procuring funds to create, operate, or manage companies;
- creating, operating, or managing trusts, companies and similar structures; and
- any other financial or real estate transaction.

Trust and company service providers, not already regulated for another service, have AML/CTF obligations when:

- creating a legal person or partnership;
- acting as a director or manager or a legal person or partnership, a partner of a partnership, or a similar role;
- providing a registered office, business address, mailing or administrative address, or a related service for a company, partnership, or other legal person;
- acting as a trustee of a legal arrangement;
- acting as a nominee shareholder for another person other than a listed company; and
- arranging for another person to act in the functions of director, trustee, or nominee shareholder in the same circumstances.

Obligations

Financial intelligence reports

German legislation requires regulated businesses to submit the following types of financial intelligence reports:

- Reports of suspicious financial activity—all reporting entities, including individuals, are obligated to report any suspicion of a money laundering or terrorism financing offence to the competent authority with a copy sent to the FIU. There is no threshold limit on reporting suspicious transactions in Germany. Reporting entities may make an STR verbally over the phone, although a written report must follow.
- Regulated entities may not complete a transaction subject to an STR without prior consent from the public prosecutor's office or before the end of the second working day after submitting the report. Reported transactions completed outside of these conditions are prohibited transactions under the Code of Criminal Procedure. Reporting entities may complete the transaction where preventing it is impossible or if delaying the transaction would inhibit an investigation.
- Legal practitioners are required to report suspicions to the competent federal professional chamber but are exempt from this requirement if the information was obtained in the course of legal advice or representing a client. Section 11 of the Money Laundering Act, however, retains legal practitioners' obligation to report if they are aware that the client deliberately uses their legal advice for money laundering.
- At the time of the last IMF evaluation of Germany, failing to comply with an obligation to report suspicious transactions did not incur a criminal penalty, although serious breaches could result in administrative sanctions (IMF 2004).
- Reports of high-value cash transactions—at the time of the most recent IMF evaluation, Germany had no systematic reporting requirement for high-value transactions (IMF 2004). Section 2 of the Money Laundering Act requires persons trading in goods to obtain customer identification prior to conducting any transactions in cash or precious metals valued at €15,000 or more. All other reporting entities are required to conduct due diligence for all transactions, singularly or where multiple transaction appear to be linked and amount to €15,000 or more.
- Reports of international movements of cash—Germany, as of 15 June 2007, requires travellers to declare to the German Customs Service in writing all cash and equivalent instruments exceeding €10,000 in value when crossing the border to or from a non-European Union country. This is in line with the European Union directive on cross-border transportation of cash.
- Reports of international movements of instruments of value—the requirement above covers bearer negotiable instruments.
- Reports of international electronic transactions—the Regulation (EC) No. 1781/2006 requires complete payer information to be sent with any transfers of funds outside the European community, however, this is not a direct requirement to submit a report to the FIU. Transfers within the European Union only require account information unless they are deemed suspicious and then further information can be requested.

Tipping-off

Section 12 of the Money Laundering Act prohibits informing the customer or third party of the existence of an STR. Tipping-off carries an administrative sanction of up to €50,000 (IMF 2004).

Anti-money laundering/counter-terrorism financing compliance programs

Section 9 of the Money Laundering Act requires reporting entities to take safeguards against being used for money laundering. Reporting entities must designate a compliance officer, develop internal principles and controls to prevent money laundering, ensure employees who deal with financial transactions are trustworthy and provide regular information to employees about money laundering and obligations under the Money Laundering Act.

Asia

The Department of State (United States) suggested that the primary sources of the funds laundered in Hong Kong are generated by financial crimes such

as corruption, tax evasion, fraud, illegal gambling and bookmaking, prostitution, loan sharking, commercial crimes and intellectual property rights infringement. This list of predicate offences for the funds laundered in Hong Kong is quite different from the narcotics trafficking origin of the funds laundered in European countries (US Department of State 2008).

Hong Kong

Anti-money laundering and counter-terrorism financing legislation

Money laundering legislation

The principal legislation enacted to combat money laundering in Hong Kong is Drug Trafficking (Recovery of Proceeds) Ordinance (Cap 405) (DTROP) and Organised and Serious Crimes Ordinance (Cap 455) (OSCO). DTROP and OSCO are collectively known as the Ordinances. Hong Kong, through the Ordinances, specifically criminalises laundering funds from drug trafficking offences as well as any proceeds from an indictable crime.

Section 25(1) of DTROP states that any person who deals with property knowing, or with reasonable grounds to believe, that the property directly or indirectly represents the proceeds of drug trafficking is guilty of an offence. The maximum penalty available for conviction on indictment is a HK$5,000,000 fine and 14 years imprisonment. The maximum penalty for a summary offence is a fine of HK$500,000 and imprisonment for three years.

Section 25(1) of OSCO replicates the offence set out in s 25(1) of DTROP but extends it to criminalise dealing with the proceeds of any indictable offence. Money laundering offences under OSCO carry the same maximum penalties for indictable and summary convictions as the money laundering offence under DTROP.

DTROP and OSCO money laundering offences use a list-based approach to predicate crimes for money laundering, although the inclusion of all indictable offences under OSCO provisions provides an extensive list. The potential predicate offences also extend to acts committed overseas that would constitute an indictable offence if committed in Hong Kong.

DTROP and OSCO Ordinances share the same definition of 'dealing with' the proceeds of proscribed offences. Each Ordinance criminalises acquiring, concealing, disguising, disposing of or converting, bringing into or removing from Hong Kong, or using the proceeds of the predicate offences as security.

Asset recovery mechanisms

OSCO also contains Hong Kong's central asset recovery provisions. Hong Kong's asset recovery system has both criminal and civil elements. Asset confiscation is permitted for the offences specified in Schedule 1 of OSCO, for organised crime offences and for the proceeds generated from any crime where they are worth at least HK$100,000.

Asset recovery may take place where a defendant has been convicted of an appropriate offence or where the proceedings have not been completed because the defendant has died or absconded. The Hong Kong system, in this respect, is a criminal one. Questions arising about the benefits gained from a specified offence, whether that offence constitutes organised crime, and the amount of funds gained, are to be answered on the balance of probabilities. This introduces some elements of civil proceedings.

The Prevention of Bribery Ordinance (Cap 201) (s 10) (POBO) contains unexplained wealth provisions for current and former prescribed officers. Prescribed officers are those holding an office under the government, officials appointed under the Basic Law, s 5A of the Exchange Fund Ordinance (Cap 66), the Chair of the Public Service Commission, all staff of the Independent Commission against Corruption and any staff member of the judiciary.

POBO creates an offence for any prescribed officer to maintain a standard of living, or to hold assets, beyond that consistent with current or previous appointments where the officer is unable to account for the wealth in question. A conviction for unexplained wealth may be followed by an order to confiscate the property involved.

Key preventative legislation

The Ordinances also outline the money laundering preventative framework in Hong Kong. OSCO and DTROP contain basic provisions for reporting funds

suspected to be the proceeds of crime and basic customer identification requirements. All persons in Hong Kong, legal and natural, are obligated to report suspicious transactions under DTROP and OSCO. Prevention and detection regulatory controls in Hong Kong are predominantly found in guidelines released by Hong Kong's three prudential regulators.

The Hong Kong Monetary Authority supervises banks and other authorised deposit taking institutions. The AML/CTF controls for authorised deposit taking institutions are found in the Hong Kong Monetary Authority's *Guideline on the Prevention of Money Laundering*, issued in 1997 and the 2006 Supplement to the *Guideline on Prevention of Money Laundering*. The Supplement was superseded by the 2007 Supplement in May 2008.

The Office of the Commissioner of Insurance's (OCI) *Guidance Note on the Prevention of Money Laundering and Terrorist Financing* regulates all insurance companies that are not also authorised deposit-taking institutions. The Hong Kong Securities and Futures Commission also released the *Prevention of Money Laundering and Terrorist Financing Guidance Note* predominantly for companies licensed under the Securities and Futures Commission. The Joint Financial Intelligence Unit (JFIUHK) issued the *Guideline for Remittance Agents and Money Changers* in 2007.

The regulatory guidelines do not direct entities to perform self-assessments of money laundering and terrorism financing risks. The guidelines released by each regulator are uniform for all of the businesses covered by each specific regulator.

The Guidelines issued by the three prudential regulators of Hong Kong are predominantly considered enforceable by FATF-GAFI standards. The guidelines for MSBs issued by JFIUHK were not considered enforceable means by the FATF-GAFI in 2008. Some designated non-financial businesses are also subject to AML/CTF rules. Few of these, however, are enforceable.

The Hong Kong Institute of Certified Public Accountants (HKICPA) has issued guidelines for members, highlighting aspects of FATF-GAFI requirements. The guidelines, however, are not enforceable although HKICPA is able to enforce some due diligence and record-keeping requirements present in the Hong Kong Standard on Quality Control 1, Code of Ethics for Professional Accountants and Hong Kong Standards of Auditing.

Real estate agents are obligated to comply with some customer due diligence and record-keeping requirements through the Estate Agents Practice (General Duties and Hong Kong Residential Properties) Regulation and the Practice Circular (issued by the Estate Agents Authority).

The legal profession is subject to basic customer due diligence, record keeping and training requirements established in the Law Society Circular 07–726.

Trust and company service providers that are also members of the Hong Kong Institute of Chartered Secretaries will be subject to the AML/CTF requirements due to be incorporated into the Code of Conduct.

Counter-terrorism financing legislation

Hong Kong criminalises the financing of terrorism in United Nations (Anti-Terrorism) Ordinance (Cap 575) (UNATMO). Section 7 of UNATMO criminalises providing or collecting funds with the intention of using them to commit a terrorist act or knowing that they will be used for a terrorist act. Section 8 criminalises making funds or financial services available to, or available for the benefit of, a person known or reasonably suspected of being a terrorist or a terrorist associate.

UNATMO is also the key legislation for freezing assets linked to terrorism. Section 6 allows the Secretary for Justice to issue a freezing order on any funds reasonably suspected to be the property of a terrorist or terrorist associate, intended to assist in the commission of a terrorist act, or that were used in the commission of a terrorist act. In s 13 of UNATMO, which permits the confiscation of terrorist property, the definition is expanded to include any funds derived from a terrorist act.

UNATMO is also the key Ordinance for prevention and detection measures for the financing of terrorism. Section 12 obligates all individuals to report any knowledge or suspicion of terrorist property to an authorised officer. Failure to do so is an offence.

Financial intelligence unit

Hong Kong's FIU, JFIUHK, created in 1989, is operated by officers from Hong Kong Police and Hong Kong Customs. JFIUHK most closely resembles an administrative style FIU as its core functions are the analysis and dissemination of information. It does not conduct investigations. Investigations are conducted by units within the Hong Kong Police Force and the Hong Kong Customs and Excise Department. JFIUHK also refers all cases to law enforcement agencies such as Narcotics Bureau, the Organized Crime and Triad Bureau of the Hong Kong Police Force, the Customs Drug Investigation Bureau of the Hong Kong Customs and Excise Department, and the Independent Commission against Corruption, as well as some regulatory bodies.

Regulated sector

Hong Kong's regulated sector encompasses the banking and finance sectors (including banks, deposit taking companies, insurance companies and insurance intermediaries, and money lenders), securities and futures companies, and real estate agents. Legal practitioners have obligations issued by the Law Society. These, however, are not considered enforceable by FATF-GAFI. Accountants (that are members of HKICPA) are subject to some obligations, although the FATF-GAFI does not consider these enforceable means either.

Obligations

Financial intelligence reports

The financial intelligence reporting regime in Hong Kong has some significant differences to those of Australia and the United States:

- Reports of suspicious financial activity—all individuals, not just reporting entities, have a legal obligation to report funds suspected to the be the proceeds of, used in connection with, or intended to be used in connection with an indictable offence to an authorised officer. To fail to do so is an offence. All individuals have the same obligation to report suspicions of terrorist property.
- Reports of high-value cash transactions—Hong Kong does not require reports of high-value cash transactions.
- Reports of international movements of cash—Hong Kong does not require reports of international movements of cash.
- Reports of international movements of instruments of value—Hong Kong does not require reports of international movements of instruments of value.
- Reports of international electronic transactions—Hong Kong does not have a general requirement to report international electronic transactions. Remittance service providers and money exchangers, however, must record details of any transaction with the value of HK$8,000 or more (or foreign currency equivalent).

Tipping-off

Hong Kong's Ordinances contain tipping-off provisions. UNATMO (s 12) contains tipping-off provisions for reports of known or suspected terrorist property, stating that any disclosure that might prejudice an investigation is an offence. Section 26 of OSCO contains similar provisions. It disallows the disclosure in criminal and civil proceedings, publishing, or broadcasting the details of any reports made. Section 26 of DTROP has similar provisions for reports filed in compliance with this Ordinance.

Anti-money laundering/counter-terrorism financing compliance programs

The guidelines released by the prudential supervisory bodies outline detailed compliance program requirements. The Hong Kong Monetary Authority's guidelines direct entities proscribe:

- statements of internal AML/CTF policies;
- customer identification, account opening procedures and ongoing due diligence;
- record keeping;
- appointment of a compliance officer;
- remittance transactions procedures;
- recognition and reporting of suspicious transactions; and
- staff training.

The guidelines released by the OCI and the Securities and Futures Commission also contain these common aspects. Hong Kong does not have a system of compliance reporting, as Australia does,

in order to monitor the compliance programs of regulated entities. The regulatory bodies responsible for each industry may apply administrative and other sanctions for non-compliance with the requirements. The Estate Agents Authority, HKICPA and the Law Society of Hong Kong, have also issued AML/CTF compliance program guidelines.

Singapore

Anti-money laundering and counter-terrorism financing legislation

Money laundering legislation

The principal legislation enacted to combat money laundering in Singapore is the Corruption, *Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act* (Cap 65A) (CDSA). CDSA criminalises eight specific money laundering offences. Four of the eight possible money laundering offences (ss 46(1), 46(2), 46(3), 43(1)) are for self-laundering, professional laundering and possession of the proceeds of drug trafficking offences. The remaining offences are for the self-laundering, professional laundering, or possession of the proceeds of criminal conduct (ss 47(1), 47(2), 47(3), 44(1)).

CDSA defines criminal conduct as a serious offence, a serious offence in another jurisdiction, or the retention, control, acquisition, use, possession, concealment, disguise, conversion, or transfer of the benefits or funds derived from the benefits of a serious offence. In short, criminal conduct can be a serious offence or receiving or laundering the proceeds of a serious offence. CDSA specifically lists the crimes considered to be serious offences in the Second Schedule. These currently number 356 and include terrorism activities. The First Schedule lists an additional six offences that constitute drug trafficking in Singapore.

Singapore increased the maximum penalty for money laundering in September 2007 with the amendments of CDSA. The maximum penalties were increased to fines of SGD$500,000 or to imprisonment for a term of seven years, or both, for an individual offender while the fine for legal persons was increased to SGD$1m.

Asset recovery mechanisms

CDSA has also Singapore's provisions for the criminal confiscation of the proceeds of crime for drug trafficking offences (s 4) and serious offences (s 5) (as listed by the Second Schedule). CDSA's asset recovery provisions are criminal provisions. Proceedings can be commenced after the conviction of an offender, although CDSA does not require the defendant to be convicted of the criminal activity generating the funds.

Each of ss 4–5 allow the value of the assets subjected to a confiscation order to be determined using an unexplained wealth approach. CDSA states that any expenditure (s 5(7)) or wealth (s 5(6)) that cannot be lawfully accounted for is presumed to be the proceeds of crime although, as noted above, the defendant must be convicted of a serious offence for an application for a recovery order to be made. Singapore does not have civil asset recovery mechanisms for offences outside of some terrorism offences.

Key preventative legislation

Singapore's regulatory regime uses legislation, regulations and notices to establish the prevention and detection requirements. The notices, which are enforceable mechanisms, contain the most detailed level of legal requirements.

The Monetary Authority of Singapore is the regulator for the financial services sector, including money exchangers and remittance businesses, and issues the bulk of regulation in these sectors. AML/CTF regulation currently extends to financial services businesses regulated by the Monetary Authority of Singapore and to legal practitioners. The Singaporean AML/CTF system is a risk-based one and, as a consequence, each industry is subject to industry-specific notices and regulations directing regulated entities to apply different standards for high-risk transactions and customers. The Institute of Certified Public Accountants of Singapore is the regulating body for approved trustees.

The Law Society of Singapore is the issuing body for AML/CTF requirements for legal practitioners. Legal practitioners are subject to the Legal Profession (Professional Conduct) Rules.

Terrorism financing legislation

Singapore has four offences for the financing of terrorism in the *Terrorism (Suppression of Financing) Act* (TSOFA) (Cap 325). The offences are providing or collecting property for terrorist acts (s 3), providing property for terrorist purposes (s 4) and using or having property for terrorist purposes (s 5).

TSOFA provides additional asset confiscation measures for the property of terrorists and terrorist entities. Unlike the asset confiscation measures in CDSA, available for serious offences, TSOFA's asset confiscation mechanisms are available based on evidence on the balance of probabilities.

The AML/CTF regulatory system in Singapore is complemented with additional provisions specifically targeted at the prevention and detection of the financing of terrorism. Section 8 of TSOFA requires all persons in Singapore, and Singaporean citizens outside Singapore, to report the possession, custody, or control of assets belonging to a terrorist or terrorist organisation. Section 8 also requires all persons in Singapore and Singaporean citizens to report any information on a transaction or proposed transaction using such property to the Commissioner of Police. All persons are also required to periodically assess whether they are in control of property that may belong to a terrorist or terrorist organisation (s 9) and to provide any information that may prevent a terrorism financing offence or facilitate the detection or prosecution of a terrorism financing offence (s 10).

Financial intelligence unit

The FIU in Singapore is the Suspicious Transaction Reporting Office (STRO) which was established in 2000. STRO is part of the Financial Investigation Division of the Commercial Affairs Department of the Singapore Police Force. STRO has elements of an enforcement style FIU, as it is located within the Singapore Police Force and those of an administrative style FIU as it receives, analyses and disseminates financial intelligence reports and passes on the intelligence to law enforcement or regulatory agencies.

Regulated sector

The regulated sector in Singapore, as noted above, is almost entirely comprised of entities regulated as financial services businesses by the Monetary Authority of Singapore. A non-exhaustive list of the financial sector includes banks, finance companies, finance companies, capital markets services licensees, financial advisors, life insurers, trust companies, money changers and remittance providers, and approved trustees. Commodities futures brokers were expected to be regulated from 2008 (FATF-GAFI 2008a) although this had yet taken place as of mid 2009. Legal practitioners and casinos are currently the only non-financial service providers regulated for AML/CTF in Singapore. Singapore has two casinos which are supervised by the Casino Regulatory Authority. The Casino Regulatory Authority has issued regulations for AML/CTF controls.

Obligations

Financial intelligence reports

Singapore legislation differs from that in other countries by requiring individuals as well as regulated businesses to report suspicious transactions.

- Reports of suspicious financial activity—all regulated entities are required to submit STRs to STRO. Financial institutions must also provide a copy of the report to the Monetary Authority of Singapore. Every person in Singapore, not just regulated entities, is required to report transactions suspected to be linked to the financing of terrorism. These, however, go to the Commissioner Police rather than to the FIU.
- Reports of high-value cash transactions—there are no separate report requirements for large cash transactions. These, however, are likely to be the subject of STRs.
- Reports of international movements of cash—moving in excess of SGD$30,000 (or foreign equivalent) of cash into or out of Singapore triggers a reporting requirement.
- Reports of international movements of instruments of value—movements of bearer negotiable instruments with SGD$30,000 of value or more are subject to the same report as physical currency.

- Reports of international electronic transactions—Singapore does not require regulated entities to report the electronic movement of funds into or out of Singapore.

Tipping-off

Singapore's CDSA contains tipping-off provisions. Where an individual knows or has reasonable grounds to suspect that an investigation is proposed or currently underway, s 48(1) criminalises the disclosure of any information to any person that might prejudice that investigation. Section 48(2) criminalises disclosing information regarding a report made under CDSA to any other person that will prejudice an investigation. Singapore's tipping-off provisions exempt legal practitioners (s 48(3)) from these two offences if the disclosure is made to a client, as their advocate, or other person in the course of legal proceedings. The exemption does not apply if the disclosure is intended to further an illegal purpose.

Anti-money laundering/counter-terrorism financing compliance programs

The Monetary Authority of Singapore's Notices establish the compliance program requirements for regulated financial services businesses. Financial services businesses must nominate a compliance officer and establish an independent auditing system to ensure ongoing compliance with the requirements. The Monetary Authority of Singapore, in line with other countries, requires businesses to have internal policy statements for AML/CTF, establish customer due diligence procedures, establish record keeping systems and provide staff training. Unlike AUSTRAC in Australia, the Monetary Authority of Singapore does not require businesses to submit annual compliance reports. The Monetary Authority of Singapore does, however, conduct auditing, off-site surveillance and onsite visits.

Additional practice directions supplement the Law Society of Singapore's Legal Profession (Professional Conduct) Rules. The compliance program requirements for legal practitioners include measures for risk-based customer due diligence, staff training and record-keeping requirements. The Law Society of Singapore has the power to conduct inspections.

Republic of China (Taiwan)

Money laundering

Economic crimes are regarded as the most serious threat for money laundering in Taiwan followed by corruption and drug-related crimes (APG 2007).

Anti-money laundering and counter-terrorism financing legislation

Money laundering legislation

The principal legislation enacted to combat money laundering in Taiwan is the *Money Laundering Control Act* (MLCA Taiwan), enacted in 1996, and most recently amended in July 2007. Article 2 defines money laundering as knowingly disguising or concealing property obtained from committing a serious crime or obtained by a serious crime committed by another person. MCLA Taiwan defines a serious crime as:

- any offence carrying a minimum punishment of five years imprisonment;
- where the commission of specified offences generates proceeds valued at NT$5 or more; and
- other offences identified on a prescribed list.

Asset recovery mechanisms

Taiwan has provisions for freezing, seizing and confiscating of proceeds of crime. Several Acts contain the asset recovery provisions although MLCA Taiwan is the primary source. MLCA Taiwan allows property obtained in the commission of an offence to be confiscated or, where the property cannot be confiscated, the value of the property to be made as a payment. These provisions, and others in the Criminal Code allowing the confiscation of proceeds taken as a bribe or property used in the commission of an offence, are conviction-based. There are no civil confiscation measures in Taiwan.

Key preventative legislation

The anti-money laundering prevention and detection system in Taiwan is based around MLCA Taiwan. MLCA Taiwan contains specific AML/CTF requirements for the regulated sector as well as requiring financial institutions to establish their own

anti-money laundering procedures (Article 6). MLCA Taiwan itself contains the requirements for some customer identification, record keeping and the submission of reports to the FIU.

In response to Article 6, industry associations and bodies have published *Money Laundering Prevention Guidelines and Procedures* specifically targeting each industry within the regulated sector. There are regulations that have been issued in accordance with Acts other than MLCA that also contain requirements for AML/CTF-related areas. The result is that the prevention and detection system of Taiwan is spread across multiple areas, some more clearly legally binding than others, with different aspects and standards applied to different industries.

The industry associations that have published AML/CTF guidelines are:

- Bankers' Association;
- Securities Investment Trust and Consulting Association;
- Trust Association;
- Taiwan Securities Association;
- China National Futures Association;
- Life Insurance Association; and
- Non-life Insurance Association.

The Taiwan system has aspects of a risk-based approach as certain customers, such as non-residents and those handling high-value transactions, warrant enhanced due diligence measures.

Counter-terrorism financing

Taiwan has not yet criminalised the financing of terrorism. The Asia-Pacific Group on Money Laundering (2007) noted that Taiwan had drafted a Counter-Terrorism Bill that had not been tabled in parliament as of 2007. Taiwan has not indicated that the draft bill has been enacted. Taiwan also does not have any specific measures to recover or freeze any assets suspected to be involved in the financing of terrorism.

The regulatory regime of Taiwan does contain some references to funds intended for terrorism activities or entities. The *Money Laundering Prevention Guidelines* for each sector direct businesses to submit a report of a suspicious transaction for any activity suspected to be related to a terrorist or terrorist entity. The Bankers Association additionally directs organisations to apply extraordinary due diligence to customers and transactions that may be linked to terrorists or terrorist organisations (APG 2007).

Financial intelligence unit

The FIU in Taiwan is the MLPC that exists under the Investigation Bureau, Ministry of Justice, Republic of China (MJIB). MLPC was established in 1997 and receives financial intelligence reports, undertakes analyses, disseminates intelligence and assists the investigation of money laundering and terrorism financing cases. MLPC is a law enforcement model FIU.

Regulated sector

The regulated sector of Taiwan consists of financial institutions, as defined in Article 5 of MLCA, and the jewellery sector. Trust businesses are also included in the regime although these services are usually provided by banks.

The financial institutions included in Article 5 of MLCA Taiwan are:

- banks;
- trust and investment corporations;
- credit cooperative associations;
- credit department of farmers' associations;
- credit department of fishermen's associations;
- Agricultural Bank of Taiwan;
- postal service institutions which also handle the money transactions of deposit, transfer and withdrawal;
- negotiable instrument finance corporations;
- credit card companies;
- insurance companies;
- securities brokers;
- securities investment and trust enterprises;
- securities finance enterprises;
- securities investment consulting enterprises;
- securities central depository enterprises;
- futures brokers; and
- trust enterprises.

Foreign currency exchange service providers were included in Taiwan's AML/CTF regime in 2007, with an amendment to the Regulations Governing Establishment and Administration of Foreign Currency Exchange Bureaus by the Central Bank of China. A range of businesses may provide foreign currency exchange in Taiwan:

- hotels;
- travel agencies;
- department stores;
- handicraft shops;
- jewellery stores;
- convenience stores;
- administrative offices of national scenic areas;
- sightseeing service centres;
- railway stations;
- temples;
- museums; and
- institutions and associations providing services to foreign travellers or hotels located in remote areas.

