Australian Government
Australian Institute of Criminology

The anti-money laundering and counter-terrorism financing regime in Australia: Perceptions of regulated businesses in Australia

Julie Walters, Russell G Smith, Brent Davis, Kim-Kwang Raymond Choo and Hannah Chadwick

AIC Reports
Research and Public Policy Series
117

The anti-money laundering and counter-terrorism financing regime in Australia: Perceptions of regulated businesses in Australia

Julie Walters
Russell G Smith
Brent Davis
Kim-Kwang Raymond Choo
Hannah Chadwick

AIC Reports
Research and
Public Policy Series
117

www.aic.gov.au

ISSN 1836-2060 (Print)
1836-2079 (Online)
ISBN 978 1 922009 10 4 (Print)
978 1 922009 11 1 (Online)

Project no. 0140
Ethics approval no. PO123
Dataset no. 0141
Statistical Clearing House approval number 02031-01

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.

General editor, Research and Public Policy Series :
Dr Adam M Tomison, Director, Australian Institute of Criminology

Note: Research and Public Policy Series publications are peer reviewed

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

In Australia, legislation was introduced in 2006 that requires specified businesses (such as banks and other financial institutions, insurance companies, securities and investment companies, gambling service providers, bullion dealers and providers of alternative remittance services) to forward reports of certain financial transactions to a federal government agency, the Australian Transaction Reports and Analysis Centre (AUSTRAC). This legislation, the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act 2006 (Cth)), is part of a suite of measures to ensure that Australia complies with the international anti-money laundering and counter-terrorism financing (AML/CTF) standards developed by the Financial Action Task Force.

The AML/CTF Act 2006 (Cth) establishes a risk-based regulatory framework in which certain businesses that offer 'designated services' are required to identify their customers and their customers' financial activities that might pose a high risk of involvement in money laundering or financing of terrorism and report these to AUSTRAC. Reporting entities need to be diligent in their reporting activities and in maintaining information about their customers and transactions for the system to work effectively. In order to deter businesses from failing to comply with the legislation, the AML/CTF Act 2006 (Cth) also establishes penalties for non-compliance.

Some of the regulated businesses had comparable regulatory responsibilities under Australia's earlier anti-money laundering legislation (*Financial Transaction Reports Act 1988* (Cth)), as entities that provided certain regulated services, while others were exposed to regulatory requirements for the first time with the enactment of the 2006 Act. Businesses whose services fall under the definition in the AML/CTF Act 2006 (Cth) of what constitutes a designated service are now obliged to implement AML/CTF programs to address the level of money laundering and terrorism financing (ML/TF) risk that they believe affects their business operations. In addition, they are required to adhere to customer identification and due diligence procedures and to submit suspicious matter, threshold transaction and international funds transfer instruction reports to AUSTRAC.

As part of the Australian Institute of Criminology's research into Australia's AML/CTF regime, a survey was conducted in mid-2009 of all businesses with reporting obligations under the AML/CTF Act 2006 (Cth) at that time. The survey, which was undertaken during the early phase of implementation of the legislative reforms, provides a point-in-time review of the perceptions of affected businesses, many of who were still in the process of adapting to the new regulatory regime and consequently, in streamlining their processes. Most participants held neutral views about the regime, although there was general support for the regime in meeting its aims of deterring offenders, minimising risk and promoting good governance practices within the business community. Those who responded were also of the view that the costs that had, thus far, been incurred were not prohibitive at the time, with respondents spending an average of $1,000 during the previous 12 months in complying with the legislation.

Some of the findings from the survey however, reflected difficulties that a number of businesses had experienced, particularly those without previous regulatory obligations. In particular, some saw the regulatory regime as being too onerous for the perceived level of risk that they faced at the time. Many participants also felt that they would gain a better understanding of the risks and respond better to regulatory obligations, if a greater array of sector-specific education and training opportunities were made available. Almost all survey participants (the majority of whom were from micro or small businesses and irrespective of the sector that they represented), considered in mid-2009 that the ML/

TF risks to their businesses were low. It is possible that this assessment was, in part, based on limited exposure to the educative material describing inherent risks to their businesses that has since been made available by AUSTRAC and other industry organisations.

Changes to the AML/CTF environment in the period since the survey was conducted may have ameliorated these concerns to some extent. On a national level, the Commonwealth Organised Crime Strategic Framework, introduced in 2009, includes among its purposes the aim of enhancing relationships between the Commonwealth and regulated industries in both understanding and responding to organised crime matters. Money Laundering Working Groups were formed under the Framework and have produced a Response Plan for Heads of Commonwealth Law Enforcement Agencies (HOCOLEA). In addition, the national regulator, AUSTRAC, has produced a range of guides, typology reports and other tools to assist entities, particularly those who have experienced difficulty in adapting to Australia's risk-based AML/CTF approach, to evaluate risks and to apply appropriate compliance programs more effectively. Similarly, there has been an increase and improvement in industry-specific engagement through targeted education campaigns and the development of sector-specific guidance and supervision plans, which refer to individual exposure and risk levels.

The combination of regulator response, alongside increased familiarity with the regime, has arguably produced enhanced understanding of the benefits of the regime, as well as improved capability among businesses in achieving compliance with regulatory requirements. The findings presented in this report provide a useful gauge at a specific point in time of how over 4,000 Australian businesses and parts of some sectors regulated under the AML/CTF Act perceived the ML/TF risks they believed they faced. This is an important contribution to understanding the Australian risk environment and operation of AML/CTF regulation. However, the findings in this survey on business perceptions of ML/TF risk need to be viewed in a wider context. Business perceptions represent only one piece of the broader ML/TF picture. Due to the complexity and clandestine nature of ML/TF, most if not all businesses will only see a part of the environment. A significant amount of ML/TF and illicit financial activity can only be detected when government agencies examine larger holdings of transaction reporting and other information. Access to criminal and other intelligence may be needed to draw links across information sets to identify unusual or suspicious activity. Investigations are often required to confirm money laundering and criminal behaviour. Except in instances where law enforcement and other authorities approach businesses to gain their assistance on operational matters, business will not be privy to this wider array of information, much of which is highly classified.

AUSTRAC and other government agencies provide guidance and information on ML/TF risks, including summaries of real life cases and methods that have been detected. But this information is, by necessity, limited. Intelligence and operational sensitivities restrict the amount of information and detail authorities can provide to business on actual cases or the full extent of known ML/TF risk. Government authorities also acknowledge that they do not possess comprehensive visibility of the entire ML/TF risk environment. For these reasons, business perceptions of ML/TF risk presented in this report need to be seen as only one view of the ML/TF environment in Australia. Interpretation of those findings needs to take this limitation into account.

The results of the present study will be of use in providing a context of business perceptions as AUSTRAC conducts its own surveys of businesses to determine how well certain sectors understand risk and how well they have performed in implementing their AML/CTF obligations. The present results, taken in conjunction with AUSTRAC's ongoing survey results in the future, should provide a comprehensive body of information on how Australian businesses have approached AML/CTF and their views concerning the benefits and difficulties that have arisen in practice. This information will also provide a basis for developing future outreach activities to assist businesses with compliance in this important area of financial crime control.

Adam Tomison
Director

Contents

Figures

Boxes

Tables

Acronyms

ADIs	authorised deposit-taking institutions
AIC	Australian Institute of Criminology
AML/CTF	anti-money laundering/counter-terrorism financing
ARS	alternative remittance service
ASIC	Australian Securities and Investments Commission
ATO	Australian Taxation Office
AUSTRAC	Australian Transaction Reports and Analysis Centre
CBM-PC	cross-border movement of physical currency
DBG	designated business groups
DFAT	Department of Foreign Affairs and Trade
DNFBPs	Designated Non-Financial Businesses and Professions
FATF	Financial Action Task Force
FIU	financial intelligence unit
IFTI	international funds transfer instruction
KYC	know your customer
LTTE	Liberation Tigers of Tamil Eelam
MLRO	money laundering reporting officers
ML/TF	money laundering/terrorism financing
PEPs	politically exposed persons
SMRs	suspicious matter reports
TTRs	threshold transaction reports

Acknowledgements

The authors are grateful to the staff of the Social Research Centre who worked closely with the Australian Institute of Criminology in developing this survey and who were responsible for advising on the sampling frame, constructing and administering the questionnaire, collecting and preparing the data file, and preparing the companion Methodology Report (Challice & Eliseo 2012). We appreciate the work of colleagues at the Australian Institute of Criminology, particularly Dr Samantha Bricknell and Dr Evan Smith, for their contributions to this final publication.

Staff at the Australian Government Attorney-General's Department and the Australian Transaction Reports and Analysis Centre provided comments on earlier drafts. We are also grateful to the many individuals who agreed to participate in the survey and who agreed to be interviewed. The views expressed in this report are those of the authors alone and do not necessarily reflect the opinions or policies of the Australian Government or its agencies.

Executive summary

In 2009, the Australian Institute of Criminology (AIC) conducted a survey of 4,346 Australian businesses with anti-money laundering and counter-terrorism financing (AML/CTF) obligations under Australian legislation. The aims of the survey were to determine:

- perceptions of the risks of money laundering and financing of terrorism faced by these businesses;
- processes used by businesses in the compliance areas of customer identification and transaction monitoring;
- estimated costs for businesses to comply with the regime; and
- businesses' perceptions of the necessity and effectiveness of the regime and of the effectiveness of their compliance with it.

Methodology

Businesses were contacted by letter and telephone by staff from a social research company, the Social Research Centre, engaged by the AIC to carry out the survey. Contact details were provided by the Australian Transaction Reports and Analysis Centre (AUSTRAC) after permission in writing was obtained from AUSTRAC's Chief Executive Officer, subject to the AIC and the survey consultant agreeing to comply with strict protocols regarding security of information and confidentiality. The research was also approved by the AIC's Human Research Ethics Committee and the Statistical Clearing House of the Australian Bureau of Statistics.

Data were collected over a period of approximately 10 weeks between 31 July 2009 and 11 October 2009. Of the 10,670 addresses originally provided by AUSTRAC, 8,976 were included in the initial questionnaire mailing (a number were removed because they fell outside the sampling criteria), with 8,690 being confirmed as usable selections. A total of 4,346 survey responses were received, which was 50 percent of those selected (see Challice & Eliseo 2012 for further details). This provided a large sample of businesses from all sectors that were subject to AML/CTF regulation in Australia in 2009. The majority of respondents were small or micro businesses, as was the case with their level of representation in the regulated sector as a whole.

The participating businesses were from the gambling, banking, managed funds and superannuation, securities and derivatives, foreign exchange, alternative remittance, financial services and cash delivery sectors, and other businesses providing regulated services such as bullion dealers. Almost half of respondents came from the gambling industry (55.3%), while businesses from the financial services sector (23.5%) formed the second largest group. Only eight percent of respondents came from the banking sector. This may have influenced the results where analyses were conducted across the entire sample. Small and micro businesses comprised the majority of the sample, which may also have influenced the results in the study.

In addition to conducting the business survey, 10 individuals from businesses who completed the questionnaire agreed to participate in face-to-face interviews. These individuals worked in pubs and clubs, a credit union, a cash delivery business, a mortgage lender, a private equity firm and a currency exchange service. In addition, a representative from an Australian Government agency was interviewed. These interviews were conducted anonymously and no individuals or businesses were named or identifiable. The aim of the interviews was to ascertain additional information on some issues that the questionnaire was unable to canvass in detail. Interviews with such a small number of individuals cannot be considered to be representative of the entire regulated sector but nonetheless, the

qualitative data that were obtained provided some important, albeit subjective, insights into the operation of the AML/CTF regime in Australia.

The information presented in this report was collected during a period that coincided with the early implementation stages of Australia's AML/CTF regime. This period represented a phase during which the regulated sector was still adapting to the requirements and the effects of the legislation and as a result, some respondents might not have had a comprehensive understanding of how the legislative requirements affected their business operations. In addition, AUSTRAC has undertaken significant outreach activities with the regulated population since the data were collected.

Survey limitations

Although the current study was the first of its kind in Australia, the research was subject to a number of limitations. These are explained more fully in the separately published methodology report (Challice & Eliseo 2012). Some of the principal limitations are as follows.

It was apparent that some inconsistencies were present in how businesses from the same industry sector identified their primary sources of revenue in the self-reported demographic information.

In addition, and despite intensive pre-testing of the survey instrument and review by AUSTRAC and other stakeholders, as well as the use of a comprehensive glossary, the language used in the questionnaire to describe some aspects of the AML/CTF regime in Australia proved inaccessible to some survey respondents. This may have been more of an issue for some of the newly included business sectors. Some interviewees reported being motivated to participate in a follow-up interview in order to obtain feedback on difficulties they experienced in trying to respond to the survey. Depending on the extent of participants' difficulty in understanding some of the key terms employed, the results may not have captured the views of businesses recently included in the regime to an appropriate extent. Analysis of responses from participants who elected not to complete the survey suggested that non-corporate businesses, such as pubs and clubs, Australia Post outlets and retailers were over-represented in this group. More than 70 percent of those who elected to not complete the survey agreed that the regime was too onerous (Challice & Eliseo 2012).

Almost half of respondents consisted of businesses in the gambling industry. Businesses from the financial services sectors, such as banks, were under-represented. This might have influenced the results in situations where analysis was conducted across the entire sample. Small and micro businesses comprised the majority of the sample, which may also have influenced the results obtained in the study. At the time of writing, there was no publicly available information on the distribution of business size within the regulated sector, to determine whether the number of smaller businesses that responded were representative of the entire regulated sector.

Perceptions of the risks of money laundering and terrorism financing

Although there have been estimates that 'up to $10b a year in the proceeds of crime are available for laundering in and through Australia' (ACC 2011: 46), more than 97 percent of respondents considered that their business had a low risk of involvement in money laundering in the 2008–09 financial year. More than 95 percent of respondents across all business sectors believed that the level of risk of money laundering faced by their businesses in 2008–09 would remain the same or decrease in the ensuing two year period to 30 June 2011. Only nine businesses from the sample of more than 4,000 considered that money laundering posed a high risk to their business at the time.

Almost all of the businesses surveyed also considered that risk of terrorism financing was low in 2008–09. Again, more than 95 percent of respondents anticipated that the risk of their business becoming implicated in terrorism financing would remain the same or decrease in the two year period to 30 June 2011. Only two businesses considered that the risk of terrorism financing to their business was high.