Obligations

Financial intelligence reports

- Reports of suspicious financial activity—regulated entities are required to submit reports of suspicious financial transactions to the FIU.
- Reports of high-value cash transactions—regulated entities are required to submit a Cash Transaction Report for any transaction in physical currency of NT$1m or more to the FIU.
- Reports of international movements of cash—there are two types of reports of movements of cash into or out of Taiwan. Cross-border currency declaration forms are required for movements of US$10,000 or more of physical currency into or out of Taiwan. These are submitted to the Customs Service and forwarded onto the FIU. The Inward Passengers Carrying Baggage and Good Clearance Regulation also requires inbound passengers to pass through Goods to Declare when carrying foreign currency of US$10,00 or more, NT$60,000 or more, Chinese currency of ¥20,000 or more, or gold valued at more than US$20,000.
- Reports of international movements of instruments of value—Taiwan does not require reports for movements of instruments of value.
- Reports of international electronic transactions—Taiwan does not require international electronic transactions to be reported.

Tipping-off

MLCA creates tipping-off offences for government officials and employees of financial institutions. They are prohibited from disclosing any information, documents, pictures, or other items related to a report of a suspicious financial transaction or suspected money laundering offence to any person.

Anti-money laundering/counter-terrorism financing compliance programs

Article 6 of MLCA, directing regulated entities to establish anti-money laundering procedures, requires the procedures to have the following components at a minimum:

- internal control procedures;
- staff training;
- appointing a money laundering control officer; and
- additional requirements as set out by the Ministry of Finance.

The Financial Supervisory Commission is the single regulator in Taiwan for the financial markets and financial services industries. The Financial Supervisory Commission's responsibilities include supervising financial institutions for compliance with the AML/CTF Guidelines issued by each of the industry associations. The Financial Supervisory Commission has the power to order entities to correct any areas of non-compliance with the appropriate Guidelines and to impose fines for non-compliance with MLCA Taiwan.

The Bureau of Agricultural Finance is responsible for supervising agricultural finance institutions and the Ministry of Economic Affairs is the supervisory body for dealers in precious metals and stones. The Financial Supervisory Commission conducts examinations of financial institutions and agricultural finance companies on behalf of the Bureau of Agricultural Finance.

Comparative analysis

The AML/CTF regimes across almost all countries share a common basis in the FATF-GAFI Recommendations and the countries considered within the scope of this report are remarkably similar in their responses to and implementation of the Recommendations. The variations arise in the detail and not in the general application of the principles. Commentators such as Levi and Reuter (2006) highlight the global pressure to expand the regime to cover non-financial businesses. Reuter and Truman (2004) also highlight that difficulties can arise with this globalised approach when countries have competing interests, different levels in motivation and varying abilities to comply with the Recommendations. Similarly, along with an increased burden on reporting entities, increased regulation also comes with greater difficulties in effectively monitoring and enforcing compliance with the requirements (Reuter & Truman 2004). The balance between the need for similar regimes in transnational economies and the need to recognise these competing interests is difficult to find.

Criminalising money laundering

All of the countries considered in this study have made money laundering a criminal offence distinct from the offence that generated the funds in question. The central difference between money laundering offences across jurisdictions is the way each country defines predicate crimes (ie the activities generating funds to be laundered).

Most countries limit the predicate crimes for money laundering offences in some way. Australia, the United States, Belgium, Germany, Hong Kong, Singapore and Taiwan all restrict predicate crimes to serious offences. Germany has also specified less serious offences that may also be predicate offences. Taiwan, in contrast, placed a further restriction on what might constitute a predicate crime by adding a lower limit of NT$20m for the amount of funds in question. Germany, the United States, Hong Kong and Singapore identify specific predicate offences within legislation, such as specifically naming tax crimes, although each of these countries also had a more expansive definition which includes all serious offences.

The definition of a serious, indictable, or felony offence differs between countries and is tied to minimum imprisonment periods in each country. Most of the countries in this sample used a minimum period of 12 months imprisonment to determine whether a crime fell into the definition of a serious offence. Taiwan, however, used a minimum of five years imprisonment as the cut-off for a serious offence. The real differences in the potential application of money laundering offences in these nine countries is with the prison sentences tied to specific crimes in each jurisdiction.

The result of the different requirements for a predicate offence for a money laundering charge is that some activities can lead to money laundering charges in some countries but not in others. The real impact of the different predicate offence requirements becomes apparent with cross-border investigations, cases that need mutual legal assistance from multiple jurisdictions and attempts to recover the proceeds of crimes once they have been moved overseas. The different treatment of environmental crimes, for example, and their inclusion or exclusion as predicate offences illustrates the potential impact of the different legal definitions of money laundering between jurisdictions.

The *Lacey Act of 1900* (16 USC 3371–3378) in the United States creates felony offences for importing illegally sourced timber (16 USC 3373) that can attract prison sentences of up to five years. The funds generated by importing illegally sourced timber may become the subject of a money laundering offence in the United States as their definition of predicate crimes extends to all felony offences. The potential imprisonment terms also permit the United States to pursue civil asset recovery mechanisms for the proceeds of these offences under 18 USC 981.

Australia, in contrast to the United States, is unable to attach money laundering criminal offences to proceeds generated by the importation of illegally sourced timber. The penalties for these offences do not allow these activities to constitute a predicate crime for money laundering in Australia and, as they are not indictable offences, the funds generated cannot become the focus of a civil asset recovery application under s 19 of the *Proceeds of Crime Act 2002* (Cth).

Criminalising the financing of terrorism

Taiwan was the only country considered in this report that has not, as yet, criminalised the financing of terrorism. The remaining eight countries had enacted terrorism financing legislation. Australia criminalised financing individual terrorists, terrorist organisations and terrorist acts through providing funds and other resources. The United States and United Kingdom made funding terrorist groups or acts criminal offences. Singapore specifically mentioned individual terrorists and acts, while others such as Hong Kong focused entirely on terrorist acts and purposes.

The counter-terrorism financing offences across the countries within the scope of this report, with the notable exception of Taiwan, were more uniform than those for criminalising money laundering. This is probably, in part, because the FATF-GAFI's Special Recommendation II does not encompass additional issues such as defining or recommending approaches to predicate offences. Special Recommendation II states '[e]ach country should criminalise the financing of terrorism, terrorist acts and terrorist organisations' (FATF-GAFI 2004: 2).

Despite a greater degree of uniformity of terrorism financing offences across the eight countries, Australia and Germany exemplified quite different approaches beyond creating criminal offences for providing support to terrorism. Australia's terrorism financing offences are tied to predetermined lists of terrorist organisations, whereas Germany's legislation requires prosecutors to demonstrate that the groups in question, in each accusation of providing support to terrorism, are terrorist organisations.

Reporting requirements

The requirement to submit financial intelligence reports is the cornerstone of using regulation to prevent money laundering and the financing of terrorism. Financial intelligence reports provide information to FIUs and to the law enforcement community in each of the countries considered in this report. The reporting requirements for each jurisdiction, however, showed considerable variations.

Suspicious transactions

All of the countries in this sample require at least some service providers to submit reports of suspicious financial transactions. The conditions of the reporting requirements, however, are quite varied between countries. Australia, the United Kingdom and Taiwan require all regulated entities to submit reports of suspicious transactions. These countries define the circumstances of a suspicious transaction broadly by not restricting what constitutes a suspicious transaction in legislation or regulation. The remaining six countries place caveats, or additional guidelines, on when a report of suspicious activity is warranted or required.

The United States limits the transactions considered for reporting of this kind with a monetary threshold. MSBs are required to report suspicious transactions only where the value of the transaction exceeds US$2,000. The threshold for transactions conducted by financial institutions is US$5,000. For both types of businesses, the thresholds expanded to US$25,000 where the suspected offender was unknown.

Belgium, France and Germany also limit the transactions that might warrant a report. These three countries limit the reports by specifying the crimes that might trigger a report.

France's regulated entities are required to report transactions suspected to be connected to drug trafficking, organised crime, fraud against the European Communities, corruption, or terrorism financing. The predicate offences prompting a report are the source of some dispute in France, particularly those concerning lower level misappropriation of funds and tax evasion. The predicate crimes for reporting are not the same as those for French money laundering offences. All reporting entities have the additional requirement to submit a report where they are unable to verify the beneficial owner of assets or funds after conducting customer due diligence.

The reporting requirements of Belgium are similar to those in France in some aspects. Belgium limits reports of suspect transactions to those connected to specific crimes which include terrorism or terrorist financing, organised crime, illicit trafficking, serious fraud and organised tax fraud, corruption, environment

crime and counterfeiting. Financial institutions, professions and casinos hold additional reporting requirements on forming a suspicion that a transaction is specifically connected with money laundering or the financing of terrorism. These businesses are required to make fact submissions for these transactions.

While Belgium limits fact submissions to transactions suspected to be connected to money laundering or the financing of terrorism, Germany limits the scope of reporting suspect transactions to those linked with these two types of offences only.

The approaches taken by Hong Kong and Singapore are somewhat different. Hong Kong and Singapore also limit the crimes that might trigger a transaction report to indictable offences, in the case of Hong Kong, and to drug trafficking or other criminal conduct, in the case of Singapore. All individuals in Hong Kong, not just reporting entities, carry this obligation and an identical one to report suspicions of terrorist property.

Singaporeans who come across transactions that might be connected to drug trafficking or criminal conduct in the course of business are to submit a report. Additionally, all persons in Singapore and any Singaporean citizens overseas, are to report any transactions suspected to be linked to the financing of terrorism.

Reports of high-value cash transactions

Reporting requirements for cash transactions that exceed a threshold are less common among the sample of nine countries. Australia and the United States require regulated businesses to submit a report of any transaction made using cash above a set threshold. Taiwan also requires regulated entities to submit a report of any cash transaction valued at NT$1m. The Australian threshold is AUD$10,000 and the United States threshold is US$10,000. Regulated entities in the United States can apply for an exemption for transactions carried out by certain businesses. Australian entities are able to file a suspicious transaction report for the same transaction that triggered a threshold report. Singapore, rather than requiring a report for every cash transaction beyond a threshold, suggest that large cash transactions are likely to be suspicious and to warrant reporting in that way.

France and Germany do not require regulated entities to submit cash transaction reports. Germany, however, requires businesses to retain customer identification for cash transactions valued at €15,000 or more. French regulated entities are similarly required to scrutinise cash transactions beyond a threshold limit and to retain that information. Belgium prohibits cash payments of more than €15,000, rendering any reporting of this nature redundant. The United Kingdom and Hong Kong do not have any large cash transaction requirements.

Reports of international movements of cash and bearer negotiable instruments

Almost all of the nine countries have identical requirements to report the movements of cash across country borders on entry and exit. The cash thresholds that trigger a report are as follows:

- Australia—AUD$10,000 or more, or the equivalent in foreign currency;
- United States—more than US$10,000;
- United Kingdom—€10,000 or more for cash brought into or out of the European Union;
- Belgium—€10,000 or more for cash brought into or out of the European Union;
- France—€10,000 or more for cash brought into or out of the European Union;
- Germany—€10,000 or more for cash brought into or out of the European Union; and
- Singapore—SGD$30,000 (or foreign equivalent) or more.

Taiwan has two types of reports of movements of cash into or out of Taiwan. Cross-border currency declaration forms are required for movements of US$10,000 or more of physical currency across Taiwanese borders. Inward bound passengers with foreign currency of US$10,00 or more, NT$60,000 or more, Chinese currency of ¥20,000 or more, or gold valued at more than US$20,000 are also required to undertake additional customs screening.

Hong Kong is the only country considered not to require passengers to report international movements of cash. The United States, United Kingdom, Belgium, France, Germany and Singapore subject movements of bearer negotiable instruments to the same reporting requirements, with the same thresholds, as cash movements.

Australia was one of two countries that do not apply the same requirements for moving cash across international borders to international movements of bearer negotiable instruments. Passengers moving bearer negotiable instruments into or out of Australia can be required to submit a report by a customs or police officer but there is no mandatory reporting requirement. Taiwan also does not require mandatory reports for moving instruments of value across its borders. Hong Kong does not require a report for moving cash across its borders and similarly has no requirement for bearer negotiable instruments.

Reports of international electronic transactions

Australia is the only country in this sample to require all regulated businesses to report all IFTIs, regardless of value, to the FIU. An IFTI can be the subject of a suspicious matter report, although this is not a requirement.

The United Kingdom, Belgium, France and Germany do not require a report of every international electronic transfer of funds. These countries do, however, require financial institutions transferring funds outside of the European Union to retain customer identification information of the payee and to send this information along with the transfer instruction. Transfers within the European Union can be completed with account information only.

Hong Kong, similarly, does not require the international transfer of funds to be accompanied by a report to the FIU, although remittance providers and money exchangers are obligated to record the details of any transaction of HK$8,000 or more.

Implications of different reporting requirements

The predominant implication for the different financial report requirements in each of the nine countries is the nexus between report numbers and available information. The majority of reports lodged in Australia, for example, are IFTIs. As the fourth section illustrates, these reports constituted more than 75 percent of the reports lodged to AUSTRAC, the Australian FIU, in 2007–08 (AUSTRAC 2009a). The additional reports offer the law enforcement community and other agencies such as the Australian Taxation Office, more information to inform investigations (Smith forthcoming).

The converse implication of Australia's IFTI requirement is the vast amount of data sent to the FIU and the additional resources the FIU would require to process and analyse the information. The reporting requirements in countries such as France and Germany, which require reporting entities to file STRs for transactions suspected to be tied to money laundering only (FATF-GAFI 2010), act to restrict the volume of reports lodged with FIUs. Some of the positive consequences of more targeted yet fewer reports might include improving the quality of information and its utility (Unger & Van Waarden 2009). The data available in the fourth section is not sufficient to indicate which of these two approaches to gathering financial intelligence is more effective but these cases provide real world examples of two opposing ideals on financial intelligence reporting.

Tipping-off clauses

Each of the nine countries currently has tipping-off provisions that criminalise revealing the details of a report of a suspicious transaction to those involved. The tipping-off clauses vary in the extent of the information to remain confidential and the exemptions made to the tipping-off provisions.

The United States and France have the simplest models for tipping-off and they prohibit disclosing information connected to a filed report to those involved in the transaction. Belgium and Germany extend this to prohibit disclosures connected to a report to any third party as well as the subject of a report. Both Hong Kong and Singapore prohibit the disclosure of any information relating to reports to any person where the disclosure might prejudice an investigation.

Tipping-off in the United Kingdom applies to the details of investigations, as well as reports, and extends to all third parties. The United Kingdom also has additional tipping-off provisions for civil recoveries, asset confiscations and money laundering offences. Taiwan's provisions are similar as they encompass both reports of suspect transactions and any suspected money laundering offence.

Australia specifically prohibits disclosing the details of reports, and any person or matter that should trigger a report, to any third party. Australia also has one of the most extensive lists of persons exempt

from tipping-off. Australia, like the United Kingdom, France and Singapore, excludes legal practitioners in specific circumstances from the tipping-off requirements. Australia extends the exemptions beyond these to accountants, businesses with a joint anti-money laundering program and anyone trying to dissuade a customer from committing an offence under any law in Australia.

Case law

Australia

Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)

The AML/CTF Act offers several types of penalties for non-compliance including criminal penalties.

Failing to report moving physical currency into Australia (s 1(a)(ii)) (2009)

The defendant failed to make a declaration under s 1(a)(ii) of the AML/CTF Act when he brought AUD$72,464 into Australia in April 2009. The defendant was aware of the requirement to make a declaration and purposefully concealed the cash he knew to be the proceeds of crime. He received a sentence of eight months imprisonment for failing to make the declaration and the money was forfeited under the *Proceeds of Crime Act 2002* (Cth) (CDPP 2009).

Financial Transaction Reports Act 1988 (Cth)

R v Narayanan & Anor [2002] NSWCCA 200

Singapore Exchange and Finance Pty Limited (SEF) was a business providing currency exchange and travellers' cheques. Narayanan was the CEO, director and a shareholder of SEF. SEF was a cash dealer for the purposes of the FTR Act. SEF and Narayanan were each convicted of three offences under s 31(1) (structuring transactions) of the FTR Act and one offence under s 28(1) (failing to submit a report of a significant cash transaction) of the FTR Act. Narayanan was sentenced to 10 months imprisonment for the offences under s 31(1) and four months imprisonment for the offence under s 28(1). SEF was fined a total of $100,000.

Narayanan and SEF appealed the convictions, in part, on the grounds that the trial judge erred in his directions as to what constitutes an offence under s 31(1) of the FTR Act. In the appeal decision, the court ruled that the trial judge had erred in these directions and clarified the conditions of a reportable cash transaction.

The court stated the offence of s 31(1) is one of being party to two or more non-reportable transactions for the purpose of ensuring or attempting to ensure that the transaction was not a significant cash transaction. Conducting two or more non-reportable transactions, those involving amounts below the reportable threshold of $10,000, might not ensure that the activities do not also constitute a significant cash transaction that should trigger a report. The multiple transactions below the threshold might constitute a reportable transaction even when the parties to the transaction have attempted to avoid triggering the report. Multiple transactions for amounts less than $10,000 can be both non-reportable transactions and collectively a significant cash transaction.

Money laundering criminal cases

A Ansari v R, H Ansari v R (2007) 70 NSWLR 89; *Ansari v The Queen* [2010] HCA 18

The Ansari brothers were convicted of two charges of conspiring to launder money valued at more than $1m through their remittance business *Exchange Point*. The Ansaris took receipt of $2m cash from another man and arranged for a second individual to collect the money. The Crown alleged that the Ansaris knew that the funds would be deposited in amounts of less than $10,000 to avoid triggering reporting requirements in Australia. The Crown demonstrated that the brothers were reckless of the risk that the money would become an instrument of crime. The money laundering offence the Ansaris were convicted of conspiring to execute was the reckless laundering of funds valued at $1m or more (s 400.3(2)).

The Ansaris appealed their original conviction on the basis that it is not possible to conspire to recklessly commit an offence. The decision of the court on appeal highlighted a number of key aspects to the way money laundering offences are framed in the Criminal Code. The NSW Court of Criminal Appeal

(CCA) stated that offences for funds valued at $1m or more actually constitute six possible crimes. The six possible crimes are distinguished by the fault element involved (intent, recklessness, negligence) and whether the funds were the proceeds of crime or intended to be used as an instrument of crime.

The appeal was dismissed. Justice Howie found that there were two fault elements in question for the crime of conspiring to recklessly deal with funds intended to be the instruments of crime. The 'reckless' fault element is for the money laundering offence and separate to the intention of conspiring to commit the crime. The result of this decision is a validation of the charge to conspire to commit a money laundering offence in Australia where the fault element of the offence is recklessness rather than intent.

The Ansaris were granted leave to appeal this decision to the High Court, in 2009, on the grounds that CCA erred in holding that it was not bad in law for the Crown to charge a conspiracy to commit an offence for which the fault element is recklessness; and that CCA erred in its interpretation of the physical and fault elements of the offence of conspiracy under the Code. The appeals were unanimously dismissed.

R v RK (2008) 73 NSWLR 80; *R v LK, RK* [2010] HCA 17

RK was also charged with conspiring to recklessly deal with the proceeds of crime. RK and LK, a co-defendant, were alleged to have dealt with the proceeds of a scheme to defraud the Commonwealth Superannuation Scheme. The trial judge, Sweeney DCJ, directed a verdict of acquittal. RK and LK were not aware that the funds were the proceeds of crime. Sweeney held that the offence on the indictment was not an offence known to the law. The decision in Ansari was distinguished on the basis that, in the Ansari case, the Crown had alleged that the accused actually *did* know all of facts that made the conduct criminal. Here, only recklessness was alleged. The Crown's appeals to the NSW CCA and the High Court were unanimously dismissed.

R v Huang, R v Siu [2007] NSWCCA 259

Huang and Siu pleaded guilty to offences under the FTR Act (s 31(1)) and of money laundering under the Criminal Code (s 400.3(1)). Huang believed the funds involved to be legitimately gained funds transferred offshore to evade Australian taxes. Siu believed the money to be the funds of an illegal fishing operation.

The Crown appealed the sentences given to both Huang and Siu. The submission on behalf of the respondents in this appeal argued that the offences of money laundering under the Criminal Code were very broad and stretched between the trivial and the very serious. The respondents argued the importance of assessing the seriousness of the conduct of the offender and not merely where the alleged offence falls into this spectrum between trivial and serious crimes. The submission further argued that there was no reason to fail to consider the criminal activity the accused intended to carry out (in this case a structuring offence under the FTR Act) where an offender was convicted of a money laundering offence.

CCA stated that the offender's belief about the source of the funds in question will always be relevant for cases involving the proceeds of crime and the instruments of crime. The belief about the source of funds intended to be an instrument of crime is less important, as the offence is centred of the future use of the money.

The court upheld the Crown's appeal against the sentences received by each of the offenders and re-sentenced Huang to five and a half years imprisonment, with a non-parole period of three years and four months. Siu received five years imprisonment, with a non-parole period of two years and six months. The Court stated that a sentence of between 12 and 14 years would have been an appropriate starting point for sentencing Huang; and a sentence of at least eight years would have been an appropriate starting sentence for Siu, were it not for the discretionary factors arising from a successful Crown appeal.

Terrorism financing-related cases

Since 2001, 38 people have been prosecuted, or are being prosecuted, as a result of counter-terrorism operations in Australia and 20 have been convicted of terrorism offences under the Criminal Code. More than 40 Australians have had their passports revoked or applications denied for reasons related to terrorism (DPM&C 2010).

In Australia, actual evidence of how terrorism is financed is limited. As is the case with anti-money laundering, financial intelligence plays a role in counter-terrorism investigations and contributes to successful prosecution outcomes. The Australian cases have involved individuals who have supported overseas groups, as well as those who have planned terrorist activities within Australia—fortunately without success. Although the incidence of Australian-based financing of terrorism is minimal, there remains an ongoing need to continue counter-terrorism efforts, which includes the gathering of financial intelligence. The following matters involve allegations of financing of terrorism or provision of support for terrorist organisations in addition to other alleged offences.

R v Joseph Terrence Thomas [2008] VSC 620

On 4 January 2003, Joseph (Jack) Terrence Thomas was apprehended attempting to leave Pakistan using a Qantas Airways ticket for Australia. At the time he was apprehended by Pakistani officials, it is alleged that he was in possession of an Australian passport which had been falsified, together with US$3,500 in cash which had allegedly been provided to him by Al Qaeda. He was arrested in November 2004 and charged with one count of receiving funds from a terrorist organisation (s 102.6(1)), two counts of providing resources to a terrorist organisation (s 102.7(1)) and one count of possessing a falsified Australian passport. Initially found guilty of receiving funds from a terrorist organisation in February 2006 and sentenced to five years' imprisonment with a non-parole period of two years, his conviction was later quashed on appeal in August 2006 (*R v Thomas* [2006] VSCA 165).

The Commonwealth Director of Public Prosecutions (CDPP) successfully sought to have the case re-tried and Mr Thomas was convicted in October 2008 of the charge of possessing a falsified passport and sentenced to nine months' imprisonment. All other counts were not proved (*R v Thomas* [2008] VSC 620).

R v Faheem Khalid Lodhi [2006] NSWSC 691

In 2003, Faheem Khalid Lodhi was the first person to be found guilty of planning a terrorist attack in Australia (*Regina v Lodhi* [2006] NSWSC 691). The circumstances of the matter arose in 2001 when a man named Willie Brigitte trained at a terrorist training camp in Pakistan called Lashkar-e-Taiba, a proscribed terrorist organisation. In May 2003, Brigitte arrived in Australia from France, a few days prior to which, Faheem Khalid Lodhi set up a mobile phone account in a false name. Two calls were made from Brigitte's phone in France to Lodhi's phone—one on 7 May 2003 and the second one on 13 May 2003, the day before Brigitte left France for Australia. Lodhi met Brigitte when he arrived in Australia and they spent most of that day together. In October 2003, French authorities notified Australian authorities that Brigitte had a substantial connection with terrorism. This led to his sudden detention and deportation to France. Just before Brigitte's detention, Lohdi obtained maps of the electrical supply system in Sydney using false identification and requested a list of chemical prices by fax using a false company name.

Lodhi was arrested on 22 August 2004 and was charged with various terrorist-related offences. The Supreme Court of New South Wales was satisfied that Lodhi's plans to bomb the electricity system had only reached a very early stage, but still convicted him of a number of offences as it was satisfied that he intended to use the maps and the list of chemicals in a plot to cause the detonation of an explosive or explosives to advance the cause of violent jihad and intimidate the government and the public. On 19 June 2006, Lodhi was sentenced to 20 years' imprisonment, with a 15 year non-parole period. Mr Lodhi appealed both his conviction and sentence, but both were upheld by NSW CCA on 20 December 2007. Mr Lodhi made an application for special leave to appeal to the High Court, however, this was refused on 13 June 2008 (*Regina v Lodhi* [2006] NSWSC 691).

David Hicks

David Hicks was sentenced by a US Military Commission to seven years' imprisonment after pleading guilty to the charge of providing material support for terrorism. All but nine months of this sentence was suspended by the Convening Authority in accordance with the sentence and the terms of a pre-trial agreement. Mr Hicks was released from the Yatala Labour Prison in Adelaide on 29 December 2007. An interim control order

in relation to Mr Hicks was made by a Federal Magistrate on 21 December 2007. It was confirmed by a Federal Magistrate on 19 February 2008 (Jaggers 2008).