The money laundering and terrorism financing (ML/TF) risks that participants speculated may affect their business in the two year period to 30 June 2011 were more likely to relate to the core internal

activities of the business than to some external threat. Businesses in certain sectors also believed that some of their customers were more likely than others to pose a risk of money laundering and financing of terrorism. For example, those in the financial services sector were more likely than those in other business sectors to consider that politically exposed persons (PEPs) and foreign companies posed greater money laundering risks than other types of customers. Individuals (both Australian and overseas residents) were the customer type most frequently nominated as posing higher risks of both money laundering and financing of terrorism than corporate customers.

Compliance

Survey participants were asked about three aspects of their AML/CTF activities—the procedures used to identify customers (so-called 'know-your-customer' (KYC) procedures), the extent to which they undertook ongoing customer due diligence and the extent to which they undertook pre-employment screening processes. It was found that 85 percent of businesses conducted ongoing customer due diligence procedures, with 80 percent complying with KYC requirements and 75 percent conducting pre-employment screening.

There was no significant difference in terms of rates of compliance with customer due diligence requirements between businesses that took the view that they faced few risks of money laundering or financing of terrorism and those who believed that they were at higher levels of risk. Similarly, there was no significant relationship between compliance with the three anti-money laundering measures outlined above and the perceived effectiveness of the regime generally.

A significant relationship was found between the business sector of participants and their likelihood of complying with KYC, ongoing due diligence and pre-employment screening processes. Businesses from the financial services sector were significantly more likely than other businesses to perform ongoing due diligence and KYC procedures. Businesses from these sectors, such as banks, as well as those offering cash delivery services were more likely than other sectors to conduct pre-employment screening.

Anti-money laundering/ counter-terrorism financing software

A number of software applications have been developed to assist businesses to comply with AML/CTF obligations. Some of these facilitate customer identification by enabling names to be matched with lists of internationally proscribed persons and organisations, while others enable transactions to be tracked and monitored for reporting purposes. The present survey asked respondents to indicate which types of software they used, if any, and to state whether or not the software they used was effective in meeting legislative obligations. Since 2009, a number of businesses may have begun using software for compliance purposes.

Less than one-quarter of businesses indicated that they used software for AML/CTF compliance purposes. Those in the gambling sector were the least likely to use AML/CTF software. The majority of businesses considered that procedures undertaken by staff and internal audit were effective in monitoring transactions, while only a few businesses agreed that software was an effective means of monitoring transactions for AML/CTF purposes.

Reporting suspicious matters

Australian reporting entities are required to submit various financial transaction reports to AUSTRAC. Reporting entities are required to lodge suspicious matter reports (SMRs) upon forming a suspicion that a customer may be dealing with the proceeds of crime or involved an offence or tax evasion. SMRs are discretionary reports and in Australia, may be triggered at any stage of a transaction.

Survey respondents were asked to indicate the circumstances in which the non-reporting of suspicious transactions to AUSTRAC may be justifiable. The largest proportion of businesses considered under-reporting of suspicious matters to be unjustifiable, while most businesses considered that over-reporting of suspicious matters could be justifiable. More than 70 percent of businesses

agreed over-reporting was justifiable where they were unsure of what a transaction involved. Almost 60 percent agreed that over-reporting was justifiable in order to avoid penalties for non-compliance.

Participants' views on under-reporting and over-reporting suspicious matters were associated with business sector. Businesses in the banking sector were the least likely to consider over-reporting justifiable in certain circumstances. Financial services sector businesses, such as banks, and securities and derivatives firms, were more likely to consider under-reporting justifiable in certain circumstances than other types of businesses.

The participants' business sector was also associated with the likelihood of identifying a suspicious matter in the year to 30 June 2009. Banks, despite holding more restrictive views on the justifiability of over-reporting than other business types, were most likely to have identified a transaction suspected of being linked to money laundering in the year to 30 June 2009. Participants outside the banking sector were more inclined than not to report a suspicious matter, while those in the banking sector were the most likely to actually encounter and identify a suspicious matter. None of the surveyed businesses reported matters involved with the financing of terrorism.

Compliance costs

Participants were also asked to estimate the approximate cost of complying with the AML/CTF regime over the 12 month period ending 30 June 2009. Owing to the fact that the period 2008–09 was one during which some businesses were starting to implement their AML/CTF systems, costs incurred during this period may have been quite high. The median expenditure on AML/CTF compliance was $1,000, with 57 percent of businesses reporting an AML/CTF expenditure of $1,000 or less for the year. The range of compliance expenses across the entire sample was from zero costs to $60m for the year in question. Managed funds and superannuation businesses had the highest median compliance costs of $6,000 in the 2008–09 financial year, while businesses from the foreign exchange sector and those classified as 'other' reported median costs of below $500.

Two-thirds of businesses believed that their costs would remain the same as in the 2008–09 year for the two years to 30 June 2011. Staff training and professional development, staff salaries, record keeping, monitoring and reporting accounted for the majority of compliance costs for Australian businesses.

The survey also sought to determine if businesses' expenditure on compliance in 2008–09 was associated with their views on the extent to which they considered compliance with the regime to be too onerous. It was found that businesses with higher costs were not more likely than other businesses to view compliance with the regime as being too onerous for the risks involved. The likelihood of participants viewing compliance with the regime as being too onerous, however, did not directly increase with the level of expenditure. Businesses that spent $1,000 or less in 2008–09 were more likely to give neutral responses to the question of whether the regime was too onerous for the risks involved than those that had higher expenditure.

Attitudes towards the AML/CTF regime

The largest proportion (45.5%) of respondents neither agreed nor disagreed that the system was too onerous with respect to money laundering risks. The proportion of respondents who agreed with the statement (30%) was slightly higher than the proportion who did not (25.7%). These findings indicate there was no strong feeling either way about the onerous nature of the regime. The businesses that considered the burden of compliance too onerous for the risks involved were the ones that also considered the regime to be less than effective in minimising the risks of ML/TF.

Some businesses anticipated that compliance with the AML/CTF regime would be an onerous process when it was introduced in 2006, but later found that compliance was relatively simple or found that AML/CTF enhanced existing compliance programs or other risk management processes, therefore not requiring fundamental changes to procedures already in place.

Overall, two-thirds of Australian businesses considered the regime to be effective in deterring

offenders, minimising risk of financial crime, minimising risks of money laundering, minimising risks of terrorism financing, maintaining the integrity of the financial system and promoting good governance practices. Respondents viewed the regime as being neither effective nor ineffective in facilitating proceeds of crime recoveries and minimising the risk of reputational damage.

Conclusion

Overall, it appeared that the Australian businesses regulated under the AML/CTF regime in 2009 who responded to the current survey believed that the risk of money laundering was low and that the risk of financing of terrorism was even lower. Overall, the perception of respondents was that the benefits of the regime appeared to justify the compliance burden that many businesses experienced. Respondents felt that there was a continuing need to improve the levels of education about the risk of money laundering and financing of terrorism in order to ensure that all levels of business in Australia appreciated the aims of the regime and how their compliance activities may assist in preventing and deterring serious financial crime.