Mohamed Haneef

Dr Mohamed Haneef was charged on 14 July 2007 that 'on or about the 25th of July 2006 in the United Kingdom, he intentionally provided resources, namely a subscriber information module (SIM) card to a terrorist organisation consisting of a group of persons including Sabeel Ahmed and Kafeel Ahmed, being reckless as to whether the organisation was a terrorist organisation' (CDPP 2008: 51), contrary to s 102.7(2) of the Criminal Code. On Friday 27 July 2007, the Director of Public Prosecutions discontinued the prosecution of Dr Haneef for the alleged offences after the case was assessed in accordance with the Prosecution Policy of the Commonwealth (Coorey et al. 2007).

Aruran Vinayagamoorthy and Anor v DPP [2007] VSC 265

In 2009, three men—Aruran Vinayagamoorthy, Sivarajah Yathavan and Arumugan Rajeevan Tash—pleaded guilty to offences under the *Charter of the United Nations Act 1945* (Cth) for making money available to an entity, the Liberation Tigers of Tamil Eelam (LTTE), proscribed for the purposes of that Act. It was the prosecution's case that $1,030,259 was made available to the LTTE. Although the judge at sentencing found it was not possible to say precisely how much money was made available, he considered that they were large amounts. It was also the prosecution's case that Mr Vinayagamoorthy made an estimated $97,000 worth of electronic components available to the LTTE over a period of about two years. The court accepted that the defendants were motivated partly by a desire to assist the Tamil community. The three were sentenced to terms of imprisonment, but released on good behaviour bonds (*R v Vinayagamoorthy & Ors* [2010] VSC 148, 31 March 2010).

R v ABN and others [2009] VSC 21

In November 2005, 10 men were arrested in Melbourne and charged with terrorism offences under Part 5.3 of the *Criminal Code Act 1995* (Cth). A further three men were arrested in March 2006 and charged with similar and related offences. All 13 were alleged to have been members of a local unnamed terrorist organisation led by the defendant. It was alleged that the organisation was committed to preparing, planning, assisting in, or fostering the commission of terrorist acts in an effort to influence the Australian Government to withdraw its troops from Iraq and Afghanistan. Four of the 13 accused were acquitted, with the balance convicted following either pleas of guilty or a contested trial. Three of the accused were also convicted of attempting to make funds available to a terrorist organisation. The court found that they intended to do this by selling parts from stolen cars and using the proceeds of sale for the purposes of the organisation. The court accepted evidence that an amount probably in the order of $7,000 had been raised through other means. Seven of the convicted prisoners have appealed against their convictions. At the time of writing, the appeals had been heard but the decision was reserved (CDPP 2009).

R v Mohamed Ali Elomar and others [2010] NSWSC 10

In February 2010, five men were sentenced to lengthy terms of imprisonment for their participation in a conspiracy to commit acts in preparation for a terrorist act or acts involving the detonation of explosive devices and/or the use of firearms. The aim was to advance the cause of violent jihad so as to coerce, or influence by intimidation, the Australian Government to alter or abandon its policies of support for the United States and other western powers in the Middle East and other areas involving Muslims. The evidence of the financing of the proposed acts indicated that relatively small sums of money were involved and that these were self-funded. One offender paid $2,100 as a deposit on 10,000 rounds of ammunition. Another offender paid a $200 deposit for chemicals, while another paid $433 for more ammunition. Other finance was arranged using coded SMS text messaging, although the court found that it was unclear where the money had actually come from (*Regina (Cth) v Elomar & Ors* [2010] NSWSC 10).

United States

Definition of money laundering

The following two cases have addressed the definition of a money laundering offence. Each case has acted to narrow the definition of money laundering in the United States to a more specific offence from the broad definition initially pursued.

***Regalado Cuellar v United States* 06–1456 (2008)**

In 2003, Cuellar was stopped by police in Texas and found with more than US$80,000 hidden in his car. Police suspected these were funds related to drug trafficking. Cuellar was charged and convicted of money laundering under the Bank Secrecy Act for attempting to smuggle the cash across the border. He appealed this decision on the grounds that in order to satisfy the components of 'concealment' in the statute, an activity needs to attempt to make the origins of the money appear legitimate, which he had not attempted to do. Cuellar argued that, at most, he was guilty of the lesser offence of cash smuggling. The conviction was overturned in a split decision, but later reviewed and upheld on the basis that there are different ways 'concealment' can be established and that the statute used the word in a broad sense.

The Supreme Court unanimously overturned this conviction. The Court found that the federal money laundering statute (18 USC s 1956(a)(2)(B)(i)) does not require proof that a defendant attempted to legitimise tainted funds, however, the government must demonstrate that a defendant did more than merely hide the money during its transport. This significance of this case is in establishing that money laundering is more than hiding illicit proceeds. It requires a further design to create the appearance of legitimate wealth.

***United States v Santos et al* 06–1005 (2008)**

Santos and Diaz were convicted of money laundering under the Bank Secrecy Act for transactions they had performed using the funds generated by an illegal lottery. The defendants performed the transactions in the course of running an illegal lottery. The transactions included, among other items, paying the lottery winners. The convictions were based on interpreting the term 'proceeds of crime' in the federal money laundering statute (18 USC s 1956(a)(1)) to mean any funds generated illegally. The conviction was later quashed, based on an alternative interpretation of 'proceeds' which other legislation defines as either the profits of crime of the receipts of crime. The appeal judgement, that profits from crime were required for a money laundering offence, was confirmed by the Supreme Court in June 2008.

Definition of money laundering—conspiracy to commit money laundering

The following case de-limited the circumstances required for a conviction of conspiring to commit money laundering. Whitfield and Hall were co-petitioners in this case.

***Whitfield v United States* 03–1293 (2005) & *Hall v United States* 03–1294 (2005)**

Whitfield was convicted on various charges, including mail fraud and money laundering in violation of 18 USC 1956(a)(1)(A)(i) as well as conspiracy to commit money laundering under the Bank Secrecy Act (18 USC 1956 (h)). Whitfield sought, in the first trial, to instruct the jury that in order to prove a conspiracy to commit money laundering, there needed to be proof of an overt act to further the conspiracy beyond reasonable doubt. This was denied and he appealed on this basis.

The appeal was not successful. The court held that 18 USC 1956 (h) does not require an overt act in order for a conviction of conspiring to commit money laundering and thus concluded that the jury had been correctly instructed. This section of the code specifies that

> Any person who conspires to commit any offense defined in this section or section 1957 shall be subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy.

The conviction was again upheld in the Supreme Court, in January 2005, on the grounds that the text of the code did not specifically identify an overt act, nor could one be implied.

The financing of terrorism

Weiss v National Westminster Bank Plc 05–CV–4622 (2007)

The families of attack victims in Jerusalem launched a civil case against National Westminster Plc (NatWest). The plaintiffs argued that NatWest provided financial services for a group raising funds for HAMAS, the perpetrator of the attacks, after it was declared a terrorist organisation in 1995. The financial services were provided to Interpal, a British charity that the plaintiffs alleged had been identified as a fundraiser for HAMAS. The plaintiffs claimed that NatWest was aware of the association between Interpal and HAMAS and continued to provide financial services. NatWest claimed that an investigation into links between Interpal and HAMAS cleared Interpal of any wrongdoing.

NatWest motioned to have the case dismissed in 2006 and was partially successful. The motions to dismiss the claims of knowingly providing material support or resources to a foreign terrorist organisation in violation of 18 USC s 2339B and financing acts of terrorism, in violation of 18 USC s 2339C were denied. The outcome of the case has yet to be decided.

New York Branch of Arab Bank, New York

The Arab Bank, headquartered in Jordon, received civil penalties of US$24m from both FinCEN and the Office of the Comptroller of the Currency (OCC) for violations of the Bank Secrecy Act in 2005. Arab Bank's fines were discharged in a single payment of US$24m to the United States Department of Treasury. Arab Bank's anti-money laundering program was found to be inadequate, its risk management of US dollar transactions were inadequate and the bank lacked internal controls to manage money laundering and terrorism financing risks for transactions for beneficiaries and parties that were not account holders at Arab Bank.

Arab Bank, following on from the FinCEN assessment and the administrative fines, was sued by Linde (*Linde et al. v Arab Bank Plc*) and others (such as *Litle et al. v Arab Bank Plc* and *Coulter et al. v Arab Bank Plc*) for offences related to providing material support to terrorists. The outcome of this case has yet to be decided.

Stanley Boim and Joyce Boim v Holy Land Foundation for Relief and Development et al.

The plaintiffs' son was killed in the West Bank in 2005 in a shooting conducted by gunmen believed to be acting on behalf of HAMAS. The Boims sued Arab and Muslim charities, and individuals, in the United States who were claimed to be making funds available to HAMAS under s 2333 of the US Criminal Code which allows for US nationals to recover damages suffered in acts of international terrorism. The Boims' originally won damages in *Boim v Quranic Literacy Inst* 340 F Supp 2d 885 (ND Ill 2004) for US$52m which was later tripled to US$156m.

In December 2007, the Seventh Court of Appeals ordered a retrial of the case for multiple reasons, including:

- The responsibility of HAMAS for the Boim's son's death had not been conclusively shown.
- Evidence that the defendants had engaged in some act of helping HAMAS, even with the knowledge of its activities and a desire for those activities to succeed, does not mean that a defendant caused a particular injury. Causation is a distinct element requiring proof for liability to be shown.

United Kingdom

Failing to disclose suspicious activity

R v Griffiths and Patterson [2006] EWCA Crim 2155 (UK)

A United Kingdom solicitor, Phillip John Griffith, undertook the conveyance of property. The transaction was a property purchase by a long-time friend and business associate of Griffith from a seller with a criminal record, at a significant undervalue. Griffith was subsequently convicted for failing to disclose to authorities that he knew or suspected money laundering was taking place. Griffith was sentenced to 15 months imprisonment. The sentence was reduced to six months on appeal in 2006, on the grounds that the offence represented a lapse in judgement rather than a desire to benefit from criminal activity. The conviction brought an end to his professional life.

Arrangements

Bowman v Fels [2005] EWCA Civ 226

The *Bowman v Fels* Court of Appeal judgement arose out of a property dispute between ex-cohabiters. Prior to a county court hearing, Bowman's legal advisors suspected Fels had included the costs of some work he had carried out on the property in question in his business and VAT lodgements. Bowman's legal advisors filed a report of their suspicions to NCIS.

Bowman's legal advisor believed POCA 2002 UK prevented disclosing to either the client, or to the defendant's legal team, that a report had been filed. The solicitor sort to adjourn the property dispute proceedings out of concern that 'appropriate consent' regarding the matter would not be forthcoming by the hearing date. There was concern over whether the report would affect the court proceedings (Camp 2007; Law Society UK 2005).

The appeal questioned whether a legal practitioner acting for a client in legal proceedings must disclose suspicions of money laundering immediately in order to avoid being guilty of the criminal offence of being concerned in an arrangement which he knows or suspects facilitates criminal activity. The question in *Bowman v Fels* was whether the offence applied to a legal advisor who came to suspect the other party had engaged in money laundering. The secondary question was whether POCA 2002 UK was intended to override the issues underlying Legal Professional Privilege (LPP).

The *Bowman v Fels* case concluded that the offence in POCA 2002 UK s 328 was not intended to cover ordinary conduct of litigation and the legislator would not have thought those activities to constitute 'being concerned in an arrangement' which facilitates money laundering.

The *Bowman v Fels* case confirmed that POCA 2002 UK was not intended to override LPP. When deciding whether to make a disclosure to SOCA, legal practitioners need to consider whether the information on which the suspicion is based on is subject to LPP (Camp 2007; Law Society UK 2005). Prior to *Bowman v Fels*, case law on this subject had been drawn from *P v P* which was effectively overturned by the Bowman case.

K Ltd v National Westminster Bank Plc and ors [2006] EWCA Civ 1039

The case raised questions under s 328 of POCA 2002 UK concerning 'arrangements'. NatWest claimed that to comply with a payment request from a customer would mean the bank became concerned in an arrangement it suspected would facilitate the use of criminal property. To avoid this, NatWest submitted a disclosure to obtain appropriate consent to conduct the transaction. Consent was not given within the seven day period, but was before the moratorium period of 31 days expired. During this time, as the bank did not process the transaction, the customer made a claim for an interim injunction to force the bank to comply with the customer's instructions. The interim injunction was refused. The transaction was conducted after consent was given, although the customer then appealed the refusal to grant the interim injunction as legal costs were still an issue.

The customer claimed that the bank was breaching its contract by refusing to perform the transaction. The claim highlighted a conflict between NatWest's actions to obey the law and their obligation to their client. The court found that 'Parliament has laid down the relevant procedure with which the bank has lawfully and properly complied' and the appeal was dismissed (*K Ltd v National Westminster Bank Plc and ors* [2006] EWCA Civ 1039: para 6).

Stephen Judge (City Index) (UK) 2006

Formerly the Money Laundering Reporting Officer (MLRO) for City Index, Stephen Judge was charged under s 327 of POCA 2002 UK for proceeding with a transaction totalling £30,787 prior to the seven day consent period expiring. Judge had made an SAR about the transaction but had not received consent to proceed before processing it. There was no suggestion of dishonesty on the part of Judge and he admitted to processing the transaction. Judge maintained the transaction was completed only to avoid tipping-off the customer to the report which would have been an offence in itself. The charges were controversial as it was viewed that the case was based on a technical breach of the law only. The charges were eventually dropped in August 2006 because it could not be proven that the transaction in question was tied to criminal property.

Squirrel Ltd v National Westminster [2005] EWHC 664 (Ch)

NatWest filed an SAR based on suspected tax evasion and froze the customer's account while waiting for authorisation from the FIU. In line with tipping-off requirements, the bank provided no reasons to the customer as to why the account was frozen and the customer commenced legal action to unfreeze the account. The bank argued to either unfreeze the account or to disclose to the customer the reasons behind freezing the account would be an offence under POCA 2002 UK. The bank was found to have acted properly and the account remained frozen (Freshfields Bruckhaus Deringer 2005).

Suspicion

R v DaSilva [2006] EWCA Crim 1654

DaSilva was convicted of charges under s 93A(1)(a) of the *Criminal Justice Act 1988* (UK) for

> assisting another person to retain the benefit of criminal conduct knowing or suspecting that that other person was or had been engaged in criminal conduct.

DaSilva was also charged, alongside her husband, with obtaining money transfers by deception. DaSilva was acquitted of these additional charges while her husband was convicted.

DaSilva appealed the conviction on the grounds that the judge had given the jury a dictionary definition of the word 'suspecting' and then added gloss to the definition. DaSilva argued this made the term 'suspicion' too broad. The appeal decision found that the direction on the definition of 'suspecting' was misguided, it was insufficient to overturn the Supreme Court decision and the convictions were upheld.

While this case was prosecuted under previous legislation, it has provided some general guidance on the term 'suspicion', which remains a central element of the AML/CTF regime. The suspicion must be based on 'a possibility, which is more than fanciful' and 'must extend beyond speculation' (Law Society UK 2008: np).

Predicate offences

R v NW and others [2008] EWCA Crim 2

In January 2008, a prosecutor appealed a decision to dismiss the trial of four defendants facing multiple money laundering charges. The trial was dismissed as the prosecution had been unable to prove the type of predicate offences that generated the proceeds involved in the suspected money laundering activities.

The case centred on £100,000, transferred out of the United Kingdom that prosecutors alleged were the proceeds of NW's criminal activity. The offence generating the money could not be determined. The case questioned whether the criminal conduct, or at least the type of criminal conduct, had to be determined in order to generate a conviction for money laundering under ss 327–328 of POCA 2002 UK. The appeal concluded that Parliament could not have intended for there to be no need to give particulars on the criminal conduct and dismissed the appeal.

Terrorism—asset freezing

A, K, M, Q & G v Her Majesty's Treasury [2007] EWHC 869 (Admin)

A high court judgement in April 2008 ordered that measures for asset freezing and terrorism introduced under the Terrorism (United Nations Measures) Order 2006 and the Al Qaida and Taliban (United Nations Measures) Order 2006 be struck down as the UN orders had never passed through Parliament. The case *A, K, M, Q & G v HM Treasury* was an appeal on the asset freezing orders imposed by the UN orders above. The judge found the freezing orders to be unlawful and ordered these to be quashed. Due to the recent nature of this case the effect of the decision is yet to be determined.

Belgium

In November 2007, in a challenge to the anti-money laundering legislation, the Belgian Bar Association launched a second challenge to the implementation of the Second Money Laundering Directive. The decision reinforced that legal practitioners remained

covered by the anti-money laundering provisions in Belgium. It also outlined the conditions which provide exemptions to an obligation to make a disclosure. Any information gathered by a lawyer in the process of providing legal advice was bound by secrecy and could not be disclosed to authorities.

Information gathered outside this provision and within the confines of financial, corporate or real estate matters outlined in legislation, must be disclosed the Bar to be passed onto the FIU. If any additional information was required of a lawyer once a disclosure has been made, contact must go through the Bar, rather than between parties directly.

France

A decision on 10 April 2008 in France's highest administrative court, the Conseil d'Etat, found that EU member states are required to include the professional secrecy of legal practitioners within anti-money laundering legislation, rather than allowing the option to do so, as outlined in the Second Money Laundering Directive. The decision allows the widest meaning of 'legal advice'. The court also ruled that the FIU should not have direct access to legal practitioners but would need to go through the bar or the senior executives of law firms. This decision is in line with the decision in Belgium outlined above.

Hong Kong

Predicate offences

***HKSAR v Lee Wai-yiu, Fung Man-kwong, Mok Chang-wing* [2007] CACC 100/2006**

The three applicants and a fourth man were charged with an illegal gambling offence. Two of the defendants were convicted of that offence and all four were convicted of money laundering (s 25(1) and s 25(3) of OSCO). The defendants appealed the money laundering conviction. The money laundering convictions were based on the defendants' knowledge that the funds passing through their accounts (from the illegal gambling business) were definitely the proceeds of crime as they had committed these crimes.

The defendants sought leave to appeal the money laundering convictions on the grounds that a conviction for knowing (rather than for suspecting) that funds were the proceeds of crime relies on the judge also finding that the funds in question were from an indictable offence. In this case, the judge did not find two of the defendants guilty of the indictable offence suspected to be the source of funds. The appeal asked the court to consider if a money laundering offence requires a conviction of a predicate crime. Leave to appeal was denied and the court reaffirmed that OSCO did not require a conviction of a predicate offence to convict an offender for money laundering.

***Oei Hengky Wiryo v HKSAR* [2007] FACC 4/2006**

The circumstances of this case are similar to those of Lee, Fung and Mok and the question placed before the court on appeal was identical. Oei was convicted of illegal gambling, conspiracy and money laundering, also for dealing with the proceeds of his own crime. Oei, unlike Lee et al. was convicted of the offence generating the funds. The defendant appealed all three convictions, during which the Court considered the question of the necessity of a predicate offence, despite rejecting the appeal against the conviction of illegal gambling. The court reaffirmed that convictions under s 25(1) and s 25(3) were not reliant on proving a predicate crime.

Sentencing decisions

***HKSAR v Jain Nikhil and anor* [2006] CACC405/2006**

Jain Nikhil and Jain Aman Kumar, nationals and residents of India, allegedly opened bank accounts in Hong Kong with business registration certificates in the name of the companies in which they wished to open an account and forged passports. These bank accounts were subsequently used to launder approximately HK$6.6m. The proceeds were generated from a variation of the Nigerian scam and victims included an American doctor working in Brazil and a French merchant working in the People's Republic of China who remitted a total of US$561,000 and €209,339 to the account held by Jain Nikhil. The defendants later sought leave to appeal the sentences. The court upheld the sentences on appeal, stating that among other aspects, the amount of money involved in the case was a factor in determining the given sentence.

Comparison

What constitutes money laundering?

One common element of these cases is defining the actions that constitute a money laundering offence. This has been debated in these cases when defining what constitutes 'structuring', 'concealing', 'profits' of crime and 'suspicion'. Each of these cases has attempted to define the scope of the money laundering offences in the respective countries.

The Australian case *R v Narayanan* addressed the definition of structuring under the FTR Act. The court defined 'structuring' as two or more non-reportable transactions conducted to ensure, or to attempt to ensure, that the transaction was not a significant cash transaction. The court stated that multiple transactions, which had been subjected to structuring, could still collectively constitute a significant cash transaction.

The United States has recently decided two cases that narrowed the scope of money laundering offences in that country, one in terms of the process of laundering, the other in terms of what can be laundered. *Regalado Cuellar v United States* centred on the definition of 'concealment'. It was found that hiding currency for the purpose of transport was, in itself, not an act of laundering. The second case, *United States v Santos* et al. questioned what was meant by 'proceeds of crime' and it was found that it referred only to the profits generated.

Further cases defined actions that can constitute a conspiracy to commit money laundering. In Australia, *A Ansari v R, H Ansari v R* and *R v RK* defined the requirements for conspiracy to commit money laundering where the fault element of the offence is recklessness. *Ansari* allowed a broader interpretation of the offence as intent is not essential in the fault element. *RK* narrowed the circumstances where a conspiracy to commit a reckless action could be applied. In the United States, Whitfield (*Whitfield v United States*) and Hall (*Hall v United States*) argued it was not possible to conspire to commit money laundering without proof of an overt act, however, the courts ruled that conspiracy was enough and the offence of conspiracy was to be treated the same as an actual act of money laundering.

In the United Kingdom, the definition of 'suspicion' in relation to money laundering was tested by *R v DaSilva*. The case narrowed the definition slightly to require suspicion, which is more than fanciful, in order for an offence of money laundering, or assisting, to be upheld.

Cases have also questioned the need for a predicate offence to enable money laundering convictions. In Hong Kong, the cases of *Oei Hengky Wiryo v HKSAR* and *HKSAR v Lee Wai-yiu, Fung Man-kwong, Mok Chang-wing* demonstrated that a conviction for a predicate offence was not necessary in order to prove money laundering. A more detailed question was that in *R v NW and others* in the United Kingdom. The issue is this case was not whether the conviction must be obtained but whether the predicate offence must be identified. The finding in this case was that there was a need to identify at least what the predicate offence involved. Similarly, the decision to dismiss the case of *Judge*, the United Kingdom lawyer charged for processing a transaction without authorisation, was brought about because there was insufficient proof that the money involved in the transaction in question was indeed the proceeds of a crime.

Reporting requirements and legal practitioners

The application of AML/CTF legislation to legal practitioners has generated substantial debate. The cases outlined in this report demonstrate some of the issues at the centre of the contention. The most contested issue in the cases here is one of legal professional privilege and whether AML/CTF legislation was intended to override it. The recent decisions in the European Union and *Bowman v Fels* in the United Kingdom confirmed that this was not the case and legal practitioners are indeed exempt from reporting requirements if they are acting in the process of giving legal advice to a client. These decisions limit the ability to fully include legal practitioners in AML/CTF regulations and simultaneously highlight the difficulty in adopting identical legislation to cover professionals generally and legal practitioners specifically.

Further issues debated in these cases revolve around the offence of making an 'arrangement'

for money laundering. In *Bowman v Fels*, the case questioned whether a legal practitioner could be involved in arrangements for money laundering if they do not immediately disclose any knowledge or suspicion. This case found that this section of POCA 2002 UK was not intended to cover legal practitioners in the context of legal advice or litigation and furthermore, it would not override legal private privilege.

Two additional cases involving financial institutions debated the role of regulated entities in money laundering and prevention when a SAR has been submitted to the FIU. In *K v NatWest*, the bank refused to complete a transaction before authorisation from the FIU and was subsequently sued by the customer for breaching contract. Likewise, in *Squirrel v NatWest*, the bank froze the account of a customer they had made a report on and refused to disclose why, for fear of committing a tipping-off offence under POCA 2002 UK. In both cases, the bank was found to be justified in freezing the accounts and in not disclosing the reason to the customer.

Where the situation has been reversed and a transaction has been processed before permission was granted, legal action was taken against the officer who processed the transaction. Stephen Judge was charged with being involved in money laundering arrangements after processing a transaction to avoid committing a tipping-off offence by default, which he argued would happen if the transaction was not allowed.

Conclusion

The regulatory regimes in the countries covered in this section are each based on the FATF-GAFI Recommendations and as such, they each share expected similarities in their coverage and implementation. The differences in the regimes relate to how the regulations and requirements are imposed, rather than in the underlying principles that inform them. Differences arise in how, and if, the countries in this report attempt to regulate the professional sector. This is of particular relevance to legal entities, who are bestowed confidentiality rights in the course of their core business. The ongoing case law in this area highlights the contention and difficulty in striking a balance between the apparently opposing needs of regulation and privacy.

With regard to the Australian regime, it was found that the systematic reporting requirements introduced under the AML/CTF Act exceed those enacted in most of the other countries covered in this report. While there were requirements in every country to submit a disclosure of suspicious financial activity in some form, Australia was the only country that required reports for each of the following—systematic report for suspicious financial activity, high-value cash transactions, international movements of cash, international movements of value and international funds transfers—indicating the scope of the formal regime in Australia exceeds the others in this regard.

The analysis of regulatory regimes and case law in this section relating to terrorism financing show that considerable developments have been made to include it into legislation and regulations, but this highly controversial area remains mostly unsanctioned. The impending cases on this topic may have serious implications for the responsibilities of the regulated sector to identify their customers and the purposes of their financial transactions. The case of *A, K, M, Q & G v Her Majesty's Treasury* in the United Kingdom demonstrates how a serious topic matter and the potentially high cost of a terrorist attack may lead to more punitive regulations than those imposed on less emotive offences.

It is important to remember that several of the countries in this report are currently amending legislation or regulations relating to anti-money laundering and counter-terrorism financing. Australia is debating the introduction of a second tranche of reforms and countries in the European Union are updating their requirements based on the Third Money Laundering Directive. The next 12 months should see substantial changes to regulated sectors in these countries. This will allow a more substantial evaluation of regulatory regimes as case law and legislation interpretation continue to develop and the evidence base around compliance grows as regulated entities attempt to comply with requirements. For a country such as Australia, where many of the AML/CTF requirements are relatively new, and the regulated sector is rapidly increasing, the experiences of these overseas sectors will allow for a valuable learning experience.

The profile of designated entities

This section examines the size and composition of the regulated sectors in Australia, the United States, the United Kingdom, Belgium, France, Germany, Hong Kong, Singapore and Taiwan. While the aim is to provide a profile of the regulated sectors in these countries, there are considerable limitations in the data that were able to be provided and as a result, the discussion is less definitive than originally planned.

The largest gaps in the available information are for industries without prudential regulation or other long-standing registration processes. Additional issues of accessing English translations of documents, different year dates for collecting the information between countries and between industries and ambiguities in the exact businesses that might provide regulated services mean that the data presented should be considered estimations at best.

Many of the countries included in this section consider MSBs (such as remittance providers and issuers of travellers' cheques) as financial services. To facilitate a comparison between counties, in this context, providers of these services are described as MSBs.

Australia

The enactment of the AML/CTF Act in Australia vastly extended the number of businesses regulated for money laundering purposes beyond those with responsibilities under the earlier FTR Act. Legislative provisions that would have amended the AML/CTF Act to expand the range of regulated businesses were released for public comment in 2007. The draft amendment proposed expanding the scope of the regulations to real estate agents, some professional services and dealers in precious metals and stones. The amendments to the AML/CTF Act, expanding the regime's requirements to these industries, had not been implemented at the time of writing.

Australia's regulated sector currently includes:

- financial services (banks, credit unions, building societies, lending, leasing and hire purchase companies, asset management companies, financial planners (who arrange for the issue of financial products), life insurers, superannuation funds, custodial services companies and security dealers);
- MSBs (stored value card issuers, issuers of traveller's cheques, foreign exchange dealers, remittance dealers and cash couriers);

- the gambling sector (casinos, bookmakers, TABs, clubs and pubs, internet and electronic gaming service providers); and
- bullion dealers.

Confirming, or estimating, the full extent of the regulated sector in Australia is a task made difficult by the legislation's approach to defining the regulated sector. The AML/CTF Act names the services that are to be regulated for AML/CTF purposes, but not specific business types. AUSTRAC reported that Australia regulated approximately 17,700 businesses for AML/CTF in 2009. As of 30 June 2009, a total of 13,415 businesses were regulated by AUSTRAC and required to submit a compliance report (AUSTRAC 2009a). Table 1 outlines that around 40 percent of businesses regulated for AML/CTF were MSBs and 29 percent were businesses providing financial services. The remaining 31 percent of regulated non-financial businesses were encompassed in the regime were bullion dealers or providers of gambling facilities.

Table 1 Estimated size of the regulated sector in Australia, 2009

Sector	Estimated providers (n)	Proportion of total (%)
Financial services	5,200	29.38
MSBs	7,000	39.55
Non-financial businesses	5,500	31.07
Total	17,700	100.00

Sources: AUSTRAC 2009g

United States

The United States' expansion of the regulated sector for AML/CTF came with the PATRIOT Act. The PATRIOT Act added numerous business types to the definition of financial institutions and included a range of non-financial businesses to the regime. As noted in the second section, these included broker-dealers, casinos, futures commission merchants, introducing brokers, commodity pool operators, commodity trading advisors, providers of remittance services and dealers in precious metals, stones or jewels. The regulated sector in the United States is also based on regulating specific services and not specific entities.

The service providers identified as financial institutions under the Bank Secrecy Act, with AML/CTF obligations, are:

- banks (commercial banks, savings and loan associations, credit unions);
- federally regulated securities brokers;
- currency and exchange houses;
- funds transmitters;
- check-cashing businesses;
- persons subject to state or federal bank supervisory authority;
- casinos and card clubs; and
- insurance companies offering selected products, such as life insurance, annuity contracts, property and casualty insurance and health insurance.

The United States has also included additional service providers in the definition of financial institutions. Some of these businesses, such as those involved in settling real estate transactions, have not yet had AML/CTF rules issued by FinCEN.

Table 2 shows the estimated number of businesses within the US regulated sector from each of the three categories of financial services, MSBs and non-financial businesses. MSBs are the largest group of businesses with AML/CTF responsibilities in the United States, comprising around 74.4 percent of all businesses covered using the available figures. Businesses providing financial services represent around 18.7 percent of the entire regulated sector and non-financial businesses (for which figures are not available for all services) constitute approximately 6.9 percent of the estimates given by FATF-GAFI in 2006 (FATF-GAFI 2006).

Table 2 Estimated size of the regulated sector in the United States, 2006

Sector	Estimated providers (n)	Estimated proportion of total (%)
Financial services	56,447	18.68
MSBs	224,844	74.42
Non-financial businesses	>20,845	6.90
Total	>302,136	100.00

Source: FATF-GAFI 2006

Table 3 goes some way to explain the breakdown of the US regulated sector. Estimates for the number of trust companies and dealers in metals and stones are not available.

Table 3 outlines the number of banks in the United States in 2006 by regulatory agency. The different business structures of banks determine which regulatory agency supervises the banking business.

The OCC supervises the 1,818 Federal Deposit Insurance Corporation (FDIC)-insured nationally chartered commercial banks and the 50 federal branches and agencies of foreign banking organisations. The Federal Reserve supervises the 907 FDIC-insured state chartered banks that are members of the Federal Reserve System and 204 uninsured US branches and agencies of foreign banking organisations.

The FDIC itself supervises the 5,245 FDIC-insured, state-chartered commercial and savings banks that are not members of the Federal Reserve and eight FDIC-insured US branches of foreign banking organisations. Savings associations are supervised by the Office of Thrift Supervision. Of the 8,695 credit unions listed in Table 3, 5,393 were insured, federally chartered and regulated by the National Credit Union Administration (NCUA) and 3,302 were NCUA-insured, state-chartered and regulated by state supervisory authorities. The remaining 319 credit unions were privately insured, state-chartered and regulated.

Table 3 Regulated entities in the United States, 2006—estimates of service providers

Sector	Business type	Providers (n)
Financial services	FDIC insured nationally chartered commercial banks	1,818
	State chartered banks—members of federal reserve	907
	Uninsured US branches of foreign banks	204
	State-chartered banks not members of federal reserve	5,245
	Insured US branches of foreign banks	8
	Savings associations	862
	Credit unions	8,695
	Trust companies	No estimate
	Broker dealers	6,296
	Mutual funds	8,000
	Investment advisors	10,283
	Futures commission merchants	211
	Brokers in commodities	1,711
	Commodity trading advisors	2,635
	Commodity pool operators	1,783
	Domestic insurance companies	7,789
	Total	56,447
MSBs	MSBs (registered)	24,844
	MSBs—estimated total	200,000
	Total	224,844
Non-financial businesses	Casinos	845
	Precious metals and stones	20,000
	Total	>20,845
Total		>302,136

Source: FATF-GAFI 2006

The estimates of MSBs in Table 3 stem from the number of businesses that had registered with FinCEN by 5 April 2006. A total of 24,884 MSBs had registered with FinCEN by this date, although Coopers & Lybrand (in FATF-GAFI 2006) estimated that this could exceed 200,000. The 200,000 figure includes 40,000 US Postal Service outlets that sell money orders, as well as a number of agents of MSBs. The primary businesses, in these cases, are responsible for maintaining a complete list of agents with which they do business. FATF-GAFI further estimated that eight companies sell the bulk of MSB financial products and the agents of these eight companies account for most of the MBS outlets (FATF-GAFI 2006).

Professions in the United States, such as legal practitioners and accountants, are not subject to preventive AML/CTF requirements beyond the criminal enforcement risks associated with the violation of counter-terrorism financing requirements and assisting money laundering (Levi & Reuter 2006). FinCEN estimated that there were 845 casinos and card clubs operating in 34 states, tribal nations and territories in the United States at the time of the mutual evaluation in 2006. Fourteen states license casinos in the United States and the industry saw more than US$800b wagered at casinos and card clubs in 2004, which was 85 percent of the total amount of money wagered for all legal gaming activities in the United States (FATF-GAFI 2006).

In 2008, there were 29.6 million businesses in the United States, according to Office of Advocacy estimates based on data from the US Department of Commerce, Bureau of the Census (US Office of Advocacy 2009). As there were 302,136 regulated entities in 2006, it appears that approximately one percent of all businesses in the United States are regulated by FinCEN for AML/CTF purposes, a percentage comparable to that in Australia.

The United Kingdom

The United Kingdom, like Australia, defines the limits of its regulated sector by function rather than naming specific business sectors. Also like Australia, the extent of the regulated sector in the United Kingdom was recently expanded with new regulations. The Money Laundering Regulations 2007 expanded the regulated sector to include a number of non-financial businesses previously without AML/CTF obligations. These included auditors, accountants and tax advisors, independent legal professionals, trust or company service providers, estate agents, high-value dealers and casinos.

FATF-GAFI (2007a) estimated the total number of businesses with AML/CTF obligations in 2007 to be at least 206,566. Financial service businesses made up 27.2 percent of this figure, MSBs accounted for approximately 30.1 percent and businesses in the non-financial sector comprised the remaining 42.7 percent. Table 4 shows the estimated numbers of businesses in each of the three areas from the UK Mutual Evaluation.

Table 5 divides the number of regulated entities in the United Kingdom according to the specific type of businesses offering designated services. As is the case with the Australian figures, some of the totals given, particularly for MSBs and non-financial businesses, are the best estimates available.

Table 4 Estimated size of the regulated sector in the United Kingdom, 2007

Sector	Estimated providers (n)	Estimated proportion of total (%)
Financial services	28,969	27.15
MSBs	32,131	30.12
Non-financial businesses	>45,588	42.73
Total	>106,688	100.00

Source: FATF-GAFI 2007a

Table 5 Regulated entities in the United Kingdom, 2007—estimates of service providers

Sector	Business type	Providers (n)
Financial services	Personal investment	5,006
	Investment management	1,635
	Securities and futures	975
	Banking (including building societies and e-money issuers)	400
	Insurance	1,201
	General insurance	9,473
	Mortgages	3,589
	Professional firms	652
	Credit unions	562
	Other	614
	Category not supplied	4,862
	Total	28,969
MSBs	Money transmission only	9,767
	Bureau de change only	4,276
	Cheque casher only	1,371
	Bureau de change and money transmission agent	407
	Cheque casher and money transmission agent	311
	Bureau de change and cheque casher	534
	Bureau de change, cheque casher and money transmission agent	15,465
	Total	32,131
Non-financial businesses	Casinos	140
	Real estate agents	10,000
	High-value dealers	1,500
	Solicitors	>12,673
	Barristers	15,045
	Conveyancers	230
	Notaries	1,000
	Accountants	No estimate available
	Trust and company service providers	5,000
	Total	>45,588
Total		>106,688

Source: FATF-GAFI 2007a

The UK financial services industry

The United Kingdom employs over one million people in financial service businesses. It is one of the largest commercial banking sectors in the world. The United Kingdom insurance industry is the largest in Europe and third largest in the world (FATF-GAFI 2007a). Most of the 28,969 financial institutions are supervised by the FSA and the remaining institutions are European Economic Area (EEA)-authorised institutions. EEA-authorised institutions are banks from other countries within the European Union with

branches in the United Kingdom or UK banks with branches elsewhere. The FSA and EEA banks in the United Kingdom or supervised in the United Kingdom are shown in Table 6.

MSBs in the United Kingdom must register with HMRC. For businesses that use agents, such as remittance services (money transmitters), the principal is the registered entity. The agents of the business must comply with the regulations, although the principal remains responsible for the level of compliance. Table 7 gives an indication of the number of principals responsible for MSBs in the United Kingdom. The number of premises is the figure included in Tables 5 and 6.

Non-financial businesses

Non-financial business numbers are more difficult to gauge as not all are required to register with a supervisory authority or other agency. The numbers of non-financial businesses, by business type, are shown in Table 8.

Table 6 Banks authorised by either Financial Services Authority or European Economic Area, 2007 (n)

Financial sector	FSA-authorised financial institutions	EEA-authorised institutions	
		UK branches (EEA)	UK (cross-border) services (EEA)
Personal investment	5,005	0	1
Investment management	1,632	3	0
Securities and futures	967	6	2
Banking (including building societies and e-money issuers)	301	94	5
Insurance	723	74	404
General insurance	9,473	0	0
Mortgages	3,588	0	1
Professional firms	652	0	0
Credit unions	562	0	0
Other	605	5	4
Category not supplied	3	52	4,807
Total	23,511	234	5,224
Overall total	28,969		

Source: FATF-GAFI 2007a

Table 7 Principals and agents of money service businesses in the United Kingdom, 2007

Business type	Registered principals (n)	Premises (n)	Premises (%)
Money transmission only	1,515	9,767	30.3
Bureau de change only	852	4,276	13.3
Cheque casher only	546	1,371	4.2
Bureau de change and money transmission agent	244	407	1.2
Cheque casher and money transmission agent	103	311	0.9
Bureau de change and cheque casher	73	534	1.6
Bureau de change, cheque casher and money transmission agent	288	15,465	48.1
Total	3,621	32,131	

Source: FATF-GAFI 2007a

Note: Percentages may not total 100 due to rounding

Table 8 Non-financial businesses in the United Kingdom, 2007—including calculations and estimates

Business type	Entities (n)
Casinos	140 currently operating out of 165 total. Internet casinos have recently been legalised and will have to register. No estimates are available yet
Real estate agents	Approximately 10,000 firms
High-value dealers	Just over 1,500
Legal practitioners	100,938 solicitors holding practicing certificates in England and Wales. 1,976 practicing in Northern Ireland, 9,637 in Scotland 14,000 barristers in England and Wales, 585 in Northern Ireland, 460 advocates in Scotland
Conveyancers	Most conveyancing is done through legal firms, but there are 230 separate firms who specialise in conveyancing alone
Notaries	About 1,000 in England and Wales, Scotland. All are solicitors
Accountants (including auditors)	No estimate as registration not compulsory
Trust and company service providers	5,000 estimated but figures are hard to gauge

Source: FATF-GAFI 2007a

In the United Kingdom, there were 2.15 million enterprises registered for Value Added Tax and/or Pay as You Earn in 2009, compared with 2.16 million in March 2008 (ONS 2009). Using the 2008 estimate of the number of enterprises of 2.16 million, and the number of businesses with AML/CTF obligations in 2007 of 206,566, it appears that approximately 9.6 percent of all businesses were regulated by SOCA for AML/CTF purposes. This is a considerably higher proportion than in Australia or the United States. The reasons may lie in the inclusion of the UK's regulated sector of the large number of professional legal and accountancy practices.

Belgium

Belgium's AML/CTF regime covers core financial institutions (banking, credit, investment, insurance, mortgage, lease-financing, derivatives), adds key MSBs (currency exchange and funds transport) and many non-financial businesses (notaries, bailiffs, auditors, approved accountants, tax advisors, tax specialist-accountants, real estate agents, dealers in diamonds and gambling establishments and gaming halls). As with other countries, such as the United Kingdom, legal practitioners in Belgium have AML/CTF requirements only when engaging in financial and real estate transactions. Comprehensive information on the numbers of regulated entities across each business type is not available for Belgium. Selected numbers of entities with AML/CTF requirements are shown in Table 9.

Table 9 Selected reporting entities in Belgium, 2006

Sector	Business type	Providers (n)
Financial services	Banks	105
	Investment and securities companies	74
	UCI management companies	6
	Financial holding companies	7
	Settlement institutions	2
MSBs	Bureaux de change	21

Sources: CBFA 2007

Banking was by far the largest component of Belgium's financial sector in 2006. The banking sector in Belgium was a larger contributor to gross domestic profit than that of the banking sector in the United States (FATF-GAFI 2005a). Belgium banks are increasingly foreign owned, with just under half of the banks operating in Belgium in 2006 being foreign-owned entities (see Table 10).

Table 10 Banks operating in Belgium, 2006 (n)	
Banks authorised in Belgium	59
Banks governed by Belgian law	51
Banks	32
Savings banks	16
Securities banks	2
Municipal savings banks	1
Foreign banks—non European Union-based banks	8
Foreign banks—European Union-based banks	46
Total banks	105

Source: CBFA 2007

Table 11 provides a breakdown of the investment companies operating in Belgium in 2006.

Table 11 Investment firms in Belgium by business type, 2006	
Investment firms governed by Belgium	53
Stockbroking firms	27
Portfolio management companies	22
Financial instrument broking firms	1
Financial instrument placing firms	3
Investment firms—governed by European Union country	17
Investment advice company	3
Derivative specialist	1
UCI management company	6
Total	80

Source: CBFA 2007

France

The regulated sector in France encompasses financial institutions, real estate agents, casinos and gaming houses, high-value dealers (including precious stones and metals and art and antiques dealers) and accountants. Legal professionals in France have obligations when engaging in real estate or financial transactions. The numbers of banking and finance companies in France is falling. Table 12 shows that the number of credit and finance companies in France in 2008 was 1,253. Of that number, nine were in the process of liquidation or having their licence withdrawn.

Germany

Germany's AML/CTF regulatory regime extends across core financial institutions:

- credit institutions (who provide banking services);
- financial institutions (any financial service provider that is not a credit institution such as remittance providers, currency exchange, credit card providers);
- insurance companies (providing accident insurance with a premium redemption clause, life insurance and insurance brokers placing these policies);
- financial enterprises (such as those providing leasing contracts, investment advice and money broking services);

Table 12 Credit institutions (finance companies) in France, 2008 (n)	
Credit institutions approved in France (Établissements de credit agrees en France)	672
Credit institutions approved in other European countries (Établissements tablissements de credit de l'espace economique European exercant en libre etablissement (succurales))	69
Credit institutions in Monaco (Établissements de credit agrees pour exercer leur activite a Monaco)	27
Credit institutions approved in other European countries exerting in free performance of service (Établissements de credit de l'espace economique European exercant en libre prestation de services)	476
Credit institutions—course of withdrawal agreement (Établissements de credit dont l'agreement est cours de retrait)	2
Credit institutions—liquidation (Établissements de credit don't la liquidation est en cours)	7
Total	1,253

Source: Banque de France 2008

- legal practitioners and notaries (engaging in real estate and financial transactions or trust matters);
- auditors, tax consultants, accountants;
- real estate brokers; and
- casinos.

Germany's economy is the third largest in the world, when measured by market exchange levels. The German financial system is traditionally bank-oriented rather than stockmarket oriented.

Estimates of the number of regulated entities within the industries covered by Germany's AML/CTF legislation are not available in English. Table 13 presents the number of banks in Germany in 2004.

Table 13 Banks authorised in Germany, 2004 (n)

Credit co-op	1,340
Savings bank	477
Commercial banks	357
Regional banks	12
Total banks	2,186

Source: Library of Congress, Federal Research Division 2008

Hong Kong

Hong Kong's regulated sector encompasses legal practitioners, real estate agents, accountants, trust and company service providers, and the dealers of precious metals and stones, in addition to the banking and finance sectors. Regulated entities in Hong Kong's banking and finance sectors take in banks, deposit-taking companies, insurance companies and insurance intermediaries, money lenders, and securities and futures companies.

Table 14 estimates the number of businesses regulated for AML/CTF purposes in Hong Kong's financial sector, as well as MSBs and non-financial businesses. The FATF-GAFI (2008b) does not consider the non-financial businesses listed in Table 14 as included in Hong Kong's regulated sector. These industries have industry-based AML/CTF obligations rather than legislated (and externally enforceable) obligations.

Table 14 Regulated entities in Hong Kong, 2008–09—estimates of service providers

Sector	Business type	Entities (n)
Financial services	Banks	200
	Insurers	172
	Insurance agencies	2,342
	Insurance brokers	559
	Securities and futures	2,896
	Total	6,169
MSBs	Money lenders	741
	Remittance providers	1,760
	Total	2,501
Non-financial businesses	Accountants	3,705
	Real estate agents	4,589
	Legal practitioners—firms	712
	Notaries	380
	Total	>9,386
Total		>18,056

Sources: EAA 2009; FATF-GAFI 2008b; HKICPA 2009; HKMA 2009; Law Society of Hong Kong 2008; OCI 2009; Securities and Futures Commission 2009

Hong Kong's banking sector is substantial. Sixty-eight of the 100 largest banks in the world operated in Hong Kong in 2009 (HKMA 2009). Hong Kong's insurance industry is also substantial. In 2009, the industry was comprised of 172 companies. Of those companies, 46 were long-term insurers and 107 were general insurers. The remaining 19 offered composite services.

Singapore

Singapore's regulated sector is comprised almost entirely of businesses regulated by the Monetary Authority of Singapore (MAS). The only additional service providers with AML/CTF regulatory obligations are legal practitioners and approved trustees. The MAS is the issuing body of AML/CTF regulations for the financial sector and the Law Society of Singapore issues the AML/CTF requirements for legal practitioners. The Institute of Certified Public Accountants of Singapore is the regulating body for approved trustees.

The types of businesses regulated by the MAS include service providers that are considered MSBs in other countries. Tables 15 and 16 consider remittance providers, money changers and money brokers as MSBs. Tables 15 and 16 present figures from January 2010, with the exception of the number of legal practitioners in Singapore. The most current figures available for legal practitioners are from 2009 and these appear in both Tables.

Table 15 gives figures for the number of businesses providing financial services, MSBs and non-financial businesses with AML/CTF regulatory obligations. Financial service businesses represent 60 percent of the total regulated sector, MSBs approximately 15 percent and non-financial businesses 25 percent.

Table 15 Estimated size of the regulated sector in Singapore, 2009–10

Financial services	1,914
MSBs	473
Non-financial businesses	855
Total	3,242

Sources: CRA 2009; Law Society of Singapore 2009; MAS 2009

Capital markets service license holders include businesses that deal in securities and trade in futures contracts, leveraged foreign exchange traders, advisors on corporate finance, fund managers and businesses that provide securities financing and custodial services for securities. Multiple companies provide more than one of these services and are not counted for each service. Financial advisor's licence holders, from which banks and other entities registered with a different core business are exempt, have been included in Table 16 rather than as individual categories of advisors.

Republic of China (Taiwan)

Taiwan's regulated sector is almost entirely comprised of businesses defined as financial institutions. These are currently:

- banks;
- trust and investment corporations;
- credit cooperative associations;
- credit departments of farmers' associations;
- credit departments of fishermen's associations;
- Agricultural Bank of Taiwan;
- postal service institutions which also handle the money transactions of deposit, transfer and withdrawal;
- negotiable instrument finance corporations;
- credit card companies;
- insurance companies;
- securities brokers;
- securities, investment and trust enterprises;
- securities finance enterprises;
- securities investment consulting enterprises;
- securities central depository enterprises;
- futures brokers; and
- trust enterprises.

Taiwan has also included jewellery businesses in the AML/CTF regime. Jewellers in Taiwan play a substitute role for financial institutions and exchange large amounts of Taiwanese currency to foreign currency in addition to dealing in gems and gold.

Foreign currency exchange was added as a regulated service for AML/CTF in Taiwan in 2007. Foreign currency exchange can be carried out by a very wide range of businesses in Taiwan. The types of businesses permitted to provide this service are hotels, travel agencies, department stores, handicraft shops, jewellery stores, convenience stores, administrative offices of national scenic areas, sightseeing service centres, railway stations, temples, museums, institutions and associations providing services to foreign travellers in remote areas, and hotels located in remote areas. The number of businesses providing currency exchange services outside of their core business was not available. Table 17 shows the number of service providers for business types from the available information.

Table 16 Regulated entities in Singapore, 2009–10—estimates of service providers

Sector	Business type	Entities (n)
Financial services	Local banks	6
	Foreign banks	113
	Financial holding companies	1
	Merchant banks	46
	Representative offices of banks	33
	Institutions with Asian currency units	161
	Finance companies	3
	Singapore Government Securities Market—primary dealers	11
	Singapore Government Securities Market—secondary dealers	23
	Approved holding companies	1
	Approved exchanges	2
	Designated clearing houses	2
	Recognised market operators	25
	Holders of capital markets services licence	224
	Holders of financial adviser's licence	70
	Exempt financial advisers—companies providing financial advisory services to not more than 30 accredited investors	289
	Exempt fund managers—companies providing fund management services to not more than 30 qualified investors	486
	Exempt corporate finance advisers—companies advising on corporate finance to only accredited investors	122
	Exempt leveraged foreign exchange traders—companies carrying on business in leveraged foreign exchange trading for the purpose of managing customer's funds to only accredited investors	4
	Registered insurers	152
	Authorised reinsurers	6
	Lloyd's Asia scheme	20
	Representative offices of insurers and reinsurers	4
	Insurance brokers	63
	Exempt insurance brokers carrying on business as direct insurance brokers	23
	Other relevant organisations	24
	Total	1,914
MSBs	Money changers	377
	Remittances	86
	Money brokers	10
	Total	473
Non-financial businesses	Holders of trust business licence	40
	Exempt persons carrying on trust business—advocates and solicitors	32
	Legal practitioners (2009)	781
	Casinos	2
	Total	855
Total		3,242

Sources: CRA 2009; Law Society of Singapore 2009; MAS 2009

Table 17 Regulated entities in Taiwan, 2007—estimates of service providers

Sector	Business type	Entities (n)
Financial services	Insurance—life	30
	Insurance—other	24
	Domestic bank	45
	Foreign bank branches	36
	Credit cooperatives	29
	Farmers' association credit departments	253
	Fishermen's association credit departments	25
	Securities investment and trust enterprises	2
	Bills finance companies	14
	Postal savings system	1
	Agricultural Bank of Taiwan	1
	Futures brokers	Unknown
	Trust brokers	Bank's complete function
	Total	>460
MSBs	Currency exchange	Unknown
Non-financial businesses	Jewellers	Unknown
	Total	Unknown
Total		>460

Source: APG 2007

Comparative analysis and conclusions

The core financial institutions (the banking industry, finance companies and insurance industry) are regulated for AML/CTF purposes in all nine countries considered in this section. The variations in the regulated sectors between these countries are in the inclusion or exclusion of key MSBs and non-financial businesses.