Businesses without previous exposure to AML/CTF compliance were more likely to report difficulties with the system and to consider the regime as being overly onerous compared with the risks involved. Some of those businesses indicated they were experiencing difficulty with conducting risk assessments, implementing risk-appropriate measures and complying fully with the regulatory obligations.

Educational materials and training activities tailored to businesses without previous exposure to AML/CTF or other forms of financial regulation, or without other extensive compliance activities, were identified as potentially improving compliance and effective implementation of legislative requirements. Initiatives aimed at these sectors would be likely to improve businesses' capacity to conduct a risk assessment, which is the central component of the risk-based AML/CTF system. It might be inferred from the recommendations of respondents for better dissemination of education and training materials that the information made available to the regulated sector at the time of the survey did not assist some reporting entities in understanding and complying with the AML/CTF regime. In the period since the survey was conducted, AUSTRAC has developed a more extensive range of education, training and guidance materials, including industry-specific guidelines, risk management tools to assist small and medium-sized business to identify, assess and treat risks and annual typology reports describing known methods by which specific sectors have been used for ML/TF purposes. In addition, the private sector has developed new training courses for those involved in AML/CTF compliance work. For example, the Diploma of Applied Anti-Money Laundering and Counter-Terrorism Management is a new workplace-focused qualification, developed jointly by the Australian Financial Markets Association and the International Compliance Association. More recent surveys being undertaken by AUSTRAC as part of its 2010–11 supervision strategy should reveal whether longer exposure to the AML/CTF regime has delivered greater understanding of ML/TF risks and enhanced capacity to comply with regulatory obligations.

The findings presented in this report need to be viewed as part of a wider context, as business perceptions represent only one piece of the broader ML/TF picture. Due to the complexity and clandestine nature of ML/TF, most if not all businesses will only see a part of the environment. A significant amount of ML/TF and illicit financial activity can only be detected when government agencies examine larger holdings of transaction reporting and other information to which businesses rarely have access.

AUSTRAC and other government agencies provide guidance and information on ML/TF risks, including real life cases and methods that have been detected. But this information is, by necessity, limited. Intelligence and operational sensitivities restrict the amount of information and detail authorities can provide to businesses on actual cases or the full extent of the known ML/TF risk. Government authorities also acknowledge that they too do not possess comprehensive visibility of the entire ML/TF risk environment. For these reasons, business perceptions of ML/TF risk presented in this report need to be seen as only one view of the ML/TF environment in Australia.

Introduction

In 2009, the AIC undertook a survey of businesses that were, at that time, regulated under Australia's AML/CTF legislation. The aims of the survey were to determine:

- perceptions of the risk of ML/TF faced by these businesses;
- the processes they use in the compliance areas of customer identification and transaction monitoring;
- the estimated costs of compliance with the regime; and
- the perceptions of the necessity and effectiveness of the regime and of the effectiveness of compliance.

The survey focused on the experience of businesses with the AML/CTF regime in Australia in the 12 months prior to 30 June 2009 and also on expectations of how these aspects might change during the two year period from 1 July 2009 to 30 June 2011. This timeframe refers to the initial period of implementation of AML/CTF legislation by the Australian Government and the responses described herein refer to that period alone.

Specifically, the survey examined the following areas:

- information about respondents' business sector, staffing and turnover;
- AML/CTF procedures and software used for pre-employment screening of staff, due diligence and KYC;
- extent and effectiveness of customer identification and due diligence;
- extent and effectiveness of transaction monitoring and reporting;
- views concerning under- and over-reporting to AUSTRAC;
- current and future compliance costs;
- effectiveness of the AML/CTF regime and opinions about the extent to which the regime is onerous;
- views about how the regime could be improved; and
- current and future perceptions of ML/TF risks.

This report describes the results of the survey and where appropriate, integrates this information with the findings of previous surveys conducted by consultancy practices and government agencies.

In addition to conducting the survey, 10 individuals from businesses that completed the questionnaire agreed to participate in face-to-face interviews. These individuals worked in pubs and clubs, a credit union, a cash delivery business, a mortgage lender, a private equity firm and a currency exchange service. In addition, a representative from an Australian Government agency was interviewed. These interviews were conducted anonymously and no individuals or businesses were named or made identifiable. The aim of the interviews was to ascertain

more detailed information on some issues that the questionnaire was unable to canvass in detail. Interviews with such a small number of individuals cannot be considered to be representative of the entire regulated sector but nonetheless, the qualitative data that were obtained provided some important, albeit subjective, insights into the operation of the regime in Australia.

The anti-money laundering/counter-terrorism financing regime

The primary aims of those who commit economic crimes are to secure a financial advantage and to be able to make use of the stolen funds without being detected by police and regulatory agencies. Many offenders, but by no means all, seek to disguise the origins of their criminally derived funds by engaging in the process of money laundering. Others, however, simply disburse money with little attempt at concealment, which often leads to detection by police, followed by prosecution and punishment.

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 be in the financial system, such as where funds have been misappropriated electronically from business accounts. 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, thereby 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 offenders seek to enjoy the benefits of their crimes, without risk of detection.

In response to mounting international concern about money laundering, the Financial Action Task Force (FATF) was established in 1989. FATF is an inter-governmental body that sets international standards and develops and promotes policies to combat ML/TF. In 1990, FATF issued a set of 40 Recommendations to combat money laundering. The 40 Recommendations sets out the framework for anti-money laundering efforts and provides a set of countermeasures covering the criminal justice system and law enforcement, the financial system and its regulation, and measures to enhance international cooperation.

The FATF AML/CTF standards typically recommend provisions that criminalise ML/TF, enable freezing and recovery of assets linked to proceeds of crime and terrorist activities, and create a preventive regulatory system that aims to make ML/TF more difficult to commit and more likely to result in the detection and punishment of offenders. AML/CTF preventive measures are not uniform between countries but each regime broadly encompasses aspects of:

- customer identification;
- transaction monitoring;
- transaction reporting;
- record keeping;
- staff training; and
- compliance reporting.

AML/CTF preventive measures, unlike the criminal sanctions and asset recovery systems, are aimed at and implemented through private sector businesses rather than by law enforcement and prosecutorial agencies. The FATF's Recommendations suggest that countries implement preventive AML/CTF requirements for financial institutions and selected

non-financial businesses and professions that FATF believes are at risk of becoming involved in money laundering, the financing of terrorism or financing the stockpiling of weapons of mass destruction (FATF 2012).

Following the attacks on the United States on 11 September 2001, FATF expanded its mandate to address the financing of terrorism and created an additional eight (and subsequently 1 further) recommendations aimed at combating the funding of terrorist acts and terrorist organisations (Jensen 2005). The structure of the 9 Special Recommendations reflects the different aims of the two crimes and the different typologies used to commit each offence. The 9 Special Recommendations were intended to work in concert with the earlier 40 Recommendations targeted at money laundering and not as an independent separate system to address the financing of terrorism.

In June 2003, FATF completed a major review of its recommendations and on 15 February 2012, issued revised standards on combating ML/TF and stockpiling weapons of mass destruction. The revised FATF Standards strengthen global safeguards and further protect the integrity of the financial system by providing governments with stronger mechanisms to take action against financial crime, while also addressing new priority areas such as corruption and tax crimes. The revised Recommendations have been strengthened to deal with areas of increased risk and to deal with new threats such as the financing of proliferation of weapons of mass destruction. They are also emphasise transparency and are tougher on corruption. In addition, there is more flexibility for compliance in low risk areas, which allows financial institutions and other designated sectors to apply their resources to higher risk areas. FATF (2012) calls upon all countries to effectively implement these measures in their national systems. The AIC has published a separate study in which the response to the FATFs recommendations in a number of selected countries was reviewed (Walters, Budd, Smith, Choo, McCusker & Rees 2012).

The AML/CTF regime broadly refers to three core components adopted universally (to varying degrees) by developed nations and by the majority of developing countries to address both crimes (Chaikin & Sharman 2009). The FATF Recommendations form the basis for AML/CTF systems internationally (Sharman 2008).

Australian anti-money laundering legislation was implemented 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 suspicious 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 *Financial Transaction Reports Act 1988* (Cth) (FTR Act), was enacted to create barriers in Australia's financial and gambling sectors to discourage financially motivated offenders 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 required cash dealers to report suspicious transactions to AUSTRAC and to report certain domestic currency transactions and currency transfers to and from Australia, of $10,000 or more. The Act also required cash dealers to report international funds transfer instructions and verify the identities of account holders or signatories, as well as block withdrawals by unverified signatories to accounts exceeding certain credit balance or deposit limits. The Act also created an offence of opening or operating a bank account or similar account with a cash dealer in a false name. The FTR Act specified penalties for non-compliance with its reporting requirements or for provision of false or incomplete information. The reporting and identification requirements, backed by penalties for offences, provided a strong deterrent to money launderers and facilitators of money laundering.

The FTR Act was originally developed for a financial system in which most transactions were face-to-face and took place over the counter at branches of financial institutions. However, cashless, non face-to-face electronic transactions are increasingly replacing traditional cash-based transactions and

the range of financial services available to consumers outside the traditional banking sector has expanded greatly. Money laundering methodologies have continued to evolve, as these commercial and technological developments have created opportunities for criminals to exploit.

In 2005, FATF conducted its third review of Australia's AML/CTF regime and found that Australia did not comply with all of the FATFs Recommendations that were current at the time (FATF 2005). Partly as a consequence of this, Australia introduced the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act 2006 (Cth)) to address the concerns raised by FATF. The primary concerns related to customer due diligence and the resourcing of AUSTRAC. To some extent, it may be said that Australia's regulatory regime was criticised for not addressing a number of areas that had never been incorporated into its aims, such as the monitoring of PEPs (persons linked to senior positions in judicial, political, management or military arenas). In this regard, FATF's concerns about Australia's regulatory arrangements mirror FATFs expanded concerns beyond money laundering (and its initial emphasis to its links with the narcotics trade) to terrorism and terrorism financing. There was also a perception that the previous legislative regime had been too prescriptive and cumbersome, resulting in 'defensive reporting', a practice that threatened to overload regulators with information of dubious relevance and accuracy, and an inflexible response to new developments in money laundering techniques (Ross & Hannan 2007: 139).

In keeping with most comparable regulatory regimes (such as those in the United States and United Kingdom), the AML/CTF regime in Australia is risk based. The regime requires businesses that supply designated services to comply with the legislation, but there is discretion in how they meet some of these obligations. The focus of the legislation is on the nature of the service rather than on the entity that supplies it. The reporting entity is largely given responsibility—with general guidance and education from AUSTRAC—for both determining the level of risk represented by any customer and any transaction, and the appropriate response. Responsibilities such as customer due diligence show a change in emphasis from a regulatory 'tick and flick' based regime to one that emphasises the responsibility of reporting entities to maintain ongoing knowledge of their customers. The presumption is that a risk-based regime allows financial bodies (which presumably have more practical experience in dealing with actual clients) to be given more latitude in determining what level of risk any particular client or transaction represents and how best to manage that risk (Ross & Hannan 2007).

Under the FTR Act, AUSTRAC's responsibilities were related to specific industries and less than 4,000 cash dealers. Under the AML/CTF Act 2006 (Cth), a larger number of entities are regulated. At 30 June 2011, AUSTRAC reported that a total of 18,484 entities were enrolled with AUSTRAC Online (AUSTRAC 2011); a much broader family of regulated entities than under the FTR Act). Although AUSTRAC is the AML/CTF regulator in Australia, it does not have any law enforcement or prosecutorial powers. Therefore, it is an administrative-style Financial Intelligence Unit (FIU) that supplies information to a wide variety of government bodies. The financial intelligence it provides is used by these partner agencies to investigate cases of alleged financial crime, which may then be referred for investigation by police and prosecution.

The Australian legislative framework

Australia's legislative framework proscribes ML/TF and includes asset recovery mechanisms, as well as various preventive regulatory measures.

Money laundering offences

Division 400 of the *Criminal Code Act 1995* (Cth) (the Criminal Code) outlines the federal money laundering offences for Australia. The Criminal Code defines money laundering broadly and the only limit it places on predicate crimes is to restrict these to indictable offences—that is, money laundering involves dealing in the proceeds of indictable offences, as opposed to summary offences dealt with in lower courts. Division 400 of the Criminal Code specifies 18 separate money laundering offences of dealing with the proceeds and instruments of crime and an additional offence

of possessing the proceeds of crime. Offences for dealing with the proceeds and instruments of crime are distinguished by the value of the money or property involved and the mental element of the offence. The decision in *R v RK* [2008] NSWCCA 338 indicated that each of the 18 'dealing' offences created two separate offences. The first is an offence of dealing with the proceeds of crime; the second is an offence for dealing with the instruments of crime as Chief Justice Spigelman noted (at para 6):

> s 400.3(2)(c) creates an offence where a person is reckless as to a relevant fact. Furthermore, it creates two distinct offences where either:
>
> (A) the money or property is proceeds of crime and the person is reckless as to the fact that the money is proceeds of crime (s 400.3(2)(b)(i) and (c)).
>
> (B) there is a risk that the money or property will become an instrument of crime and the person is reckless as to the fact that there is a risk that it will become an instrument of crime (s 400.3(2)(b)(ii) and (c)).

All Australian states and territories, with the exception of the Northern Territory, have other money laundering offences. Offences relating to financing of terrorism, however, are solely at the federal level.

Financing of terrorism offences

Offences relating to the financing of terrorism are contained in two pieces of federal legislation, each of which has a separate definition of *terrorist organisation* that is applicable.

The Criminal Code contains general offences that proscribe the financing of terrorism. The *Suppression of the Financing of Terrorism Act 2002* (Cth) amended the Criminal Code by including a range of offences relating to the financing of terrorism. The *Anti-Terrorism Act (No. 2) 2005* (Cth) further amended the Criminal Code's financing of terrorism offences in 2005. The Criminal Code's offences currently encompass getting funds to, from, or for a terrorist organisation intentionally or recklessly, collecting funds to finance terrorism and collecting funds to finance a terrorist. Division 102 also criminalises the provision of resources or support to a terrorist organisation.

Terrorist organisations are defined by the Criminal Code as organisations:

- directly or indirectly engaged in, preparing, planning, assisting in, or fostering a terrorist activity, irrespective of whether one occurs; or
- that have been proscribed as terrorist organisations by the Attorney-General.