Table 18 outlines the extent to which non-financial businesses have been integrated into the AML/CTF regimes of the countries considered. The way AML/CTF requirements are applied to legal practitioners across these jurisdictions shows the greatest variation. Hong Kong and Singapore have included legal practitioners in the full scope of the requirements. Legal practitioners in Germany, Belgium, the United Kingdom and France have obligations when dealing with customers in financial transactions or the settlement of real estate transactions. Legal practitioners in the United States, Taiwan and Australia have not been included unless, in Australia, the legal practitioner holds an Australian Financial Services Licence or provides a service designated under the AML/CTF Act. AUSTRAC estimated that fewer than four legal practitioners fell into this category into 2008. Legal practitioners in Australia are included in the scope of the older FTR Act.

The requirements for legal practitioners in the United Kingdom, France, Belgium, Germany and Singapore are further complicated by legal professional privilege. Legal professionals in these countries, which would otherwise have AML/CTF obligations for at least some transactions, are exempt from the obligation to report suspicious transactions under some circumstances. Where the information was gained in circumstances protected by legal privilege, the lawyer involved is not required to submit a report.

The non-financial businesses encompassed in Australia, the United Kingdom and Singapore (3

Table 18 Inclusion of non-financial businesses in AML/CTF regimes

Sector	Aus	US	UK	Belgium	France	Germany	HK	Singapore	Taiwan
Lawyer	No	No	Yes[a]	Yes[a]	Yes[a]	Yes[a]	Yes[d]	Yes	No
Accountant	No	No	Yes	Yes	Yes	Yes	Yes[d]	No	No
Real estate	No	No	Yes	Yes	Yes	Yes	Yes	No	Yes
Metal	Yes	Yes	Yes[b]	No	Yes[b]	No	No	No	Yes
Stones	No	Yes	Yes[b]	Yes[c]	Yes[b]	No	No	No	Yes
Casinos	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No[e]

a: Legal professionals do not have AML/CTF obligations unless engaging in financial or real estate transactions

b: Dealers in precious metals and stones are considered high-value dealers and are regulated

c: Diamond merchants are regulated in Belgium but not dealers of precious stones generally

d: FATF-GAFI does not include these as part of the regulated sector due to industry self-regulation

e: Casinos are currently illegal/not in operation

Table 19 Non-financial businesses, money service businesses and the financial sector as a proportion of the regulated sector in Australia, the United Kingdom and Singapore[a]

	Estimated entities (n)	Estimated proportion of total (%)
Non-financial businesses		
Australia	5,500	31.01
United Kingdom	>45,588	42.73
Singapore	855	26.37
MSBs		
Australia	7,000	39.55
United Kingdom	32,131	30.12
Singapore	473	14.59
Financial services		
Australia	5,200	29.38
United Kingdom	28,969	27.15
Singapore	1,914	59.04

a: Data available for each country

Source: AIC analysis

countries with the most data available to estimate the size of the regulated sector) contributed the largest proportion of the regulated sectors in those countries. Table 19 shows that the non-financial businesses regulated for AML/CTF in the United Kingdom comprised more than 40 percent of the total regulated sector in that country. The large representation of non-financial businesses in the United Kingdom's regulated sector is unsurprising given that accountants, real estate agents, high-value dealers and the gambling sector have been included.

Table 19 illustrates that the number of businesses providing financial services outweigh the number of those in the non-financial sector who provide money services in Australia and the United Kingdom. In Singapore, however, companies in the finance industry outnumber those in either the money service industry or a non-financial industry.

Estimates for the United Kingdom suggest that finance sector companies are the smallest component. Even with an absence of data for some regulated non-financial industries in the United States, the

Table 20 Regulated entities in the banking and insurance industries[a] (n)

Country	Banks	Insurance
Australia	57	103—all
United States	8,182	7,789—all
United Kingdom	400—including building society and e-money issuer	10,674—all
Belgium	105	Unknown
France	1,253	Unknown
Germany	2,186	Unknown
Hong Kong	200	172
Singapore	165	158—all and reinsurers
Taiwan	81	54—all
Total	12,582	>18,881

a: Data available for each country

Sources: APRA 2010a, 2010b

existing information suggests that finance sector companies also comprise a small number (20%) of the total regulated sector in the country. Hong Kong showed a similar pattern. The proportion of regulated businesses that fell into the finance sector in Hong Kong is approximately 30 percent.

A comparison across countries of the number of businesses providing regulated services is complicated by the different types of businesses providing the service and the lack of availability of data for some countries. Table 20 presents the figures (where available) for two of the core finance sector services regulated in all countries—banking and insurance.

In relation to the size of the regulated AML/CTF sector as a proportion of the entire business sector, the broad estimates provided in Table 20 show considerable variation, from Australia and the United States having approximately one percent of businesses being regulated for AML/CTF purposes to the United Kingdom with almost 10 percent regulated. The differences lie largely in the inclusion of the professional sectors in the United Kingdom, which account for very large numbers of businesses subject to regulation.

Conclusion

The lack of data for some countries and for some of the industries regulated for AML/CTF resulted in limitations in developing estimates of the size of the regulated sectors for each of the nine countries of interest. Despite the limitations, the information available suggests that there are common characteristics among some of the countries included. The most prominent of these was the apparent concentration of businesses with AML/CTF obligations in money services and non-financial industries.

The recent inclusion of many regulated services falling into the MSB and non-financial business categories means that a large proportion of all businesses with AML/CTF obligations are new additions to the regimes. The concentration of AML/CTF from MSBs and DNFBPs has several possible impacts for regulators, law enforcement, regulated businesses and for the effectiveness of the regime as a whole.

Businesses that have recently acquired AML/CTF regulatory responsibilities are, arguably, more likely to require assistance from regulatory bodies to

achieve compliance. The AML/CTF regime has expanded to include businesses, such as those from the gambling sector in Australia, with little experience with regulatory compliance and no experience with complying with financial regulation. This means that they need additional support to become compliant, with a particular focus on accessible training materials and education workshops (Walters et al. forthcoming). The fourth section will consider differences in the compliance activities of financial businesses and those from the money service and non-financial sectors.

Besides the difficulties newly included businesses might face complying with AML/CTF requirements is the potential for incomplete or ineffective compliance. This may include incomplete reports of suspect activities or difficulties instigating or adapting principles of risk-based compliance (AUSTRAC 2009g). One of the potential implications for law enforcement agencies and others accessing the financial intelligence gathered by an AML/CTF regime include reductions in the quality of the information gathered.

Extent of compliance and enforcement activity

The fourth section aims to compare the compliance of regulated businesses with the components of the preventative AML/CTF regimes in Australia, the United States, the United Kingdom and the selected countries in the European Union and Asia. Compliance activities and measures of compliance differ between these countries, reflecting the different regulatory requirements contained within each AML/CTF regime. This section compares compliance activity by measuring the volume of financial activity reports submitted by regulated entities and the volume of enforcement activity taken in each country against money laundering. Suspect transaction reporting and criminal money laundering prosecutions are common to all regimes but they remain proxy measures of compliance or enforcement activities within a single country.

This section also aims to compare the enforcement activity undertaken against the AML/CTF criminal provisions, an actions taken against regulated businesses for non-compliance, in those countries. The different approaches taken to criminal offences and regulatory compliance outlined in the second section make drawing conclusions from direct comparisons between countries problematic. The figures are better able to indicate changes over time within each country.

Australia

Compliance

The AML/CTF Act requires reporting entities to routinely submit three types of reports to AUSTRAC. These are significant cash reports (Threshold Transaction Reports), international wire transfer reports (IFTIs) and reports of suspicious financial activity. Individuals entering or leaving Australia are required by the AML/CTF Act to submit reports of cross-border movements of physical currency and cross-border movements of bearer negotiable instruments. Combined, these totalled over 19 million reports in 2008–09. The volume of each type of report can be seen in Table 21.

Suspicious matter reports (SMRs), required by the AML/CTF Act, may be filed by regulated businesses at any stage of providing, or proposing to provide, a service designated by the Act. Regulated businesses in Australia may file SMRs after providing a designated service or in the process of an enquiry about a service.

The number of SMRs submitted to AUSTRAC steadily increased between 2002–03 and 2005–06, with a one percent decrease in the number of reports submitted in 2006–07. The volume of reports increased once again in 2007–08 and 2008–09. The volume of reports was substantially higher in 2009 than in 2002. The trend in suspicious financial reports can be seen in Table 22.

Table 21 Reports submitted to AUSTRAC, 2008–09

Type of report	Reports (n)
Suspicious financial activity	32,449
Reports of high-value cash transactions	3,373,280
Reports of international movements of cash	38,669
Reports of international movements of instruments of value	1,635
Reports of international electronic transactions	16,325,870
Total reports	19,771,903

Source: AUSTRAC 2009a

Table 22 Suspicious financial activity reports submitted to AUSTRAC

Year	Reports (n)	Change from previous financial year (%)
2008–09	32,449	11.6
2007–08	29,089	19.0
2006–07	24,440	–1.5
2005–06	24,801	44.1
2004–05	17,212	49.9
2003–04	11,484	42.5
2002–03	8,054	3.1

Sources: AUSTRAC 2009a, 2007

Enforcement

FATF-GAFI criticised the rate of Commonwealth-level prosecutions in Australia for money laundering in the 2005 mutual evaluation (FATF-GAFI 2005b). FATF-GAFI highlighted that only five convictions were obtained between 2003 and 2005 for money laundering under the Criminal Code. The volume of charges dealt with by the CDPP has increased since the mutual evaluation (CDPP 2007). Table 23 outlines the number of defendants dealt with by the CDPP for money laundering-related offences between 2002–03 and 30 April 2010. The CDPP dealt with 74 defendants under the AML/CTF Act between 2006–07 and 30 April 2010.

The AML/CTF Act offers several types of penalties for non-compliance, such as criminal and civil penalties for contraventions and infringement notices for non-compliance with the reporting requirement for cross-border movements of instruments of value. Part 15 Division 5 of the Act allows AUSTRAC to give remedial directions to reporting entities, apply for injunctions and accept enforceable undertakings.

AUSTRAC's enforcement activity, as of December 2009, has resulted in three enforceable undertakings. AUSTRAC accepted the first two enforceable undertakings in July 2009, a third enforceable undertaking in November 2009 and a fourth enforceable undertaking in June 2010.

AUSTRAC may accept a voluntary undertaking from a person (or reporting entity) to comply with the AML/CTF Act, or Anti-Money Laundering and Counter-Terrorism Financing Rules, by taking or avoiding a specific action. The undertaking is usually accepted in lieu of pursuing criminal or civil penalties and is enforceable in court. It does not exclude the possibility of criminal, civil, or administrative action for any areas outside of the agreement or any areas of non-compliance identified once the undertaking has expired.

AUSTRAC may issue a remedial direction to reporting entities that have contravened a civil provision of the AML/CTF Act. The content of the direction aims to ensure the reporting entity no longer contravenes the civil provision and does not

Table 23 Defendants dealt with for money laundering offences, 2002–03 to April 2010 (n)

Act	2002–03	2003–04	2004–05	2005–06	2006–07	2007–08	2008–09	2009–10	Total
POCA s 81, s 82	1	9	0	1	3	0	1	0	15
Criminal Code s 400	n/a	5	6	11	14	40	42	50	168
AML/CTF Act	n/a	n/a	n/a	n/a	16	37	9	12	74
FTR Act	131	168	79	76	53	23	19	17	566
Total	132	182	85	88	86	100	71	79	823

Source: CDPP personal communication 23 June 2010

do so in the future. The remedial direction is enforceable in a court and contravening a remedial direction may result in a civil penalty. The AML/CTF Act allows the AUSTRAC chief executive officer to require regulated businesses to appoint an external auditor, undertake an external audit of the business' AML/CTF program or a specific aspect of the requirements and submit a report to AUSTRAC. AUSTRAC had issued seven written notices requiring an external audit by July 2010 (AUSTRAC 2010b).

Barclays Bank PLC—for its Australian branch, BarCap

AUSTRAC accepted an enforceable undertaking from Barclays Bank PLC, trading as BarCap in Australia, on 1 July 2009 (AUSTRAC 2009c). BarCap is licensed to operate a banking business and is a cash dealer under the FTR Act and a reporting entity under the AML/CTF Act. The enforceable undertaking stemmed from an onsite assessment conducted by AUSTRAC. AUSTRAC's concerns covered the reporting requirements as well as risk assessments of BarCap's customers, services, service delivery methods and dealings with higher risk countries, record-keeping requirements, customer identification procedures, correspondent banking procedures and the AML/CTF program (AUSTRAC 2009b). AUSTRAC also expressed some reservations about the legitimacy of assessing any of the services provided by an investment bank such as BarCap as low or medium-risk services (AUSTRAC 2009b).

The BarCap enforceable undertaking allows AUSTRAC to command documents to assess their compliance until the undertaking has expired. The enforceable undertaking required BarCap to commission an independent assessment of the company's compliance with the AML/CTF Act each year between 2009 and 2011. The undertaking expires in December 2011 or if BarCap implements a remedial action plan before this date (AUSTRAC 2009b).

Mega International Commercial Bank Co Ltd

AUSTRAC also accepted an enforceable undertaking from Mega International Commercial Bank Co Ltd (Mega) on 1 July 2009. Mega is licensed to operate a banking business in Australia. Mega undertook to develop and implement an AML/CTF program and record-keeping and customer identification systems, and to develop and implement systems to meet the reporting obligations under the AML/CTF Act and the FTR Act. Mega was directed to review all transactions between January 2002 and December 2009 and file all appropriate financial intelligence reports with AUSTRAC. Mega's enforceable undertaking further required the bank to commission external reviews of its compliance with the requirements of the undertaking and with the AML/CTF Act, and subsequent regulation and rules to be submitted to AUSTRAC (AUSTRAC 2009d).

Paypal Australia Ltd

Paypal Australia Ltd (Paypal) entered into an enforceable undertaking in November 2009. Paypal holds an Australian Financial Services Licence and is an authorised deposit-taking institution for purchase payment facilities. Paypal is further licensed to provide online payment mechanisms for goods and services. Paypal has undertaken to complete a revised risk assessment of its business and to review

and strengthen its risk management controls and AML/CTF program. Paypal, like BarCap and Mega, has also undertaken to engage an external consultant to conduct a review of aspects of its AML/CTF systems. Paypal's enforceable undertaking expires on 31 December 2011 (AUSTRAC 2009e).

Little Persia

AUSTRAC determined that Little Persia, a remittance service provider, was non-compliant with s 81(1) of the AML/CTF Act by failing to implement an AML/CTF program. Little Persia received a remedial direction for non-compliance in November 2009. The remedial direction directed Little Persia to submit a written AML/CTF program to AUSTRAC within 28 days of issue (AUSTRAC 2009f).

Eastern and Allied Pty Ltd

Eastern and Allied Pty Ltd, trading as Hai Ha Money Transfer, entered into an enforceable undertaking with AUSTRAC to implement a compliant risk management system, identify and report any deficiencies in its AML/CTF program and rectify those deficiencies (AUSTRAC 2010a).

The US Office of Foreign Asset Control has issued fines to both the Australian and New Zealand Banking Group Ltd and the National Australia Bank Ltd for dealing with assets in contravention of United States sanctions. The Australian and New Zealand Banking Group Ltd agreed to pay US$5,750,000 for transacting in contravention of US sanctions against Cuba and Sudan (US Department of the Treasury 2009). The National Australia Bank Ltd paid a settlement of $US100,000 for violations against US sanctions against Burma, Sudan and Cuba (US Department of the Treasury 2007).

United States

Compliance

The United States requires regulated entities to submit reports of suspicious financial activity and reports of high-value cash transactions to FinCEN. In total, approximately 18 million reports were filed in the 2008 fiscal year and 16 million of those were high-value cash transaction reports (FinCEN 2008).

The bulk of the remaining reports were Suspicious Activity Reports (SARs). Despite the difference in volume, SARs have overtaken the currency reports as the primary source of anti-money laundering information (Levi & Reuter 2006).

By 31 December 2008, over 6.7 million SARs had been filed with FinCEN since reporting began in the late 1990s (FinCEN 2009a) and the number of SARs filed annually has increased over the last 12 years. The numbers of SARs received by FinCEN, by year since 2002, are shown in Table 24. The increase in the number of reports between 2007 and 2008 was the smallest increase since 1996.

SARs tied to suspected terrorism financing increased in the months after the 11 September 2001 attacks. The volume of reports rose from just 27 in September 2001 to 1,342 in the following six months. These figures then decreased over the next year (Levi & Reuter 2006). FinCEN (2009a) reported a further 26 percent decrease in the number of SARs filed for suspected terrorism financing between 2007 and 2008.

Table 24 Suspicious financial activity reports filed with FinCEN (by fiscal year)

Year	SARs to FinCEN (n)	Change from previous year (%)
2008	1,290,590	3.21
2007	1,250,439	15.90
2006	1,078,894	17.37
2005	919,230	33.33
2004	689,414	35.92
2003	507,217	80.26
2002	281,373	

Source: FinCEN 2009a

The majority of reports are historically filed by the financial sector. Deposit-taking institutions filed 56.76 percent of SARs in 2008, MSBs filed 41.20 percent, casinos and card clubs filed 0.86 percent, and securities and futures companies filed 1.17 percent of the SARs FinCEN received in 2008 (FinCEN 2009a). SARs filed by non deposit-taking institutions fell between 2007 and 2008.

Structuring and money laundering remained the most common suspected offences that triggered

SARs filed by deposit-taking institutions in 2008. These two offences, and generic BSA activities, triggered 44 percent of reports. These activities, in previous years, generated 47 percent of reports.

Enforcement

The United States has an extensive history of enforcing Bank Secrecy Act violations and money laundering. Levi and Reuter (2006) estimated in 2006 that approximately 2,000 people were convicted of money laundering offences (as the primary offence or otherwise) each year in the United States between 1994 and 2001. The data reproduced in Table 25 illustrates that the proportion of money laundering charges that led to a conviction during that period ranged between 42 percent and 59 percent. Money laundering was one of the most serious charges laid against around 70 percent of those accused of a money laundering offence between 1994 and 2001.

One of the requirements of financial institutions in the United States is to develop adequate anti-money laundering programs and there have been numerous cases of enforcement action for failing to comply with this requirement. Some of these cases are outlined below. Despite the extensive regulatory enforcement activity historically, or perhaps because of the enforcement activity, there has been a decrease in the number of financial institutions found by FinCEN to have failed to develop anti-money laundering programs in recent years. FinCEN found around five percent of all institutions had an insufficient program in 2007, a decrease from almost eight percent in 2005 (FinCEN 2007).

Nevertheless, in 2007, FinCEN processed 248 actions against financial institutions with significant Bank Secrecy Act violations or deficiencies. This number was slightly up from 241 in 2006 (FinCEN 2007, 2006).

US banks, under the Bank Secrecy Act and the PATRIOT Act, must have anti-money laundering programs that meet four requirements:

- the development of internal policies and procedures;
- the designation of a compliance officer;
- an ongoing employee training program regarding AML/CTF issues; and
- an independent audit.

The following cases demonstrate that US financial entities of all sizes struggle with the current requirements for AML/CTF programs contained in the Bank Secrecy Act and PATRIOT Act. Each of the cases discussed are compliance-related cases which were dealt with by issuing a Consent to the Assessment of Civil Money Penalty Order (Consent Order) rather than going to court. Here, the entity involved agrees to pay a civil penalty for compliance failures. As a result, the cases have not reinterpreted either legislation and instead show the application of the regulations in detail. The substantial fines applied for the violations in question do not consider the size of the entity involved.

Table 25 Money laundering charges and prosecutions in the United States, 1994–2001

Year	Money laundering charges (n)	Money laundering convictions (n)	Money laundering convictions (as % of charges)
2001	2,110	1,243	58.91
2000	2,503	1,329	53.10
1999	2,656	1,371	51.62
1998	2,719	1,199	44.10
1997	2,376	1,108	46.63
1996	1,994	1,080	54.16
1995	2,138	906	42.38
1994	1,907	933	48.93

Source: Levi & Reuter 2006

Riggs Bank NA 2004

Riggs Bank entered into a Consent Order with FinCEN in 2004. FINCEN alleged that Riggs' AML/CTF program was inadequate. With regard to the first criteria outlined above, FinCEN noted that the bank did not assess risk in a systematic way across its various operations and that customer due diligence was not always followed (particularly with regard to accounts with overseas countries and politically exposed persons). The bank did not file SARs in a timely fashion and sometimes failed to file them at all. With regard to the second criteria, although a Bank Secrecy Act officer had been appointed, the officer in question failed to establish a procedure for effectively monitoring day to day performance or suspicious activity. With regard to the third criteria, FinCEN held that there was inadequate training of staff on AML/CTF risks, particularly for new customers and MSBs, evidenced by the lack of awareness of Rigg's staff on new MSB regulations. Finally, with regard to the final criteria, FINCEN held that the independent audit had not been timely or adequate and did not address key issues such as Bank Secrecy Act compliance, AML/CTF vulnerability, or the SAR process.

FinCEN determined that Riggs' conduct had taken place over a number of years and that it was wilful as Riggs had demonstrated a reckless disregard for its statutory or regulatory obligations. Riggs was fined US$25m.

Beach Bank, Miami Florida 2006

Beach Bank, in Miami Beach, Florida and the Beach Bank Liquidating Trust (an institution-affiliated party of the bank) were subjected to a FDIC cease and desist order due to concerns that the bank's management was not providing adequate guidance on compliance with the Bank Secrecy Act. The bank was a small state institution and the board was not experienced. The bank's compliance activities were deficient in a number of areas, including monitoring of MSBs, inadequate audits and poor adherence to 'know your customer'. Beach Bank and Liquidating Trust were fined US$400,000 each by FinCEN in 2006.

Union Bank of California NA 2007

The matter of Union Bank of California NA 2007 also concerned an inadequate AML/CTF program. The bank, in particular, did not have adequate internal systems for monitoring suspicious activity by high-risk customers, including a Mexican casas de cambio (a money exchange service). Though the bank had set up an internal financial intelligence unit in 2004, it failed to adequately resource this unit, resulting in many SARs being filed in an inadequate form, in a less than timely manner, or not filed at all. Union Bank was fined US$10m by FinCEN in 2007. The US Department of Justice further ordered Union Bank to forfeit US$21,600,000.

American Express Bank International, Miami, Florida 2007

FinCEN found issued civil penalties to American Express Bank International, Miami Florida and to American Express Travel Related Services Company Inc, Salt Lake City in 2007. FinCEN found that American Express Bank's anti-money laundering program was inadequate in a number of ways. The program lacked adequate internal controls, an adequate independent audit and failed to designate compliance personnel. FinCEN noted that the organisation's international profile made it more vulnerable than most companies to money laundering but that it nevertheless continued to operate without adequate safeguards. FinCEN found that the failure to comply with the Bank Secrecy Act were endemic to the bank's procedures and that there had been inadequate SAR filing for over US$500m worth of suspicious transactions. FinCEN's civil penalty for the compliance breaches of American Express Bank International was US$20m and a further US$5m for American Express Travel Related Services Company Inc. American Express Bank also forfeited US$55m.

United Bank for Africa PLC New York Branch, New York 2008

In 2008, the OCC found that the United Bank for Africa PLC New York Branch, New York (headquartered in Nigeria), had failed to institute an adequate anti-money laundering program. The OCC had issued the bank with a number of warnings about its shortcomings in this area.

The OCC's Consent Order noted the bank's failure to establish arrangements for politically exposed persons, including senior politicians in Nigeria and Nigerian diplomats, as well as other high-risk organisations such as MSBs, jewellery and precious metal dealers, import-export businesses and offshore corporations. The bank also failed to effectively monitor routine transactions for signs of money laundering.

The OCC found that branch personnel were not sufficiently trained to recognise suspicious activity and that the bank's compliance responsibilities were not clearly set out. The inadequate anti-money laundering program was assessed by an insufficient independent auditing system and the SAR activities of the bank were quite inadequate as 60 percent of the SARs filed from 2005 to 1 February 2008 were extremely late. The United Bank for Africa's Consent Order was for US$15m.

Sigue Corporation and Sigue LLC, San Fernando, California 2008

Sigue provides money transmission services to Mexico and Latin America through 7,000 agent businesses in the United States. Sigue entered into a deferred prosecution agreement for criminal charges for violations of the Bank Secrecy Act. The company failed to identify broader patterns of money laundering including transactions conducted by federal agents using funds which were represented to be illicit. Between 2003 and 2005, more than $24.7m in suspicious transactions were processed by agents of Sigue. Some of Sigue's agents were additionally found to be structuring transactions for their customers in order to avoid reporting requirements. FinCEN found that Sigue's anti-money laundering program was deficient in all four major areas.

Sigue agreed to forfeit US$15m to the United States Government. FinCEN applied a civil penalty of US$12m for non-compliance with the Bank Secrecy Act, however, this amount was deemed to be satisfied as part of the forfeited sum.

UBS, AG, Zurich, Switzerland 2004

A foreign bank, UBS, AG from Switzerland, was issued a $100m civil money penalty from the Federal Reserve Board, the second largest penalty ever issued. The civil money penalty was issued for banknote transactions with counterparties in jurisdictions subject to sanctions under US law. These included Cuba, Libya, Iran and Yugoslavia. UBS, AG was contracted to hold US dollar currency and distribute as needed, the contract required the bank to abide by US laws concerning money laundering and US embargo provisions. UBS, AG was not permitted to transact with these countries as it was not permitted under US law to do so.

El Noa Noa Corporation, Florida 2008

El Noa Noa consented to a US$12,000 civil money penalty for failing to establish and implement a reasonably designed AML/CTF program (FinCEN 2008). In addition to these regulatory actions, the United States also has a program to share information between financial institutions and law enforcement agencies through FinCEN. Section 314(a) of the PATRIOT Act allows FinCEN to send and receive requests for information concerning transactions and accounts of individuals or entities suspected of participating in money laundering or terrorism financing activities. FinCEN receives requests from law enforcement and sends them to financial institutions every two weeks. The requests must be checked against accounts from the previous 12 months and transactions in the previous six months. The program began in 2002 and between that time and 2009, FinCEN processed 1,061 requests for information, with 741 for money laundering and 320 for terrorism financing. More than 10,000 persons of interest were identified in the requests for information (FinCEN 2008). By 2007, 6,180 suspects were identified, leading to 129 arrests, 16 convictions and $46,982,753.64 located (FinCEN 2007).

Terrorism-financing convictions

Between 2002 and February 2007, the United States prosecuted 262 individuals with criminal violations of the terrorism financing statutes as outlined in the second section. Of the 262 individuals prosecuted for terrorism financing, 176 were convicted (TRAC 2007).

United Kingdom

Compliance

The UK Financial Intelligence Unit (UKFIU) receives SARs from all of the reporting entities in the United Kingdom. The United Kingdom does not have any threshold transaction reports, therefore UKFIU processes intelligence from SARs only. SOCA took over responsibility for the regime in October 2006 (SOCA 2007). The volume of reports submitted annually has increased substantially from the earlier years of the regime. In 2008–09, SOCA received over 220,000 SARs. The figures for reporting, including the last three years under SOCA, are shown in Table 26.

Table 26 Suspicious activity reports submitted in the United Kingdom, 2002–09

Year	SARs filed (n)	Change from previous year (%)
Oct 2008–Sept 2009	228,834	8.70
Oct 2007–Sept 2008	210,524	-4.52
Oct 2006–Sept 2007[a]	220,484	
2006	212,561	8.6
2005	195,702	26.6
2004	154,536	63.16
2003	94,718	69.07
2002	56,023	86.89

a: SOCA received SARs from October 2006

Sources: Harvey 2008; SOCA 2009b, 2007

The bulk of all SARs submitted in the United Kingdom are from banks. Banks submitted 69.71 percent of all SARs filed in 2007–08. The professional sectors (which include accountants, tax advisors, barristers, other legal professionals, solicitors, real estate agents, licensed conveyancers and high-value dealers) submitted 6.85 percent of SARs in 2008–09. Legal practitioners and accounting professionals submitted most of the SARs filed by the non-financial businesses. These two professions collectively filed 14,058 reports in 2008–09 (SOCA 2009a). The 14,058 reports from both profession combined represented a drop in the volume of reports from accountants and legal practitioners submitted in 2006–07. Accountants lodged 11,300 reports in 2006–07 and legal practitioners lodged 8,110 in the same year (SOCA 2007).

PricewaterhouseCoopers (2007) conducted 148 interviews with compliance professionals working in the financial sector in the United Kingdom on anti-money laundering topics. The survey results showed that most respondents indicated low levels of suspicious transactions within their business and submitted low numbers of SARs. Fifty-eight percent of the respondents reported fewer than six suspicious transactions per year. The figures are shown in Table 27. The implications of the findings are that the bulk of the reports received by UKFIU are submitted by a concentrated number of companies.

Table 27 Suspicious financial activity reports submitted by anti-money laundering survey respondents (n)

Suspicious reports per year (n)	Respondents (%)
Less than 6	58
6–20	20
21–50	9
51–100	3
101–500	4
501–1,000	1
More than 1,000	3
Don't know	2

Source: PricewaterhouseCoopers 2007

The UKFIU disseminated 956 SARs to the National Terrorist Finance Intelligence Unit in 2007–08. This figure fell to 703 in 2008–09 (SOCA 2009b).

Enforcement

Recent enforcement activity in the United Kingdom has resulted in 756 charges, 298 cases reaching the courts and 276 convictions recorded from information derived from SOCA intelligence (SOCA 2008b). In 2008–09, 67 people were charged with money laundering in SOCA cases (SOCA 2009a).

Table 29 below shows the volume of prosecutions and convictions for money laundering offences under each piece of legislation between 2001 and

Table 28 Institutions found to have failed to apply anti-money laundering regulations in the United Kingdom

Date	Institution	Reason	Sanction
Oct 2008	Sindicatum Holdings Limited, MLRO	Inadequate client identity controls	£49,000; £17,500
Nov 2005	Investment Services UK Ltd Bond Broker	Failure to control its business effectively in relation to anti-money laundering systems and controls	£175,000
Sep 2004	Bank of Ireland	Breaches of anti-money laundering requirements	£375,000
Apr 2004	Raiffeisen Zentralbank Österreich	Breach of money laundering rules	£150,000
Jan 2004	Bank of Scotland (now HBOS)	Breach of money laundering rules	£1,250,000
Dec 2003	Abbey National PLC	Breach of money laundering rules	£2,000,000
Aug 2003	Northern Bank Limited	Inadequate know your customer and identity verification	£1,250,000
Dec 2002	Royal Bank of Scotland PLC	Breaches of money laundering rules—inadequate know your customer requirements and record maintenance	£750,000
May 2002	Northern Ireland Insurance Brokers Limited	Involvement in financial crime including money laundering	No longer able to carry out any form of regulated activity and closed down in May 2003
Aug 2001	Paine Webber International (UK) Limited	Serious compliance failures including inadequate controls to prevent money laundering, know your customer requirements, record-keeping and staff training—imposed by SFA)	£350,000

Sources: FSA 2008, 2005, 2004a, 2004b, 2004c, 2003a, 2003b, 2002, 2001

Table 29 Money laundering prosecutions in the United Kingdom, 2001–04 (n)

Legislation	Numbers	2001	2002	2003	2004
ss 49–53 *Drug Trafficking Act 1994* (previously s 14 *Criminal Justice (International Cooperation) Act 1990* (s 49) and ss 24 and 23A of *Drug Trafficking Offences Act 1986*)	Prosecuted	91	129	80	43
	Convicted	43	40	50	28
	Conversion rate (%)	47.3	31.0	62.5	65.1
Criminal Justice Act 1988 (ss 93A–93D) as amended by the *Criminal Justice Act 1993* (ss 29–32)	Prosecuted	91	127	131	95
	Convicted	32	46	58	49
	Conversion rate (%)	35.2	36.2	44.3	51.6
Proceeds of Crime Act 2002 (ss 327–334)	Prosecuted			87	409
	Convicted			15	125
	Conversion rate (%)			17.2	30.6
Total for all legislation	Prosecutions	182	256	298	547
	Convictions	75	86	123	202

Source: UK Government Home Office cited in Harvey 2008

2004. The distribution of prosecutions and convictions under each instrument differed between years, although the total under all legislation increased annually. Table 29 also shows an increase in the percentage of prosecutions that resulted in convictions.

SOCA (2006) indicated that £3.3m were seized using the UK asset recovery provisions in 2006–07. Table 30 outlines the increased asset recovery rates by SOCA since 2006–07.

Table 30 SOCA UK's asset recovery, 2007–08 and 2008–09 (£m)

Type	2007–08	2008–09
Cash seizures	8.0	9.2
Cash forfeitures	2.9	4.5
Restraint orders	46.8	128.8
Confiscation orders obtained	11.6	29.7
Confiscation orders enforced	n/a	16.7

Source: SOCA 2009a

Belgium

Compliance

Belgium requires disclosures (of suspicious transactions) as the equivalent to STRs. Belgium does not use a list-based approach to reporting—where objective indicators lead to a report being made—instead, it requires reporting entities to do preliminary analysis themselves prior to submitting the report. This leads to a lower number of disclosures, but arguably a higher quality of information (CTIF-CFI 2006). The numbers of disclosures of suspicious financial activities are shown by year in Table 31.

Table 31 Disclosures of suspicious financial activity—by year

Year	Disclosures (n)	Change from previous year (%)
2008	15,554	21.23
2007	12,830	29.1
2006	9,938	-2.06
2005	10,148	-9.6
2004	11,234	12.9
2003	9,953	-24.1
2002	13,120	

Sources: CTIF-CFI 2008, 2007, 2006

There was a 30 percent increase in the number of disclosures between 2006 and 2007, and an increase in the number of investigation files created by CTIF-CFI, which brought the number to 4,927. One explanation for this increase is a 2007 amendment to the legislation which altered the requirements for reporting transactions suspected to be linked to serious and organised tax fraud. Regulated entities are now obligated to submit a report of these matters as soon as any indicator of this activity emerged (CTIF-CFI 2007a). The increasing volume of reports submitted to CTIF-CFI continued in 2008 with a similar number of new investigation files opened as a result (CTIF-CFI 2008).

A high percentage of the disclosures received by CTIF-CFI are submitted to justice officials for prosecution. Between 2000 and 2003, 5,000 money laundering cases were submitted to Belgian justice officials, resulting in 800 convictions for money laundering during this period (FATF-GAFI 2005a). CTIF-CFI submitted 1,166 files to the public prosecutor in 2007. This was approximately 23.7 percent of the total number of investigation files opened. CTIF-CFI sent 937 files to prosecutors in 2008. An investigation file can be the result of several disclosures, meaning the total number of files is less than the total number of disclosures (CTIF-CFI 2007a).

The majority of files reported to the public prosecutor in Belgium represent funds identified in the layering stage of money laundering. Serious tax fraud was the most common suspected predicate offence (accounting for 23.7% of cases in 2008), followed by trafficking in goods and merchandise (20%) and misappropriating corporate assets (15.1%; CTIF-CFI 2008).

CTIF-CFI dealt with 175 investigation files for terrorism matters between 1993 and 2007 and 32 of these were in 2007 (CTIF-CFI 2007a). A total of 21 files tied to terrorism or terrorism financing in 2008 (CTIF-CFI 2008).

Enforcement

In 2003, 1,214 money laundering cases were dealt with in Belgium. The most recent estimate available on the forfeiture and confiscation of funds generated by organised crime was €102m in 2001 (FATF-GAFI 2005a). Belgium confiscated €747.5m in 2008 (CTIF-CFI 2008).

France

Compliance

TRACFIN received approximately 12,000 STRs in 2006 (Favarel-Garrigues, Godefroy & Lascoumes 2008). The IMF remarked in their evaluation of France that the level of reporting still appears low when considered in the context of the financial and economic market, despite the numbers of reports increasing between 2000 and 2005. The volume of reports nearly doubled from approximately 6,800 in 2002 to approximately 12,000 in 2006. The number of reports submitted between 2002 and 2006 are displayed in Table 32.

Table 32 Suspicious financial activity reports to TRACFIN

Year	Reports (n)	Change from previous year (%)
2008	14,565	16.81
2007	12,469	3.38
2006	12,047	4.2
2005	11,553	6.55
2004	10,842	20.2
2003	9,019	3.4
2002	8,719	

Sources: TRACFIN 2008, 2006

The increased volume of reporting was not necessarily matched by an increase in quality, as the number of reports forwarded onto judicial authorities remained limited. Approximately 10 percent (n=269) of the reports filed in 2003 were forwarded on (IMF 2005). By 2006, the figure had increased to approximately 400, representing just over three percent of the total number of reports (Favarel-Garrigues, Godefroy & Lascoumes 2008). TRACFIN referred 359 cases to judicial authorities in 2008 (TRACFIN 2008).

In France, the financial sector submits the largest proportion of STRs, although the volume of reports submitted by MSBs and non-financial business is increasing. Financial services businesses accounted for 98 percent of reports filed in 2005, 97 percent of reports filed in 2006, 88 percent of reports in 2007 and 86 percent of reports in 2008 (TRACFIN 2008, 2006). Banks generate the most STRs in France, accounting for about 80 percent in the years between 2005 and 2008 (TRACFIN 2008, 2006).

The levels of reporting by businesses outside of the banking sector (particularly from investment companies, casinos and high-value dealers) increased after 2000 (IMF 2005). By 2008, non-financial businesses accounted for a little over four percent of STRs, while MSBs submitted approximately 10 percent of reports (TRACFIN 2008).

IMF (2005) suggested that the low levels of reporting might be the result of inadequate supervision of these sectors. The exception to the trend of low reporting by non-financial businesses is the experience of notaries. Notaries were responsible for 56 percent of the reports filed by non-financial businesses in 2006 and 2008 (TRACFIN 2008, 2006).

Enforcement

The 359 cases TRACFIN referred to judicial authorities in 2008 included 179 cases for money laundering and, of these, 175 went before the courts. Table 33 outlines the volume of convictions for money laundering in France between 2004 and 2007. TRACFIN referred 410 cases to the judicial authority in 2007 (TRACFIN 2007).

Table 33 Money laundering convictions in France, 2004–07 (n)

Year	Ordinary money laundering	Aggravated money laundering	Total
2007	80	62	142
2006	55	21	76
2005	32	90	122
2004	23	25	48

Source: TRACFIN 2008

In 2007, 17 of TRACFINs cases alleged terrorism financing and went to the prosecutor's office (TRACFIN 2007). In 2008, five cases involving suspected terrorism financing were directed to the prosecutor's office (TRACFIN 2008).

TRACFIN has been operational since 1991 and has powers to block or freeze transactions for 12 hours after receiving an STR about the proposed transaction. This procedure, however, had only been used on seven occasions up until 2005 (IMF 2005).

Germany

Compliance

The suspicious transaction reporting regime in Germany requires regulated businesses to combine transactions tied to one customer into a single report. The numbers of STRs filed by regulated entities in Germany declined in 2003 and did not reach the same levels of reporting seen in 2002 until 2006 (FIU Germany 2006). Reporting volumes fell in 2007 and again in 2008 (FIU Germany 2008). The number of reports received by FIU Germany between 2002 and 2008 appear in Table 34.

The reporting rate for financial services fell between 2007 and 2008, whereas the volume of reports from non-financial businesses increased slightly (FIU Germany 2008). More than 80 percent of STRs submitted in 2006 were filed by credit institutions. The number of reports filed by credit institutions fell by 22 percent in 2007 and a further 13 percent in 2008. Legal practitioners, notaries, auditors, tax consultants, asset managers and other businesses filed 32 reports in 2008. This was an increase on the 13 reports filed by these sectors in 2006 (FIU Germany 2008).

Reports can also be filed in Germany by individuals and entities outside the regulated sector. These can be filed by private citizens, tax authorities, law enforcement authorities, the German customs service and other government agencies. Persons and entities outside the regulated sector filed 530 reports in 2006 (FIU Germany 2006). German tax authorities filed 25 percent fewer reports in 2008 than in 2007 (FIU Germany 2008).

The most common reason or suspicion cited in the STRs in 2008 was fraud, followed by document forgery and tax evasion, with 1,566 listings (FIU Germany 2008). The volume of listings for document forgery, tax offences and insolvency offences rose in 2008.

Table 34 Suspicious financial activity reports filed in Germany, 2002–08

Year	Reports (n)	Change from previous year (%)
2008	7,349	-23.55
2007	9,080	-9.66
2006	10,051	21.9
2005	8,241	2.2
2004	8,062	22.1
2003	6,602	-30.4
2002	8,612	–

Sources: FIU Germany 2008, 2006

Terrorism financing

Germany also publishes statistics on the volume of STRs linked to the financing of terrorism. Table 35 displays the number of reports filed between 2003 and 2008 documenting transactions suspected to be linked to terrorism financing. These accounted for between 0.6 percent and two percent of STRs. Prosecutors advised BKA on the outcome of 24 of the 65 reports filed in 2008 and each was discontinued due to insufficient suspicion (FIU Germany 2008).

Table 35 Suspicious financial activity reports relating to the financing of terrorism

Year	Reports (n)	STRs (as a % of total)
2008	65	0.9
2007	90	0.9
2006	59	0.6
2005	104	1.3
2004	114	1.4
2003	127	2

Source: FIU Germany 2008, 2006

Enforcement

The public prosecutor's office provided FIU Germany with 3,850 follow-up responses to suspect transaction reports in 2008, although the responses provided are not confined only to reports filed in 2008. Most (around 90%) noted that proceedings had been discontinued. The remaining responses reported that the reports had resulted in an indictment, penalty order, or judgement, or were relevant to other cases or pending investigations (FIU Germany 2008). The reported outcomes for 2007 and 2008 appear in Table 36. FIU Germany notes a correlation between the number of STRs filed in 2008 and the fall in each of the reported outcomes (FIU Germany 2008).

Table 36 Reported outcomes to financial intelligence unit Germany, 2007–08 (n)

Outcome	2007	2008
Indictment	58	42
Penalty order	130	138
Judgement	15	30
New investigation	118	99
Pending investigation	37	33

Source: FIU Germany 2008

The number of money laundering offences recorded under s 261 of the Penal Code more than doubled between 2002 and 2007, rising from 1,061 to 3,923. After a 40 percent decline in 2003, the number of recorded offences increased each year to 2007. These figures are displayed in Table 37. The clearance rate reflects the percentage of cases cleared up each year.

Table 37 Offences for money laundering, concealment of unlawfully acquired assets (s 261 Penal Code) in Germany, 2002–08

Year	Cases (n)	Change from previous year (%)	Clearance rate (%)
2008	2,582	-34.2	94.0
2007	3,923	30.9	94.9
2006	2,997	10.3	91.8
2005	2,023	160.6	80.8
2004	776	4.2	96.6
2003	745	-42.4	96.5
2002	1,061	20.9	95.6

Sources: BKA 2008a, 2007, 2006a, 2005, 2004a, 2003

BKA reported conducting 186 investigations into alleged money laundering in 2008 which led to filing 511 STRs tied to 92 cases (BKA 2008b). BKA seized €169.9m in assets in 2008. This is much higher than the provisional seizures made in 2003 (€69m) and 2004 (€68m; BKA 2004b). The elevated 2008 figure is the result of two seizures made in that year.

Singapore

Compliance

The volume of STRs submitted in Singapore increased each year between 2004 and 2008 (see Table 38). The largest increase occurred between 2006 and 2007, where the volume of reports submitted more than doubled. Report numbers showed a more modest increase of 68 percent between 2007 and 2008.

Table 38 Suspicious financial activity reports in Singapore, 2004–08

Year	Reports (n)	Change from previous year (%)
2008	12,158	67.44
2007	7,261	120.7
2006	3,290	58.4
2005	2,076	16.36
2004	1,784	

Source: STRO 2009

Singapore's Commercial Affairs Department (CAD), housing the STRO, were receiving 90 percent of reports electronically by March 2009 (CAD 2009). CAD introduced the Web-based Intelligence aNalytical [sic] and Graphical Visualisation System in 2008 (CAD 2008). This system facilitates prioritising and analysing STRs and automatically processes and assigns cases for action.

Enforcement

Information gathered from STROs assisted CAD, directly or indirectly, to recover SGD$110m in assets between 2000 and 2007 (CAD 2007). Singapore convicted 41 people of money laundering between 2005 and 2008. FATF-GAFI (2008a) viewed the volume of money laundering convictions in

Singapore as low for the size of Singapore's financial sector at the time of the mutual evaluation and suggested that cases focused on predicate offences rather than money laundering prosecutions. In 2008, a vast increase was seen in the volume of total convictions and the number of convictions where the launderer was not dealing with the proceeds generated by their own crimes. The money laundering convictions in Singapore for each year appear in Table 39.

Table 39 Money laundering convictions in Singapore, 2005–08 (n)

Year	Third-party money laundering convictions	Total convictions
2008	19	24
2007	2	13
2006	Unknown	2
2005	Unknown	2

Source: CAD 2009

Hong Kong

Compliance

Hong Kong had a large increase in the volume of between 2004 and 2007. Financial services businesses submitted the majority of reports in that period (see Table 40) and the volume of reporting from these businesses remained steady in that time. Four banks, holding around 50 percent of customer deposits in 2007, submitted approximately 70 percent of STRs made to JFIUHK between 2003 (FATF-GAFI 2008b).

Table 41 provides more detail on the volume of reports submitted by each type of regulated business in Hong Kong. Remittance agents and money changers showed a substantial increase in reporting volumes in 2006 and 2007 from that of 2003. The increase may have been tied to education seminars hosted by JFIUHK and some prosecutions for non-compliance (FATF-GAFI 2008b).

The non-financial business regulated in Hong Kong submitted very few reports between 2003 and 2007. Legal practitioners made the most reports during this period, although this amounted to only 13 reports. No businesses in the precious metals and stones industry made a report during this period.

Table 40 Suspicious financial activity reports filed in Hong Kong, 2004–07 (n)

Business sector	2004	2005	2006	2007
Financial services	13,827	13,169	13,329	13,362
MSBs	132	268	1119	2001
Non-financial services	17	16	17	17
Total	13,976	13,453	14,465	15,380

Source: FATF-GAFI 2008b

A very small proportion of STRs filed between 2003 and 2007 were tied to the financing of terrorism. Table 42 shows that JFIUHK, in most years with the exception of 2003, received 20 or fewer reports outlining behaviour suspected to be tied to financing of terrorism. Some investigations stemming from reports made by businesses for other matters were later tied to suspected terrorism financing during the course of the investigation. These have also been counted in Table 42.

Hong Kong initiated 104 prosecutions against remittance agents and money changers between 2000 and 2007 for failing keep the required identification records for transactions of HK$8,000 or more. The maximum penalty handed down for these prosecutions was a fine of HK$100,000, one month's imprisonment and suspending the licence to operate for one year (FATF-GAFI 2008b). Fines of HK$30,000 were imposed in 77 cases for failing to register the remittance or money changing business in the same period (FATF-GAFI 2008b).

The OCI sanctioned 22 insurance companies between 2004 and 2007 for failing to keep appropriate identification records. It issued eight oral warnings and 24 written warnings for non-compliance to these companies (FATF-GAFI 2008b).

The Securities and Futures Commission fined 14 companies for AML/CTF non-compliance between 2004 and 2007 and suspended a further 36 companies in the same period. It imposed fines between HK$30,000 and HK$700,000 for non-compliance and suspended licenses for between one month and two years and nine months (FATF-GAFI 2008b).

Table 41 Suspicious transaction reports submitted in Hong Kong by sector, 2004–07 (n)

Business sector	Business	2004	2005	2006	2007
Financial services	Banking	13,570	12,449	13,041	12,789
	Insurance	144	560	132	311
	Licensed money lenders	37	10	35	42
	Securities and futures	76	150	121	220
Total financial services		13,827	13,169	13,329	13,362
MSBs	Remittance agents and money changers	132	268	1,119	2,001
Total MSBs		132	268	1,119	2,001
Non-financial services	Accountant	1	0	0	3
	Lawyer	13	5	11	9
	Trust and company	2	11	6	5
	Real estate	1	0	0	0
	Precious metals and stones	0	0	0	0
	Other[a]	53	52	92	77
Total non-financial services		70	68	109	88
Total per year		14,029	13,521	14,557	15,468

a: Businesses or individuals that are not designated non-financial businesses or professions

Source: FATF-GAFI 2008b

Table 42 Suspicious financial activity reports related to terrorism financing, 2003–07

Year	Reports (n)	SARs (as a % of total)
2007	20	0.13
2006	19	0.13
2005	9	0.07
2004	14	0.10
2003	73	Unknown
Total	135	

Source: FATF-GAFI 2008b

Table 43 Persons convicted of money laundering in Hong Kong, 2004–09 (n)

Year	Persons convicted of money laundering (n)	Prosecutions for money laundering (n)
2009	232	Unknown
2008	248	364
2007	179	310
2006	92	116
2005	84	57
2004	49	40

Sources: DoJHK 2009, 2008, 2007, 2006, 2005; JFIUHK 2009

Enforcement

The number of individuals convicted for money laundering in Hong Kong began to increase substantially in 2004 (see Table 43), with the highest number of convictions recorded in 2008 (JFIUHK 2009). In 2008, Hong Kong convicted 248 people for money laundering from 364 prosecutions (DoJHK 2009).

In 2008, Hong Kong issued 16 restraint orders, with a total value of HK$409.98m. Asset recovery orders issued under OSCO totalled HK$11.01 and HK$1.38m under the Drug Trafficking (Recovery of Proceeds) Ordinance. Hong Kong recovered a further HK$21.51m in assets in 2008.

In 2007, orders for confiscating HK$19.45m in cash and HK$2.11m in assets were sought under OSCO. Further, orders for confiscation under DTROP were valued at HK$377,000 for cash and HK$795,000

worth of assets (DoJHK 2008). In 2006, HK$4.447m of crime proceeds was confiscated. A further HK$40.003m was restrained pending court proceedings (DoJHK 2007). Table 44 outlines the proceeds of crime recovered in Hong Kong under OSCO between 2004 and 2008.

Table 44 Proceeds of crime confiscated in Hong Kong, 2004–08

Year	OSCO (HK$m)	DTROP (HK$m)	Assets (value in HK$m)
2008	11.01	1.38	21.51
2007	19.45	0.38	2.90
2006	4.45	Unknown	Unknown
2005	18.11	Unknown	Unknown
2004	14.80	Unknown	Unknown

Sources: DoJHK 2009, 2008, 2007, 2006, 2005

Republic of China (Taiwan)

Compliance

Taiwan requires regulated entities to submit both SARs and reports of high-value cash transactions. Table 45 lists the volume of SARs submitted to the Taiwan FIU between 2004 and 2007, and the proportion of those forwarded from the FIU to law enforcement units within the Investigation Bureau or to external police or other agencies. The volume of SARs submitted by regulated entities in 2005 decreased dramatically from the 2004 figure. The number of reports the FIU forwarded to the law enforcement community remained steady between those two years. The figures provided in Table 45 do not include any reports made by businesses from the precious metals and stones sector. The APG expressed serious doubts about the effectiveness of the requirement for these businesses to make reports, as the sector had not submitted SARs by 2007 (APG 2007).