In addition, the *Charter of the United Nations Act 1945* (Cth) (CoTUNA) contains offences tied to asset freezing sanctions imposed on individuals and entities proscribed by the United Nations Security Council's 1267 list and certain other lists of proscribed persons. The individuals and organisations tied to offences under CoTUNA are identified in the Department of Foreign Affairs and Trade's Consolidated List. Section 20 creates an offence of holding a freezable asset and using or dealing with that asset, allowing another to use or deal with the freezable asset, or facilitating the use or dealing with an asset, unless the use or dealing has been authorised. Section 21 creates an offence for directly or indirectly making a freezable asset available to a proscribed entity, unless the dealing is an authorised dealing.

Asset recovery mechanisms

All Australian states and territories, in addition to the Commonwealth, have asset recovery mechanisms that enable the proceeds of crime to be recovered from entities. The bulk of the Commonwealth's asset recovery powers are held within the *Proceeds of Crime Act 2002* (Cth) (POCA 2002), which repealed the previous *Proceeds of Crime Act 1987* (Cth) (POCA 1987). The key change in the asset recovery regime in Australia that was introduced by POCA 2002 was the inclusion of a civil recovery mechanism. In addition, in 2010, the *Crimes Legislation Amendment (Serious and Organised Crime) Act* 2010 (Cth) amended POCA 2002 to include unexplained wealth provisions. The asset recovery mechanisms in some Australian states and territories, such as the Northern Territory and Western Australia, also extend the powers to recover the suspected proceeds of crime beyond civil confiscation and encompass unexplained wealth provisions.

Key preventive legislation

Australia's key AML/CTF preventive measures are contained in the AML/CTF Act 2006 (Cth) which, together with supplementary regulations and instruments, establishes Australia's compliance framework (see *Appendix* for definitions). The FTR Act, the previous core AML/CTF legislation, contains additional requirements and defines cash dealers (with reporting obligations) in Australia.

The AML/CTF Act 2006 (Cth) outlines much of the regulatory regime, as well as defining those businesses with AML/CTF regulatory obligations. The Act takes a service provision approach to describing the businesses with obligations (referred to as reporting entities). The AML/CTF regime currently applies to providers of designated services as defined in s 6. The general categories of regulated businesses are:

- 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;
- money service businesses—remittance dealers, issuers of traveller's cheques, foreign exchange dealers and cash couriers;
- the gambling sector—casinos, bookmakers, TAB's, clubs and pubs, internet and electronic gaming service providers; and
- bullion dealers.

The requirements of the AML/CTF Act 2006 (Cth) do not, as yet, extend to various non-financial service providers (known as Designated Non-Financial Businesses and Professions or DNFBPs)—such as legal practitioners and accountants engaging in financial or real estate transactions, trust and company service providers, dealers of precious metals and stones (outside of bullion dealers), and businesses in the real estate industry (although the government is considering the extension of the regime to these sectors; AGD 2009).

Australia requires all reporting entities to meet the same AML/CTF obligations, with few exceptions. Broadly, these obligations include:

- filing transaction reports, including threshold reports, to the FIU;
- performing risk-based customer identification procedures and monitoring customer transactions;
- establishing and maintaining an AML/CTF program;
- maintaining customer and transaction records;
- reporting on the level of compliance with the regime; and
- nominating a compliance officer.

The Australian regime is a risk-based system where reporting entities who provide 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. Reporting entities adjust the level of due diligence associated with each customer and transaction, according to their risk level, as well as to consider the level of risk posed by their different operations.

Financial intelligence unit

In Australia, AUSTRAC is both the FIU and AML/CTF regulator for all business sectors with AML/CTF obligations. AUSTRAC is not a law enforcement-style FIU and as such, does not have any investigative or prosecutorial powers. AUSTRAC's regulatory powers extend to monitoring compliance, issuing remedial directions, accepting enforceable undertakings and applying for civil penalty orders.

Reporting obligations

The AML/CTF regime currently requires reporting entities to provide the following reports about transactions to AUSTRAC:

- SMRs—reporting entities are required to submit SMRs on forming a suspicion that a transaction may be connected to a breach of taxation legislation or to the proceeds of crime. SMRs are discretionary reports that may be triggered for transactions of any value.
- Threshold transaction reports (TTRs; significant cash transaction reports for some entities)—reporting entities must report any transactions in physical currency beyond the threshold amount, which is currently $10,000 or more or the foreign currency equivalent. TTRs are mandatory, rather than discretionary, reports.

- Reports of international electronic transactions—reporting entities are required to report all electronic funds transfer instructions (international funds transfer instructions), regardless of value, to AUSTRAC. These are also mandatory reports.

Matters triggering TTRs and reports of international funds transfers may also be the subject of an SMR.

Anti-money laundering/counter-terrorism financing compliance programs

The AML/CTF Act requires all reporting entities to assess their own levels of ML/TF risks and to develop their own AML/CTF programs. Each program has two components. Part A of the program includes 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 KYC information requirements.

All reporting entities must report their compliance with the AML/CTF Act 2006 (Cth) annually to AUSTRAC.

Methodology

The way the current survey was undertaken, including detailed information concerning the design of the questionnaire, selection of participants, data collection, response analysis and data preparation is presented in a companion report published by the AIC (Challice & Eliseo 2012). The following is a brief summary of the key features of the methodology of the study.

The study was undertaken in two parts. The first comprised a survey administered to all businesses in Australia in July 2009 that had AML/CTF regulatory obligations. Respondents were able to complete a questionnaire online, by telephone or on paper, with responses forwarded to a consultant research organisation engaged by the AIC to administer the survey. The survey instrument also called for volunteers to participate in follow-up face-to-face interviews, which were conducted in October 2009 with 10 individuals from a range of sectors including one Australian Government department, pubs and clubs, a credit union, a cash delivery business, a mortgage lender, a private equity firm and a currency exchange service. Eight of the 10 interview participants came from the small business sector, which was the business sector in which most survey participants were employed. Interviews with such a small number of individuals cannot be considered to be representative of the entire regulated sector but nonetheless, the qualitative data that were obtained provided some important, albeit subjective, insights into the operation of the regime in Australia.

Ethical considerations

The study was approved by the AICs Human Research Ethics Committee, as well as the Statistical Clearing House of the Australian Bureau of Statistics, who monitor large surveys undertaken of Australian businesses by government agencies. Detailed protocols were also followed in connection with the provision of the sampling frame from AUSTRAC to ensure that data were held securely and that confidential information could not be compromised or released publicly. All results were reported in aggregate form in order to preserve participants' anonymity.

Survey instrument and interviews

The questionnaire asked respondents to report:

- views on, and procedures for, conducting customer identification and due diligence;
- views on, and procedures for, conducting transaction monitoring and reporting;
- views on under-reporting and over-reporting suspicious transactions;
- the extent of AML/CTF compliance costs, expectations of cost movements in the future, areas of greatest expense and means for reducing the expense;
- views on the effectiveness of the AML/CTF regime, the responsibilities assigned to businesses by the regime and means for improving how it operates;
- perceptions of money laundering risks to their business, including high-risk customers and changes to those risks; and

- perceptions of terrorism financing risks to their business, including high-risk customers and changes to those risks.