Table 45 Suspicious transaction reports submitted in Taiwan, 2004–07

Year	STR volume (n)	Sent to law enforcement (n)	Total sent to law enforcement (%)
2007	1,741	383	22.00
2006	1,281	478	37.31
2005	1,034	239	23.11
2004	4,689	299	6.38

Source: MJIB 2008, 2007, 2006, 2005

Around 45 percent of SARs submitted in 2007 identified transactions of NT$1m (US$31,000) or less. Just under eight percent involved more than NT$30m (US$945,000; MJIB 2007).

Domestic banks submitted the largest proportion of SARs lodged in Taiwan between 2004 and 2007 (see Table 46). Postal services offering remittance transfers submitted 20 percent of the reports lodged to the FIU in 2007 but only filed eight SARs in 2006. The fall in the proportion of reports lodged by local banks in Taiwan, and the increase in the volume of reports lodged between 2006 and 2007, are both consequences of the increased levels of reporting by postal services businesses.

Table 46 Suspicious activity reports originating in local banks in Taiwan, 2004–07

Year	Total SARs (n)	Local bank submissions (%)
2007	1,741	56
2006	1,281	75
2005	1,034	63
2004	4,689	97

Source: MJIB 2008, 2007, 2006, 2005

Enforcement

District prosecutors prosecuted 31 money laundering cases in 2007, a substantial decrease on the prosecutions undertaken in Taiwan in previous years (see Table 47). In 2007, the value of the money laundering proceeds from the cases prosecuted in Taiwan (including summary matters and deferred cases) was the highest for the period examined. The majority of money laundering cases each involved more than NT$30m in proceeds. The value of most cases in 2006 was less than NT$100,000 (MJIB 2007).

Table 47 Money laundering prosecutions and proceeds in Taiwan, 2004–07

Year	Money laundering prosecutions (n)	Money laundering proceeds (NT$)
2007	31	69,103,390,744
2006	691	5,110,747,140
2005	1,171	7,709,658,074
2004	809	unknown

Source: MJIB 2008, 2007, 2006, 2005

Twenty-eight of the 31 money laundering cases prosecuted in Taiwan in 2007 involved financial institutions. Two cases involved alternative remittance services and one case involved purchasing real estate. The most common money laundering approach employed by defendants was to open a dummy account at a bank (MJIB 2008). This was also the case in 2005 and 2006. Table 48 shows the money laundering cases that have involved a business outside of the financial sector.

Comparative analysis

Compliance

Suspicious financial activity reports—reporting volume

The volume of reports submitted to authorities in Hong Kong, Singapore, France, the United Kingdom, the United States and Australia steadily increased over the period for which reporting data were available. The regulated sector in each country generally submitted far more reports in 2008 or 2008–09 than in the base year for which data were available. Singapore's FIU experienced an increase in reports of more than 580 percent between 2004 and 2008. Report numbers in the United Kingdom and United States grew by 308 percent and 359 percent respectively. Singapore's increased reporting volume between 2004 and 2008, unlike the European Union countries, was not accompanied by an increase in the number of businesses in the AML/CTF regime at that time.

Table 48 Businesses allegedly used to launder money, 2005–07

Institution	Cases in 2007 (n)	Cases in 2006 (n)	Cases in 2005 (n)
Financial institutions			
Banks	24	465	871
Postal services engaged in money transfers	2	213	287
Credit unions	1	4	6
Famers' and fishermen's credit associations	1	2	2
Securities companies	0	2	2
Subtotal	28	686	1,168
Non-financial institutions			
Underground banking	2	2	2
Purchase of real estate	1	1	1
Purchase of precious metals	0	1	0
Other means	0	1	0
Grand total	31	691	1,171

Source: MJIB 2008, 2007, 2006, 2005

Germany and Taiwan recorded a fall in the volume of reports over the period of available data. In 2007, Taiwan's FIU received less than 40 percent of the reports filed in 2004. Germany's FIU received 14 percent fewer reports in 2008 than in 2002.

Reports by sector

Businesses in the financial services sector submitted the largest proportion of reports for each of the countries considered in this report. This remains true even for countries where non-financial businesses constitute a large percentage of the regulated sector.

Financial service businesses submitted 57 percent of reports filed with the US FIU in 2008, 70 percent of those filed in the United Kingdom in 2007–08, 86 percent of those filed in France in 2008 and 87 percent of reports filed in Hong Kong in 2007. Foreign exchange offices and credit institutions initiated 80 percent of reports filed in Belgium in 2007.

Despite the monopoly that financial services businesses retain on reporting suspect transactions in each of the countries in this sample, these businesses account for only a small proportion of the businesses regulated for AML/CTF. This is particularly evident in the United Kingdom where over 60 percent of reports in 2006–07 came from the financial sector, which accounted for only 14 percent of regulated businesses in that year.

Likewise, the United States saw more than half of the reports filed in 2008 lodged by deposit-taking institutions, which represented around 20 percent of businesses with AML/CTF obligations (see Table 49).

The non-financial businesses in the countries considered in this report were still filing low numbers of reports in the last year for which data were available. Numbers of reports were low in volume or non-existent. Professions with reporting requirements in the United Kingdom were responsible for only eight percent of suspicious reports in 2007, with the majority of these submitted by solicitors and accountants. In 2007 in Belgium, less than two percent of reports originated from non-financial businesses (excluding notaries), with legal practitioners and real estate agents submitting only three and two disclosures respectively. In Taiwan, only high-value dealers are required to submit reports. No businesses in this industry had submitted a report prior by 2007. The United States was the only country in this report to show comparable levels of reporting between the different sectors, with 48 percent of suspicious financial transaction reports in 2007 submitted by businesses outside of the financial sector. These businesses, however, were MSBs and not non-financial businesses or professions. Gambling businesses, the only non-financial industry regulated for AML/CTF in the United States, filed less than one percent of the reports for 2008.

Table 49 Suspicious financial activity reports submitted from the financial sector based on proportion of that sector

Country	Reports 2006–07[a] (n)	Percentage from finance sector/banks	Finance sector/banks proportion of regulated sector (%)[b]
Australia	24,440	Unknown	29.6
United States	1,157,468	51.9	20.0
United Kingdom	220,484	63.6	14.0
Belgium	12,830	79.6	Unknown
France	12,047	96.8	Unknown
Germany	10,051	80.0	Unknown
Singapore	7,261	Unknown	21.2
Hong Kong	15,363	Unknown	22.9
Taiwan	n/a	Unknown	Unknown

a: Year periods may differ due to difference in Australian and international fiscal years. France and Germany have 2006 data only, Singapore and Hong Kong have 2007 data, data from Taiwan was not available

b: Estimate only based on figures available in the second section

Source: AIC analysis

Report numbers

KPMG's (2007) global AML survey of over 200 banks and executives showed that 72 percent of respondents reported some level of increase in the number of reports of suspicious activities in the three years prior to the survey. Respondents indicated that the increase could be attributed to improved reporting systems, such as electronic filing, and increased staff awareness.

KPMG's findings suggest that the increased volume of reports does not reflect an increased volume of suspicious activity, at least as far as the financial industry is concerned, but rather an increased capacity to capture it. Amendments to the anti-money laundering regimes in each of the countries considered are also likely to have an impact on the volume of reports received, rather than increased levels of suspicious activities as such.

The way countries structure their reporting requirements will have a direct impact on the volume of reports lodged. The amount of in-house analysis that businesses are required to undertake prior to reporting a transaction will also reduce the number of reports. Countries such as Germany and Belgium require businesses to undertake some initial analysis of a reportable matter prior to submitting a report to authorities. This approach aims to systematically improve the quality of submitted reports but also to reduce the volume received. German reporting entities also combine suspect transactions tied to a single matter into one report. Countries such as Australia do not direct businesses to combine connected suspect matters into a single report and these countries will have higher report volumes, even if the portion of suspect matters remain the same. Each approach to submitting reports reveals different kinds of information. Report counting may indicate the volume of data received and potentially dealt with by the FIU and case counting may better indicate the number of individuals considered for assessment.

There are many factors that lie outside the amount of illicit activity taking place that may influence the overall volume of reports of suspect transactions in the countries considered in this report. The most direct influence on the volume of reports submitted in any particular country is the volume of transactions that might be illicit; the number of businesses that might be exposed to these transactions that are capable of reporting them; and the number of businesses that are likely to report them.

Countries with larger economies, and presumably with more businesses operating and more transactions taking place, should have larger numbers of reports even if the proportion of all transactions that are potentially illicit remain the same between nations. Economic growth within a single economy might also account for a portion of the increased volume of reported transactions even without any growth in the percentage of suspicious transactions. The international and regional importance of the financial services sector of a specific country may increase the volume of transactions, particularly transnational transactions, taking place through financial services businesses. The size and significance of the US economy is likely to have had an impact on the volume of reports submitted to FinCEN in 2008. An examination of the volume of reported suspect transactions as a proportion of the overall number of transactions would provide a more reasonable basis of comparison between countries such as Australia and the United States, but this information was not collected or reported for the timeframes under consideration in this report.

Extending the regulated sector to include more money service and non-financial businesses should increase the volume of suspect transaction reports as there are more businesses to monitor potentially illicit transactions from industries theoretically likely to be exposed to risks of money laundering. This is the basic premise for the FATF-GAFI's inclusion of the designated non-financial businesses and professions in its Recommendations. The countries in the sample considered in this report, however, do not reflect the assumption that expanding the regulated sector would lead to reports from a larger range of businesses. Financial service businesses and non-financial businesses lodged disparate volumes of reports in every country.

Businesses that have been subject to AML/CTF regulations for longer periods of time are likely to be better placed to monitor transactions more effectively and to submit more reports even if the proportion of all transactions that might be illicit were to remain the same. The experience of Australian

businesses included in the AML/CTF regime strongly suggests that capacity building within business sectors that are new to financial regulation is crucial to increase their ability to become compliant (Walters et al. forthcoming). The relationship between business sector—financial, money service and non-financial businesses—and lodging suspect transaction reports, however, is likely to be more complicated than a lack of capacity in some industries.

The low levels of reporting from businesses outside of the financial sector cast doubt on the effectiveness of the regime in reaching these industries. The IMF suggested that the inadequate supervision of non-financial industries in France is one explanation for the low numbers of reports by these industries (IMF 2005). The recent changes to regulatory regimes in several countries, including Australia and those in the European Union, means that it is too early to adequately evaluate the level of compliance in this area. Any change to AML/CTF legislation, such as expanding the requirements for each business or expanding the scope of regulated sector as occurred in Australia in 2006, is likely to influence compliance. Businesses are likely to take some time to grasp the new requirements, while regulators are likely to shift resources away from enforcement-orientated compliance monitoring to education and training. Awareness raising, education and training became focus areas for the Australian regulator, AUSTRAC, in 2009–10 (AUSTRAC 2009g).

The compliance strategies in the United States and Australia have, however, extended enforcement actions to businesses outside the financial services sector. This is more evident in the United States, where the existing AML/CTF regime pre-dated that of Australian legislation by a number of years. MSBs in the United States have been the subject of a number of enforcement actions and financial penalties which may have influenced the volume of reported transactions identified and filed by MSBs there.

The number of reported transactions, and other proxy measures of compliance, are also likely to be influenced by world events and international political will. The 11 September 2001 attacks acted as a significant prompt to change AML/CTF legislation in a number of countries, as the political will to focus on money laundering and the financing of terrorism altered with the perception of risk. The Mutual Evaluation process, a mark of international political will, prompted substantial changes to the Australian regime in 2006. A more sophisticated analysis of compliance with AML/CTF across different countries would be useful to plot any changes in report numbers against changes in the budgets of AML/CTF regulators and FIUs.

Enforcement

Effective reporting

In 2007, Belgium had one of the highest percentages of reports leading to cases being forwarded to prosecution officials. Belgium's FIU received just over 12,000 reports and submitted 1,666 cases to the public prosecutor in that year. This represented 13 percent of all reports submitted and 23 percent of the total number of files opened. Taiwan's FIU also passed on a large proportion of cases to law enforcement in 2007. The Taiwanese FIU received fewer than 2,000 reports in that year and sent more than 20 percent of these onto law enforcement agencies. France, by contrast, passed on approximately 400 reports to law enforcement which equalled three percent of the 12,000 reports received in 2007. The United Kingdom did not provide data on the number of files generated from reports of suspicious activity, but did file 766 charges which resulted in 276 convictions. This, however, was out of a total of over 220,000 reports.

The volume of money laundering prosecutions, case files, or other criminal sanctions is one of many proxy measures of the utility of suspect transaction and other financial intelligence reporting. Others not considered within the scope of this report might include the frequency with which law enforcement and other agencies access the data generated by AML/CTF regimes and its reported utility in investigations, and the feedback given to reporting businesses.

The utility of financial intelligence reporting may be dependent on the capacity of FIUs to adequately use the additional information generated each year in most countries. Insufficient resources or an inability to keep pace with the volume of reports means that authorities would be unlikely to gain any additional use from increased report numbers and

may find generating useful information from the volume of data more difficult.

The problems of defensive reporting have been documented elsewhere (Harvey 2008) and show that in periods of intense regulation, entities may seek the appearance of compliance with the obligations in order to avoid punitive sanctions rather than from concern to reduce the risk of money laundering and terrorism financing offences. For AML/CTF regulation, this can result in a higher number of reports being submitted to the FIU, with no guarantees about the quality of the information. A sudden influx of reports to the FIU can place a burden on resources and limit the effectiveness of responses. The utility of reporting is also highly dependent on the quality of the reports lodged and some countries have acknowledged this as an existing concern.

Money laundering prosecutions

As with reporting levels for suspicious financial activity, the number of people charged or prosecuted for money laundering has also seen a general increase in the nine countries analysed in this report. The reporting of enforcement figures also varies between countries.

Prosecution data in the Australian statistics show the number of charges dealt with by the public prosecutor, Germany shows the number of offences, Taiwan measured prosecutions, while the United Kingdom showed convictions and formal cautions and Hong Kong recorded only convictions. Statistics were not able to be gathered from France, Belgium, Singapore and the United States. Nevertheless, some general trend data can be extracted for the countries that published information in this area.

Most countries reported yearly increases in the levels of enforcement activity in each country. Germany, however, reported a variation to this trend, with a 40 percent decrease in the number of offences between 2002 and 2003. The number of recorded offences in Germany increased between 2003 and 2007 where, between 2005 and 2006, Germany recorded an increase of more than 160 percent in the number of convictions.

The United Kingdom saw a dramatic increase from 16 offenders found guilty or cautioned in 2003 to 1,328 in 2006. Convictions in Hong Kong climbed from 49 convictions in 2004 to 179 in 2007. Despite an increase in charges in Australia, there only exists a small number of cases of money laundering compared with other countries in this report. The number of charges under division 400 of the Criminal Code in 2006–07 was just 23. In 2005, the FATF-GAFI highlighted the low levels of prosecutions in Australia as an area of concern. The volume of prosecutions in the United States did not dramatically increase between 1994 and 2001.

The volume of prosecutions for money laundering in each country in the sample is likely to be influenced by some of the same factors that drive changes in compliance or reported suspect transactions. The primary factor most likely to increase prosecutions is the capacity and willingness of the relevant law enforcement agencies to focus on pursuing money laundering offences. Reuter and Truman (2004) suggest that the law enforcement community in the United States pursued money laundering changes rather than drugs offences in the early 2000s because the money laundering offences carried harsher sentences.

The implementation of new legislation is one example of changes to AML/CTF regimes that are likely to impact regulatory action and law enforcement activities. Reporting entities are likely to take some time to implement the regulatory requirements that come with new legislation and the law enforcement community may find additional tools in new legislation provisions.

Identifying compliance and enforcement figures as low or high in a given country relies on an assumption of the underlying volume of money laundering or suspicious transactions. A country with few money laundering activities will have low reporting of suspicious transactions. Low reporting figures may also indicate a lack of compliance with legislation. Alternatively, large volumes of reports of suspicious transactions may indicate large volumes of suspicious activities or other issues such as a high incidence of businesses engaging in defensive reporting to avoid prosecution for non-compliance.

Best practice strategies to enhance compliance

Strategies to enhance compliance

The strategies employed by the FIUs and AML/CTF regulators to enhance compliance fall into two main categories—dialogue between the FIU and reporting entities, and increasing the ease of submission. The countries considered in this report have all adopted aspects of both of these broad strategies for heightening compliance through non-punitive means.

Electronic filing

Electronic report filing systems are common throughout all nine countries examined. Available information suggests that electronic filing has all but replaced paper disclosures in most cases.

In 2008–09, AUSTRAC received more than 99 percent of all financial intelligence reports from regulated entities in Australia electronically through *AUSTRAC Online* or EDDSWeb. AUSTRAC still received paper reports from regulated businesses that submitted less than 50 financial intelligence reports, of any type, in 2008–09 (AUSTRAC 2009a).

In 2008, the United States implemented an electronic filing system for reports of suspicious activity. Reporting entities, by the end of the 2009 financial year, submitted 82 percent of SARs through the electronic system (FinCEN 2009b). FinCEN offers support to reporting businesses through publications and an e-filing help desk.

UKFIU offered several means of electronically submitting SARs in 2008–09 and reporting entities submitted 96 percent of all SARs through one of these mechanisms. UKFIU encouraged regulated businesses to file reports via SAR Online and Moneyweb (an alternate filing system which ceased to be available in early 2009). Reporting entities were able to submit reports directly into UKFIU's database after receiving an encryption certificate (SOCA 2009b).

MLPC provides software and detailed information on its use to reporting entities in Taiwan. It received 99 percent of currency transaction reports filed in 2007 electronically (APG 2007). Singapore also received 90 percent of reports of suspicious activities electronically in 2009 (CAD 2009). JFIU Hong Kong has offered electronic filing for financial intelligence reports since at least 2007 (JFIUHK 2007).

Germany began testing an electronic filing system in 2005 (FIU Germany 2005) and anticipated that the system would be operational by 2008 (FIU Germany 2007). TRACFIN received 88 percent of STRs filed in France electronically in 2008 (TRACFIN 2008). CTIF-CFI Belgium initiated an online disclosure system in 2006 (CTIF-CFI 2009).

Feedback to industry

United States

One of FinCEN's goals for the 2006–08 period was to increase the level of feedback given to reporting entities on their analysis of financial intelligence and risks of financial crimes. This remained a goal for the 2008–12 period, with FinCEN further aiming to use technology to improve the speed and quality of feedback to reporting entities. FinCEN has not indicated that reporting entities receive any specific information on how the SARs they have filed are used, although FinCEN provides more generalised feedback which includes:

- an acknowledgement response to all SARs filed with FinCEN;
- SAR Activity Reviews that include guidance on preparing reports and basic analysis of the content of SARs;
- outreach meetings with financial institutions;
- impact reports of new rules for reporting entities; and
- case examples outlining how SARs are used by law enforcement agencies.

United Kingdom

UKFIU published more information on the volume and type of feedback provided to reporting entities than FinCEN in the United States. A key feature of the feedback given to reporting entities in the United Kingdom is the systematic visits and seminars conducted within each sector. UKFIU conducted 181 visits and seminars to reporting sectors in the year to October 2007 (SOCA 2007). Table 50 indicates that the accounting, banking, legal and gaming industries received the bulk of industry visits conducted by UKFIU in this period.

SOCA also provides more general feedback to reporting businesses with website-based guidance on producing useful SARs. Reporting entities also receive alerts to industry which detail information about the SARs regime.

Each end user of the information gathered from SARs is required to nominate a contact officer for all communications with UKFIU and the reporting sector within the partnership agreements negotiated with SOCA.

France

France has not released as much information in English on the feedback systems between TRACFIN and reporting entities as other countries, making gauging the level of interaction less accurate. TRACFIN's annual report, however, contains some information intended for a reporting audience in the form of sanitised cases.

TRACFIN informs reporting entities when a report of a suspicious transaction is submitted to judicial authorities. Reporting entities, however, do not receive any additional information on the final decisions of any cases stemming from an initial report. Prior to the Mutual Evaluation of France,

Table 50 UK financial intelligence unit contact with the reporting sector, 2006–07 (n)

Industry	Sector-specific seminars	Visits	Total
Accounting	6	35	41
Banking	8	62	70
Legal	7	13	20
MSBs	1	7	8
Gaming	3	17	20
Insurance	2	10	12
Estate agents	2	5	7
Trust and company service providers	0	2	2
Factors and discounters	0	1	1
Total			181

Source: SOCA 2007

TRACFIN was also not advised of the judicial outcomes of these cases. French legislation was amended around this time to require authorities to inform TRACFIN of such outcomes. TRACFIN's annual reports contain aggregated information for cases passed onto judicial authorities (eg see TRACFIN 2008).

Favarel-Garrigues, Godefroy and Lascoumes (2008) report informal exchanges between TRACFIN and banking compliance officers that result in TRACFIN agreeing to a system that differentiates genuinely suspicious transactions from those that have been reported by a bank just to avoid attention from the banking regulator. Some of the survey respondents in the study by Favarel-Garrigues, Godefroy and Lascoumes (2008) reported excellent informal communication channels with TRACFIN, while others found gathering information in this manner more difficult. TRACFIN has indicated that it is attempting to emphasise direct contact between its employees and reporting entities, but has not released specific strategies for doing so in English-language publications.

Hong Kong

Hong Kong's JFIU has published detailed guidelines for identifying transactions that could be considered suspicious and offers advice on how to gather as much information as possible about those conducts such transactions. JFIUHK provides a letter of receipt to all reporting entities who have lodged a report. The acknowledgement letter contains a reference number for the report, which must be included in all future correspondence and indicates whether the reporting entity is permitted to continue dealing with the client in question. Each reporting entity also receives a second letter detailing the outcome of any investigation (FATF-GAFI 2008b).

Taiwan

MLPC adopted operational guidelines that include a directive to provide feedback to reporting entities (no. 9; MJIB 2006). MLPC staff conducted 195 anti-money laundering lectures in 2006, presenting to 12,040 participants. It conducted a comparable number of lectures in previous years (see Table 51; APG 2007).

Table 51 Money Laundering Prevention Centre contact with the reporting sector, 2003–07

Year	Lectures held	Attendees
2007	128	8,007
2006	195	12,040
2005	131	15,488
2004	109	7,087
2003	166	12,833

Source: APG 2007; MJIB 2008

MLPC's feedback to reporting entities includes recommendations for written commendations for individuals and entities who have reported transactions that directly assisted an investigation. MLPC made 31 such recommendations between 2002 and 2005 (APG 2007). Negative feedback is provided to the supervisory institutions responsible for imposing sanctions if they are not necessary.

MLPC further holds a conference for compliance officers in the banking industry every two years to give and receive feedback and to discuss developments in anti-money laundering trends and techniques. MLPC also organises a seminar for law enforcement bodies, staff of MLPC and other government agencies, and financial supervisory authorities to discuss problems associated with the legislation.

Germany

AML/CTF legislation in Germany obligates the FIU to regularly notify reporting entities of types and methods of money laundering and terrorism financing. The Germany Money Laundering Act further requires the public prosecutor's office to notify FIU Germany of the outcomes of criminal proceedings tied to a STR.

FIU Germany provides general feedback publically on noteworthy cases stemming from reports, such as those submitted in high volumes, as well as trends and typologies. The FIU publishes quarterly newsletters outlining case studies

Singapore

STRO in Singapore conducts outreach sessions with law enforcement agencies and business groups to gather feedback and to provide information. CAD (housing STRO) reported expanding their outreach activities to more sectors in 2009 (CAD 2009).

Australia

Australian regulated businesses do not receive specific feedback about the reports submitted or the detailed outcomes of cases. AUSTRAC publishes an annual typologies report that contains sanitised information about non-concluded matters, current investigations and concluded cases.

AUSTRAC conducted 800 industry-awareness sessions between 2006 and 2009 (AUSTRAC 2009g). The regulator also reports further engagement with businesses through media releases and interviews, presentations and other speeches, mail outs and emails, and outbound call campaigns, but has not reported the frequency with which these additional tools are used.

Training provided to industry

A number of FIUs reported providing training or assisting to train key officers in reporting entities. The sector-specific seminars run by SOCA in the United Kingdom are conducted as an education tool for money laundering reporting officers. FIU staff in Germany also attended training sessions for compliance officers in some banks and with the securities authorities in 2006. They also ran additional training lectures.

MLPC of Taiwan offers formal and informal training to reporting entities. The material offered encompasses assistance on submitting reports, providing typologies and presenting case studies. TRACFIN in France provides similar assistance in the form of typological information for training programs.

Feedback from industry and the availability of financial intelligence units to industry

The United States, United Kingdom and Hong Kong report formal processes for seeking feedback from reporting entities and others.

United States

In 2007, FinCEN surveyed reporting entities receiving SAR Activity Reviews, users of the electronic filing system, users accessing Bank Secrecy Act information and recipients of other analytical products. The 2007 surveys revealed that 94 percent of respondents were satisfied with the electronic filing system, 91 percent of users of the Regulatory Resource Centre information online rated the advice given as understandable and 70 percent of recipients of SAR Activity Reviews considered them highly valuable (FinCEN 2007).

United Kingdom

UKFIU seeks feedback from end users of SARs through a questionnaire sent out twice a year. Reporting entities contribute to the SARs Committee, the body overseeing the SARs system in the United Kingdom and the SARs Vetted Group concerned with the operational activity of the system. The British Bankers' Association, Institute of Chartered Accountants of England and Wales, and the Law Society for England and Wales are on the Committee.

Hong Kong

Reporting entities that have registered for electronic report submission in Hong Kong are able to provide feedback to JFIUHK through the report submission system. JFIUHK have not indicated the extent of this feedback or any evaluative outcomes.

Conclusion

This report has provided a preliminary review of the different approaches to addressing the problem of money laundering and the financing of terrorism in a selection of nine countries from North America, Europe, Asia and Australia. Although the largest countries are represented, this review is not a complete analysis of international responses, nor is it representative of the entire global response to AML/CTF regulation. Rather, it was designed to present comparative statistics from a variety of countries with differing legal and regulatory traditions to show how they have approached the implementation

of the FATF-GAFI Recommendations. Further, the review incorporated an analysis of the extent of data availability and examined the comparative sizes of the regulated sectors in different countries and the extent of compliance and enforcement activity.

Future comparative studies of this nature should aim to provide:

- more complete information on the legal structure and mechanisms of the anti-money laundering regimes;
- the profiles and volumes of businesses regulated for anti-money laundering;
- the compliance activities of those businesses and the regulatory and criminal enforcement in each country; and
- the strategies adopted to increase compliance as well as increase the quality of financial intelligence generated by the anti-money laundering regimes.

This would entail undertaking in-depth qualitative research with the regulators and industry associations in each country. In the case of non English-speaking locations, multilingual research would be necessary and access to business and government statistical collections. As is apparent from this review, the challenges of conducting such research are considerable, as public source material provides only a limited view of the situation. Problems also exist within individual nations where data is not being collected, or is collected in varying formats using different data fields, categories and definitions. The FATF-GAFI Mutual Evaluations provide a good deal of uniformly collected and comparable information, but often these reports are incomplete. While regulators and FIUs also collect considerable amounts of data from the regulated sectors in annual compliance reports, these are not readily available or are collected using non-uniform categories across countries.

Ideally, a single repository of AML/CTF compliance and regulatory data should be established, although in practice, the resources required for this would be prohibitive. At present, therefore, it is perhaps sufficient that FIUs, law enforcement agencies and regulators maintain a dialogue to develop the use of harmonised data recording practices for the key variables of policy importance. The present report has provided a basis for international comparison of anti-money laundering regimes across countries of interest by outlining the approaches taken to common aspects to anti-money laundering systems, identifying potential measures of performance of those systems and the current best practise strategies for increasing compliance by business and increasing the quality of the intelligence received by regulators and the law enforcement community. The present report provides an indication of the areas requiring most attention for discussion in the years ahead.

References

All URLs were correct at March 2011

Aggarwal R & Raghavan K 2006. Management board challenges complying with Bank Secrecy Act and anti money laundering regulations, in Gup B (ed), *Money laundering, financing terrorism and suspicious activities*. New York: Nova Science Publishers

Ashurst 2009. *New decree on anti-money laundering in France: Update October 2009*. http://www.ashurst.com/publication-list.aspx?id_Content=1230&expandTypeList=true&id_queryResource=5&page=2

Asia Pacific Group on Money Laundering (APG) 2007. *APG mutual evaluation report on Chinese Taipei: Against the FATF 40 recommendations (2003) and 9 special recommendations*. Sydney: APG

AUSTRAC 2010a. *Undertaking to the Chief Executive Officer of AUSTRAC for the purposes of section 197 of the AML/CTF Act by Eastern and Allied Pty Ltd, trading as Hai Ha Money Transfer—Anti-Money Laundering and Counter-Terrorism Financing Act 2006*. http://austrac.gov.au/files/eu_easternallied.pdf

AUSTRAC 2010b. *Written notices*. http://austrac.gov.au/written_notices.html

AUSTRAC 2009a. *Annual report 2008–09*. Sydney: AUSTRAC

AUSTRAC 2009b. *Undertaking to the Chief Executive Officer of AUSTRAC for the purposes of section 197 of the AML/CTF Act by Barclays Bank Plc. Enforceable undertaking—Anti-Money Laundering and Counter-Terrorism Financing Act 2006*. http://www.austrac.gov.au/files/eu_barclays.pdf

AUSTRAC 2009c. AUSTRAC accepts enforceable undertaking from Barclays Bank. *Media release* 1 July. http://www.austrac.gov.au/1jul09_2.html

AUSTRAC 2009d. *Undertaking to the Chief Executive Officer of AUSTRAC for the purposes of section 197 of the AML/CTF Act by Mega International Commercial Bank Co Ltd. Enforceable undertaking—Anti-Money Laundering and Counter-Terrorism Financing Act 2006*. http://www.austrac.gov.au/files/eu_megabank.pdf

AUSTRAC 2009e. *Undertaking to the Chief Executive Officer of AUSTRAC for the purposes of section 197 of the AML/CTF Act by Paypal Australia Ltd ACN 111 195 389. Enforceable undertaking—Anti-Money Laundering and Counter-Terrorism Financing Act 2006*. http://www.austrac.gov.au/files/eu_paypal.pdf

AUSTRAC 2009f. *Mojgan Zojaji trading as Little Persia. Remedial Direction—Subsection 191(2) Anti-Money Laundering and Counter-Terrorism Financing Act 2006*. http://www.austrac.gov.au/files/remedial_directions.pdf

AUSTRAC 2009g. *AUSTRAC supervision strategy 2009–2010*. Sydney: AUSTRAC

AUSTRAC 2007. *Annual report 2006–07*. Sydney: AUSTRAC

Australian Prudential Regulation Authority (APRA) 2010a. *List of authorised deposit-taking institutions*. http://www.apra.gov.au/adi/ADIList.cfm

Australian Prudential Regulation Authority (APRA) 2010b. *Insurers authorised to conduct new or renewal insurance business in Australia*. http://www.apra.gov.au/General/New-or-Renewal.cfm

Banking, Finance, and Insurance Commission (Belgium) (CBFA) 2007. *CBFA annual report 2007*. Brussels: CBFA

Banque de France 2008. *Liste des establissement de credit*. Paris: Banque de France

Bundeskriminalamt (BKA) 2008a. *Police crime statistics 2008*. Wiesbaden, Germany: BKA

Bundeskriminalamt (BKA) 2008b. *Organised crime: 2008 national situation report*. Wiesbaden, Germany: BKA

Bundeskriminalamt (BKA) 2007. *Police crime statistics 2007*. Wiesbaden, Germany: BKA

Bundeskriminalamt (BKA) 2006a. *Police crime statistics 2006*. Wiesbaden, Germany: BKA

Bundeskriminalamt (BKA) 2006b. *The Bundeskriminalamt: The profile*. Wiesbaden, Germany: BKA

Bundeskriminalamt (BKA) 2005. *Police crime statistics 2005*. Wiesbaden, Germany: BKA

Bundeskriminalamt (BKA) 2004a. *Police crime statistics 2004*. Wiesbaden, Germany: BKA

Bundeskriminalamt (BKA) 2004b. *Organised crime: 2004 national situation report*. Wiesbaden, Germany: BKA

Bundeskriminalamt (BKA) 2003. *Police crime statistics 2003*. Wiesbaden, Germany: BKA

Camp P 2007. *Solicitors and money laundering: A compliance handbook,* 2nd ed. London: Law Society

Casino Regulatory Authority (CRA) 2009. *Annual report 2008–09*. Singapore: CRA

Chevrier E 2004. The French government's will to fight organized crime and clean up the legal professions: The awkward compromise between professional secrecy and mandatory reporting. *Crime, Law and Social Change* 42(2–3): 189–200

Commercial Affairs Department (CAD) 2009. *Certainty amidst uncertainties: Annual report 2009*. Singapore: CAD

Commercial Affairs Department (CAD) 2008. *Transcending boundaries: Annual report 2008*. Singapore: CAD

Commercial Affairs Department (CAD) 2007. *Suspicious transaction reporting office (STRO)*. http://www.cad.gov.sg/amlcft/STRO.htm

Commonwealth Director of Public Prosecutions (CDPP) 2009. *Annual report 2008–09*. Canberra: CDPP

Commonwealth Director of Public Prosecutions (CDPP) 2008. *Annual report 2007–08*. Canberra: CDPP

Commonwealth Director of Public Prosecutions (CDPP) 2007. *Annual report 2006–07*. Canberra: CDPP

Coorey P, Marriner C, Welch D & Saulwick J 2007. Haneef released as charges dropped. *Sydney Morning Herald* 27 July 2007. http://www.smh.com.au/news/general/terrorism-charge-dropped/2007/07/27/1185339230498.html?page=fullpage

CTIF-CFI (Belgian Financial Intelligence Processing Unit) 2009. *Online disclosures*. Brussels: CTIF-CFI. http://www.ctif-cfi.be/website/index.php?option=com_content&view=article&id=32%3Adeclaration-en-ligne&catid=9%3Adeclarants-obligations&Itemid=49&lang=en

CTIF-CFI (Belgian Financial Intelligence Processing Unit) 2008. *15th annual report*. Brussels: CTIF-CFI. http://www.ctif-cfi.be/website/images/EN/annual_report/2008_ctif_cfi_en.pdf

CTIF-CFI (Belgian Financial Intelligence Processing Unit) 2007a. *14th annual report*. Brussels: CTIF-CFI. http://www.ctif-cfi.be/website/images/EN/annual_report/2007_ctif_cfi_en.pdf

CTIF-CFI (Belgian Financial Intelligence Processing Unit) 2007b. *Money laundering indicators*. Brussels: CTIF-CFI

CTIF-CFI (Belgian Financial Intelligence Processing Unit) 2006. *13th annual report*. Brussels: CTIF-CFI. http://www.ctif-cfi.be/website/images/EN/annual_report/2006_ctif_cfi_en.pdf

Deitz A & Buttle J 2008. *Anti-money laundering handbook*. Sydney: Thomson Lawbook

Department of Justice (Hong Kong) (DoJHK) 2009. *The yearly review of the prosecutions division 2008*. Hong Kong: DoJ

Department of Justice (Hong Kong) (DoJHK) 2008. *The yearly review of the prosecutions division 2007*. Hong Kong: DoJ

Department of Justice (Hong Kong) (DoJHK) 2007. *The yearly review of the prosecutions division 2006*. Hong Kong: DoJ

Department of Justice (Hong Kong) (DoJHK) 2006. *The yearly review of the prosecutions division 2005*. Hong Kong: DoJ

Department of Justice (Hong Kong) (DoJHK) 2005. *The yearly review of the prosecutions division 2004*. Hong Kong: DoJ

Department of the Prime Minister and Cabinet (DPM&C) 2010. *Counter-terrorism white paper: Securing Australia, protecting our community*. DPM&C: Canberra

Financial Standards Foundation 2011. *Anti-money laundering France. eStandards forum*. http://estandardsforum.org/france/standards/anti-money-laundering-combating-terrorist-financing-standard

Estate Agents Authority (EAA) 2009. *Licensee statistics*. http://www.eaa.org.hk/licensing/statistics.htm

Europa 2009. Anti-money laundering: Commission takes action to ensure that France, Poland and Spain implement EU laws. *Media release (European Commission)* 29 Jan. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/159&type=HTML&aged=0&language=EN&guiLanguage=en

Europa 2008. Anti-money laundering: Commission takes measures against 15 member states for non timely implementation. *Media release (European Commission)* 5 Jun. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/860&format=HTML&aged=0&language=EN&guiLanguage=en%20in%202008

European Commission 2009a. *21st meeting of the committee on the prevention of money laundering and terrorist financing: Tuesday, 16 June 2009*. http://ec.europa.eu/internal_market/company/docs/financial-crime/meetings/20090616-summary_en.pdf

European Commission 2009b. *22nd meeting of the committee on the prevention of money laundering and terrorist financing: Monday, 5 October 2009*. http://ec.europa.eu/internal_market/company/docs/financial-crime/meetings/20091005-summary_en.pdf

Favarel-Garrigues G, Godefroy T & Lascoumes P 2008. Sentinels in the banking industry: Private actors and the fight against money laundering in France. *British Journal of Criminology* 48: 1–19

Financial Action Task Force (FATF-GAFI) 2010. *Anti-money laundering and combating the financing of terrorism: Mutual evaluation report, Germany*. Paris: FATF-GAFI/OECD

Financial Action Task Force (FATF-GAFI) 2008a. *Third mutual evaluation report on anti-money laundering and combating the financing of terrorism Singapore: Executive summary*. Paris: FATF-GAFI/OECD

Financial Action Task Force (FATF-GAFI) 2008b. *Third mutual evaluation report anti-money laundering and combating the financing of terrorism Hong Kong, China*. Paris: FATF-GAFI/OECD

Financial Action Task Force (FATF-GAFI) 2008c. *FATF IX Special Recommendations*. Paris: FATF-GAFI/OECD

Financial Action Task Force (FATF-GAFI) 2007a. *Third mutual evaluation report on anti-money laundering and combating the financing of terrorism: United Kingdom of Great Britain and Northern Ireland*. Paris: FATF-GAFI/OECD

Financial Action Task Force (FATF-GAFI) 2007b. *Annual review of non-cooperative countries and territories 2006–2007: Eighth NCCT review*. Paris: FATF-GAFI/OECD

Financial Action Task Force (FATF-GAFI) 2006. *Third mutual evaluation report on anti-money laundering and combating the financing of terrorism: United States of America*. Paris: FATF-GAFI/OECD

Financial Action Task Force (FATF-GAFI) 2005a. *Summary of the third mutual evaluation report on anti-money laundering and combating the financing of terrorism: Belgium*. Paris: FATF-GAFI/OECD

Financial Action Task Force (FATF-GAFI) 2005b. *Third mutual evaluation report on anti-money laundering and combating the financing of terrorism: Australia*. Paris: FATF-GAFI/OECD

Financial Action Task Force (FATF-GAFI) 2004. *FATF 40 Recommendations*. Paris: FATF-GAFI/OECD

Financial Crimes Enforcement Network (FinCEN) 2009a. By the numbers. *SAR Activity Review* 12. Washington, DC: FinCEN

Financial Crimes Enforcement Network (FinCEN) 2009b. *Annual report fiscal year 2009*. Washington DC: FinCEN

Financial Crimes Enforcement Network (FinCEN) 2008. *Annual report fiscal year 2008*. Washington DC: FinCEN

Financial Crimes Enforcement Network (FinCEN) 2007. *FinCEN annual report fiscal year 2007*. Washington DC: FinCEN

Financial Crimes Enforcement Network (FinCEN) 2006. *FinCEN Annual report fiscal year 2006*. Washington DC: FinCEN

Financial Services Authority (FSA) 2008. FSA fines firm and MLRO for money laundering controls failings. *Press release* (FSA) 29 October. http://www.fsa.gov.uk/pages/Library/Communication/PR/2008/125.shtml

Financial Services Authority (FSA) 2005. FSA fines bond broker and managing director for anti-money laundering failures. *Press release* (FSA) 9 November. http://www.fsa.gov.uk/Pages/Library/Communication/PR/2005/117.shtml

Financial Services Authority (FSA) 2004a. FSA fines Bank of Ireland 375,000 for breaches of anti-money laundering requirements. *Press release* (FSA) 2 September. http://www.fsa.gov.uk/Pages/Library/Communication/PR/2004/077.shtml

Financial Services Authority (FSA) 2004b. The Financial Services Authority (FSA) has today fined Raiffeisen Zentralbank [Ö]sterreich's London branch ('RZB London') 150,000 for breaches of the FSA's Money Laundering Rules. *Press release* (FSA) 6 April. http://www.fsa.gov.uk/Pages/Library/Communication/PR/2004/035.shtml

Financial Services Authority (FSA) 2004c. FSA fines Bank of Scotland Plc 1,250,000 for money laundering rule breaches. *Press release* (FSA) 15 January. http://www.fsa.gov.uk/Pages/Library/Communication/PR/2004/001.shtml

Financial Services Authority (FSA) 2003a. FSA fines Abbey National companies 2,320,000. *Press release* (FSA) 10 December. http://www.fsa.gov.uk/Pages/Library/Communication/PR/2003/132.shtml

Financial Services Authority (FSA) 2003b. FSA fines Northern Bank 1,250,000 for money laundering control failings. *Press Release* (FSA) 7 August. http://www.fsa.gov.uk/Pages/Library/Communication/PR/2003/084.shtml

Financial Services Authority (FSA) 2002. FSA fines Royal Bank of Scotland Plc 750,000 for money laundering control failings. *Press release* (FSA) 17 December. http://www.fsa.gov.uk/Pages/Library/Communication/PR/2002/123.shtml

Financial Services Authority (FSA) 2001. Paine Webber International (UK) Limited fined £350,000. *Press release* (FSA) 22 August. http://www.fsa.gov.uk/pubs/additional/sfa009-01.pdf

FIU Germany 2008. *Annual report 2008*. Wiesbaden, Germany: Bundeskriminalamt, FIU Germany

FIU Germany 2007. *Annual report 2007*. Wiesbaden, Germany: Bundeskriminalamt, FIU Germany

FIU Germany 2006. *Annual report 2006*. Wiesbaden, Germany: Bundeskriminalamt, FIU Germany

FIU Germany 2005. *Annual report 2005*. Wiesbaden, Germany: Bundeskriminalamt, FIU Germany

Freshfields Bruckhaus Deringer 2005. *Dispute resolution focus*. Autumn 2005. http://www.freshfields.com/publications/pdfs/2005/13077.pdf

Gup B 2006. *Money laundering, financing terrorism and suspicious activities*. New York: Nova Science Publishers

Harvey J 2008. Just how effective is money laundering legislation? *Security Journal* 21: 189–211

Harvey J 2005. An evaluation of money laundering policies. *Journal of Money Laundering Control* 8 (4): 339–345

Hong Kong Institute of Certified Public Accountants (HKICPA) 2009. *Annual report 2009*. Hong Kong: HKICPA

Hong Kong Monetary Authority (HKMA) 2009. *Banking policy and supervision*. http://www.info.gov.hk/hkma/eng/bank/index.htm

Howell J 2007. *The EU's efforts in the fight against terrorism in the context of the Financial Action Taskforce's nine special recommendations and the EU counter terrorist financing strategy: Final report*. Surrey, UK: John Howell & Company Ltd

International Bar Association Anti-Money Laundering Group (IBA) 2009. *The lawyer's guide to legislation and compliance: France*. http://www.anti-moneylaundering.org/europe/france.aspx

International Monetary Fund (IMF) 2005. France: Financial sector assessment program—detailed assessments of observance of standards and codes including banking supervision, insurance regulation, securities legislation, monetary and financial policy transparency, payments systems, securities settlement, and anti-money laundering and combating the financing of terrorism. *IMF Country Report no. 05/186*. Washington: IMF

International Monetary Fund (IMF) 2004. Germany: Report on the observance of standards and codes—FATF recommendations for anti-money laundering and combating the financing of terrorism. *IMF Country Report no. 04/213*. Washington: IMF

Investigation Bureau, Ministry of Justice, Republic of China (MJIB) 2008. *Anti-money laundering annual report 2007*. Hsin-tien City, Taiwan: MJIB

Investigation Bureau, Ministry of Justice, Republic of China (MJIB) 2007. *Anti-money laundering annual report 2006*. Hsin-tien City, Taiwan: MJIB

Investigation Bureau, Ministry of Justice, Republic of China (MJIB) 2006. *Anti-money laundering annual report 2005*. Hsin-tien City, Taiwan: MJIB

Investigation Bureau, Ministry of Justice, Republic of China (MJIB) 2005. *Anti-money laundering annual report 2004*. Hsin-tien City, Taiwan: MJIB

Jaggers B 2008. *Anti-terrorism control orders in Australia and the United Kingdom: A comparison*. Research paper no. 28, 2007–08. Canberra: Parliament of Australia Parliamentary Library. http://www.aph.gov.au/library/pubs/rp/2007-08/08rp28.htm#_Toc197240508

Joint Financial Intelligence Unit (Hong Kong) (JFIUHK) 2009. *Statistics*. http://www.jfiu.gov.hk/eng/statistics.html

Joint Financial Intelligence Unit (Hong Kong) (JFIUHK) 2007. *Suspicious transaction report*. http://www.jfiu.gov.hk/eng/how.html

Jones & Zgonec-Rože 2009. Freezing assets of 'terrorists'—how fair is the UN sanctions committee? *Law Society Gazette* 10 September. http://www.lawgazette.co.uk/in-practice/practice-points/freezing-assets-terrorists-how-fair-un-sanctions-committee

KPMG 2007. *Global anti-money laundering survey 2007: How banks are facing up to the challenge*. http://www.kpmg.com.au/Portals/0/2007%20AML%20Survey%20-%20Web%20Version.pdf

Law Society (United Kingdom) 2008. *Anti-money laundering practice note 22 February 2008*. http://www.lawsociety.org.uk/productsandservices/practicenotes/aml/449.article

Law Society (United Kingdom) 2005. *Law society guidance on Bowman v Fels (2005) EWCA Civ 226*. http://www.lawsociety.org.uk/documents/downloads/BowmanvFelsGuidance0905.pdf

Law Society of Hong Kong 2008. *About the society*. http://www.hklawsoc.org.hk/pub_e/about/

Law Society of Singapore 2009. *Annual report 2009*. Singapore: Law Society of Singapore

Levi M & Reuter P 2006. Money laundering, in Tonry M (ed), *Crime and justice: A review of research* vol 34. Chicago: Chicago University Press: 289–386

Library of Congress, Federal Research Division 2008. *Country profile: Germany*. Washington, DC: Library of Congress

Monetary Authority of Singapore (MAS) 2009. *Number of financial institutions and relevant organisations in Singapore*. http://www.mas.gov.sg/fi_directory/index.html

Neve R, Vervoorn L, Leeuq F & Bogaerts S 2006. *First inventory of policy on counterterrorism: Germany, France, Italy, Spain, the United Kingdom and the United States—'research in progress'*. The Hague: Wetenschappelijk Onderzoeken Documentatiecentrum (WODC). http://transcrime.cs.unitn.it/tc/fso/Altre pubblicazioni/first inventory of policy on counterterrorism - italian contribution to ncbt.pdf

Office of the Commissioner of Insurance (OCI) 2009. *Authorised insurers and insurance statistics*. http://www.oci.gov.hk/stat/menu.html

Office for National Statistics (ONS) 2009. *Inter-departmental business register*. London: ONS. http://www.statistics.gov.uk/cci/nugget.asp?id=1238

Peters M nd. FIU Germany—structure, policy, and activities to combat ML and TF. Paper with author J Walters: Canberra

PricewaterhouseCoopers Forensic Services 2007. *Anti-money laundering survey*. London: PricewaterhouseCoopers LLP

Reuter P & Truman E 2005. Anti-money laundering overkill? *The International Economy* 19(1): 56–60

Reuter P & Truman E 2004. *Chasing dirty money*. Washington DC: Institute for International Economics

Schott PA 2004. *Reference guide to anti-money laundering and combating the financing of terrorism,* 2nd ed. Washington, DC: The World Bank

Securities and Futures Commission 2009. *Market & industry statistics*. http://www.sfc.hk/sfc/html/EN/research/stat/stat.html

Serious Organised Crime Agency (SOCA) 2009a. *Annual report 2008–09*. London: SOCA

Serious Organised Crime Agency (SOCA) 2009b. *Suspicious activity reports regime annual report 2009*. London: SOCA

Serious Organised Crime Agency (SOCA) 2008a. *The United Kingdom threat assessment of serious organised crime 2008–09*. London: SOCA

Serious Organised Crime Agency (SOCA) 2008b. *Serious Organised Crime Agency annual plan 2008–09*. London: SOCA

Serious Organised Crime Agency (SOCA) 2007. *The suspicious activity reports regime annual report 2007*. London: SOCA

Serious Organised Crime Agency (SOCA) 2006. *The United Kingdom threat assessment of serious organised crime 2006–07*. London: SOCA

Smith RG (ed) forthcoming. *Anti-money laundering and counter-terrorism financing monitoring report 2007–09*. Monitoring report. Canberra: Australian Institute of Criminology

Sproat P 2007. An evaluation of the UK's anti-money laundering and asset recovery regime. *Journal of Crime, Law, and Social Change* 47: 169–184

Suspicious Transaction Reporting Office (Singapore) (STRO) 2009. *Statistics*. http://www.cad.gov.sg/amlcft/stro/Statistics.htm

TRACFIN 2008. *Annual report 2008*. Paris: TRACFIN

TRACFIN 2007. *Annual report 2007*. Paris: TRACFIN

TRACFIN 2006. *Annual report 2006*. Paris: TRACFIN

Transactional Records Access Clearinghouse (TRAC) 2007. *Terrorism enforcement: International, domestic and financial*. http://trac.syr.edu/tracreports/terrorism/177/#T2

Unger B & Van Waarden F 2009. How to dodge drowning in data? Rule-and-risk-based anti money laundering policies compared. *Review of Law and Economics* 5 (2): 953–985

United States Department of State 2008. *2008 international narcotics control strategy report*. Washington DC: United States Department of State

United States Department of the Treasury 2009. *Settlement agreement MUL-464334*. http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Documents/anz_08242009.pdf

United States Department of the Treasury 2007. *Office of foreign assets control: Enforcement information for September 7, 2007*. http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Documents/09072007.pdf

United States Office of Advocacy 2009 (US Office of Advocacy). Advocacy: the voice of small business in government. *The Small Business Advocate* 8: 7. Washington, DC: Small Business Administration. http://www.sbaonline.sba.gov/advo/aug-sep09.pdf

Walters J, Smith RG, Davis B & Choo K-KR forthcoming. *The anti-money laundering and counter-terrorism financing regime in Australia: Perceptions of Australian businesses*. Research and public policy series. Canberra: Australian Institute of Criminology