The follow-up interviews addressed the same themes, with a specific focus on the perceptions of money laundering and terrorism financing risks to business, the risk management practices used to mitigate those risks, the costs of complying with the AML/CTF requirements and the extent and utility of contact with AUSTRAC.

Respondents, sector and profile

AUSTRAC provided an initial sampling frame of 10,670 businesses believed to provide designated services under the AML/CTF Act 2006 (Cth) in 2009. The final sampling frame consisted of 8,690 businesses, of which 4,346 (50%) responded.

The confidential release of the mailing list was undertaken with the authority in writing of AUSTRAC's Chief Executive Officer at the time and was subject to strict conditions as to usage and confidentiality. A number of security measures were implemented by the Social Research Centre to ensure necessary privacy protocols were maintained and these are described by Challice and Eliseo (2012).

The difference between the number of businesses in the initial sampling frame provided by AUSTRAC and the final sampling frame used was explained because of duplicate entries in the initial list, which were present because many businesses were members of a Designated Business Group (DBG) who only needed to be contacted once. A DBG comprises two or more businesses or persons that join together to adopt and maintain joint AML/CTF program obligations under the legislation. Finally, over 1,000 of the records had incomplete or incorrect contact information.

Survey respondents fell into nine broad industry sectors. Respondents self-identified as working in:

- managed funds or superannuation—providing services as an investment company, managed fund, superannuation company, or unit trust manager;
- banking—encompassing banks, building societies, credit unions, finance corporations, friendly societies, housing societies, merchant banks and SWIFT;
- financial services—such as factorers, forfeiters, hire purchase companies, lease companies and pastoral houses;
- securities/derivatives—including futures brokers, investment banks and securities dealers;
- gambling—casinos, clubs, gambling houses, hotels and pubs, on course bookmakers, sports bookmakers and TABS;
- foreign exchange—providing services as foreign exchange providers, payment service provider/ postal and courier service providers, travel agents and issuers of travellers' cheques;
- cash delivery services—such as cash carriers, cash custodians and payroll service providers;
- alternative remittance dealers—including both corporate remitters and remittance providers;
- other—Australia Post outlets, news agents and other retailers, and bullion dealers.

Respondents were asked to identify the industry sector generating the largest proportion of income, or funds under management, in the year to 30 June 2009. The distribution of survey respondents across the nine industry sectors is shown in Table 1. Businesses generating the largest proportion of their income from gambling services (n=2,251) comprised more than 50 percent of respondents. The survey participants' businesses ranged in size from zero employees (those with casual or contract staff only) to more than 200 employees. The distribution of businesses provided in Table 2 shows that 79.7 percent of respondent businesses employed fewer than 20 full-time equivalent employees at 30 June 2009. This reflects the concentration of small businesses (76%) that identified their main revenue stream as coming from gambling activities.

As shown in Table 2, more than 90 percent of the survey sample was represented by small or micro businesses. Due to the absence of publicly available information, at the time of writing, on the distribution of business size within the regulated sector, it was unable to be established whether the number of

smaller businesses that responded to the survey were representative of the regulated sector as a whole. For this reason, care must be taken when interpreting the findings presented in this report.

Table 3 shows that the annual turnover for 81 percent of respondents, outside the managed funds and superannuation industries, was less than $5m for the year to 30 June 2009. Managed funds and superannuation companies, shown in Table 4, were asked to estimate their funds under management at 30 June 2009 with two-thirds (66.2%) reporting that they held less than $1m.

Respondents primarily occupied senior management roles within their companies. Approximately 65 percent (n=2,684) were owners, directors, or senior executives. A further 8.8 percent identified themselves as managers (n=364). Table 5 shows that few respondents were employed as risk or compliance officers (10.8%; n=448) or money laundering compliance officers (4.7%; n=194). The large number of managers, executives, or owners who participated in the survey is most likely due to the high proportion of small businesses that participated in the survey.

Table 1 Respondents, by industry sector

Industry sector	n	%
Managed funds and superannuation	356	8.8
Banking	313	7.7
Financial services	169	4.2
Securities and derivatives	115	2.8
Gambling	2,251	55.3
Foreign exchange	214	5.3
Cash delivery services	58	1.4
Alternative remittance businesses	195	4.8
Other businesses	397	9.8
Total	4,068	

Note: Percentages may not total 100 due to rounding

Source: AIC AML/CTF Australian businesses survey [computer file]

Table 2 Full-time equivalent employees at 30 June 2009

FTE employees	n	%
0	405	11.1
1–4	1,422	38.9
5–19	1,087	29.7
20–49	419	11.5
50–99	160	4.4
100–199	90	2.5
200+	75	2.1
Total	3,658	

Note: Percentages may not total 100 due to rounding

Source: AIC AML/CTF Australian businesses survey [computer file]

Table 3 Annual turnover, 2008–09

Turnover 2008–09	n	%
<$100,000	125	7.5
$100,001–$500,000	329	19.7
$500,001–$1,000,000	248	14.8
$1,000,001–$5,000,000	651	39.0
$5,000,001–$10,000,000	148	8.9
>$10,000,000	171	10.2
Total	1,672	

Note: Percentages may not total 100 due to rounding

Source: AIC AML/CTF Australian businesses survey [computer file]

Table 4 Funds under management at 30 June 2009

Funds under management	n	%
$0	253	36.2
$1–$100,000	93	13.3
$100,000–$500,000	82	11.7
$500,000–$1,000,000	35	5.0
$1,000,000–$5,000,000	59	8.4
$5,000,000–$10,000,000	14	2.0
$10,000,000–$50,000,000	49	7.0
>$50,000,000	114	16.3
Total	699	

Note: Percentages may not total 100 due to rounding

Source: AIC AML/CTF Australian businesses survey [computer file]

Table 5 Primary role of survey respondents within the regulated business

Respondents' role	n	%
Owner/director/Chief Executive Officer/Managing Director	2,684	64.7
Risk/compliance officer	448	10.8
Manager	364	8.8
Accountant/auditor	259	6.3
Money laundering compliance officer	194	4.7
Administration	84	2.0
Other	80	1.9
Legal officer/lawyer	38	0.9
Total	4,151	

Note: Percentages may not total 100 due to rounding

Source: AIC AML/CTF Australian businesses survey [computer file]

Reference periods

All retrospective survey questions asked respondents to consider the 12 month period to 30 June 2009. The reported volumes of suspicious transactions, AML/CTF implementation costs and cost areas all related to this period. Respondents were also asked to consider the two year period between 1 July 2009 and 30 June 2011 when responding to the prospective questions about future trends. These questions addressed respondents' views concerning expected changes to AML/CTF implementation costs and any changes to risks of money laundering or terrorism financing that they considered were likely to occur within their business during the specified two year period.

How this survey differs from other similar studies

The AML/CTF Australian businesses survey is the first large-scale study of Australian businesses regulated with respect to AML/CTF preventive measures. More than 4,000 Australian businesses responded to the survey from a population of around 17,700 businesses with AML/CTF regulatory obligations (AUSTRAC 2009b). This sample captured businesses from all regulated sectors and encompassed micro, small, medium and large businesses. The AML/CTF Australian businesses survey, as noted above, examined:

- businesses' perceptions of ML/TF risks;
- application of core components of the AML/CTF regulatory requirements, including specific detail on their approach, confidence and use of software when conducting customer identification and transaction monitoring measures;
- costs of implementing the measures;
- views on the necessity and effectiveness of the regime; and
- views on improving the regime.

The AML/CTF Australian businesses survey differed from AUSTRAC's survey of compliance officers in relation to the topics covered and the sample used. AUSTRAC's (2010a) survey examined the specific responsibilities of compliance officers and the AML/CTF reporting chain of command and focused predominantly on businesses offering financial services. In addition, more than half of the sample of AUSTRAC's study came from businesses that employed more than 50 staff members, while in this study less than 10 percent of businesses had 50 or more employees.

The present survey also examined in greater detail aspects of AML/CTF compliance documented in previous surveys undertaken in overseas jurisdictions. Gill and Taylor (2004) surveyed financial institutions in the United Kingdom in 2001 concerning the utility of AML/CTF regulation and the importance of customer identification requirements. They analysed 466 responses from those businesses surveyed. More recently, PricewaterhouseCoopers (2007) examined the perceptions and implementation by businesses of the risk-based approach to AML/CTF by financial services entities in the United Kingdom and the associated costs of doing so. Their research involved 148 interviews with money laundering reporting officers (MLROs) and other compliance professionals with anti-money laundering responsibilities from across the financial services sector including retail banks, investment banks, insurers and investment managers, and covering a range of different sized organisations. KPMG India (2009) sent a survey to 100 financial institutions in India and considered the application of transaction monitoring, the costs associated with AML/CTF compliance, risk-based assessments and customer identification, by banks and non-bank financial services in India. As such, these previous surveys have involved quite small samples and have been focused on quite specific aspects of the AML/CTF regime. The present survey was far more extensive, involved a survey of regulated businesses in Australia and examined a wide range of issues to do with AML/CTF regulation and compliance in Australia.

In view of the differing samples and objectives of these and other surveys, it has not been possible to draw direct comparisons between the present findings and those previously reported. Where some limited comparisons are appropriate, however, these have been identified and reported in the discussion below. The broader question of how Australia's legislative response compares with those in other countries has been addressed in a separate AIC publication (see Walters et al. (2012)).

Perceptions of money laundering and terrorism financing risks

One of the central tenets of the FATF Recommendations is a risk-based approach to preventing and detecting money laundering and the financing of terrorism (FATF 2012). A risk-based approach requires regulated businesses to determine the risks of ML/TF they face, identify customers and transactions posing high levels of risk, and mitigate those risks by implementing enhanced due diligence procedures (FATF 2007). Effective compliance with a risk-based AML/CTF regime requires businesses to understand the potential risks posed to their businesses and respond to them effectively (Gurung, Wijaya & Rao 2010).

Ross and Hannan (2007) have identified three risk elements, each of which needs to be considered in effective money laundering risk assessments—probabilistic, consequence and vulnerability risks. Probabilistic risk assessment involves the establishment of an association between an observable action and an activity the observer would like to detect. If money laundering and identity fraud have a strong association, to use Ross and Hannan's (2007) example, then the presence of identity fraud would suggest a high risk of money laundering. The assessment of consequence risk is tied to the potential impact of an activity. A small cash transaction may be illicit but its potential impact may be far smaller than a large illicit transaction. Monitoring large transactions in this example would be a better risk mitigation practice. Vulnerability risks are those that impede effective monitoring or detection, such as regulatory deficiencies or the presence of opaque transactions. Kini (2006) argues that the high-profile AML/CTF regulatory enforcement activity in the United States around 2006 illustrates the significance of a considered risk assessment program. ABN AMROs correspondent banking business with Russian banks constituted a high-risk activity in a high-risk location; Bank Atlantic's high net-worth business in Florida also entailed a high-risk business in high-risk locations. The banks, in both cases, failed to employ adequate AML/CTF controls and FinCEN, the AML/CTF regulator in the United States, imposed large penalties on both banks (Kini 2006). These cases illustrate the need for regulated businsses of all sizes to have an effective AML/CTF plan in place to assess the level of ML/TF risks that face their operations and to respond to such risks appropriately.

Perceptions of money laundering risks

One of the primary aims of the current study was to determine how Australian businesses perceived the AML/CTF regime and in particular, their views on the

customers that pose highest risks of money laundering, the types of money laundering risks posed to their businesses and the best ways in which they might be reduced. The respondents to the survey by industry sector and their primary role in the regulated business, are listed in Tables 1 and 5 respectively. Table 6 provides case studies of the types of high-risk customers that regulated businesses in Australia may encounter.

The AML/CTF Australian businesses survey asked respondents to identify the types of customers they viewed as posing the greatest risk of being involved in money laundering. Respondents were able to nominate multiple types of customers posing greater risks, selected from the following list:

- domestic companies;
- registered foreign companies;
- trustees;
- partnerships;
- incorporated and unincorporated associations;
- registered cooperatives;
- domestic government bodies;
- foreign government bodies;
- charities and not-for-profit associations;
- PEPs;
- Individuals—Australian residents (including sole traders); and
- Individuals—foreign residents (including sole traders).

Approximately 40 percent of all survey respondents nominated individual foreign residents as the type of customer posing the greatest risk of money laundering (see Table 6). A slightly smaller proportion (37.2%) selected individual Australian residents as those customers posing the greatest risks of money laundering. The proportions of respondents who nominated each customer type show that participants were least likely to nominate domestic government bodies as posing high risks of money laundering (4%).

While most respondents ascribed the greatest risks of money laundering to Australian and foreign resident individuals, the data showed some differences between how customers are perceived by different business sectors surveyed. Participants from the gambling sector held different views on who constituted a high-risk customer than did those from the financial services sectors such as banks.

A high proportion of survey respondents were from the gambling sector (n=2,252) and they appeared to perceive Australian residents as posing a greater risk of money laundering than respondents from the banking sector or those from the securities and derivatives sector. Approximately 41.2 percent of respondents from the gambling sector identified individual Australian residents as the customer group posing the greatest risk of money laundering, while 36.8 percent of banking sector respondents and 25.4 percent of securities and derivatives sector respondents considered Australian individuals to be high risk. In each case, the mean results for those in the gambling sector regarding clients perceived to present the greatest risk of money laundering were significantly different from those in the banking sector ($Z=31.5$; $p \leq 0.0001$) and those in the securities and derivatives sectors ($Z=35.6$; $p \leq 0.0001$).

Respondents from the gambling sector were, however, much less likely to consider that individual foreign residents held increased risks of money laundering (34%) than those in either the banking sector (54.9%) or in the securities and derivatives sector (57%). In each case, the mean results for those in the gambling sector concerning money laundering risks of foreign sector customers were significantly different from those in the banking sector ($Z=23.9$; $p \leq 0.0001$) and those in the securities and derivatives sector ($Z=29.2$; $p \leq 0.0001$).

Gambling sector respondents were also less likely to perceive PEPs as being high-risk customers than respondents from the banking sector or from the alternative remittance services sector. A relatively small percentage of gambling sector respondents (15.2%) identified PEPs as those who presented the greatest risk of money laundering; more than one-third of banks (38.2%) cited PEPs as high-risk customers. Comparing the means between these groups, significant differences were found between the perceptions of gambling and banking sector respondents with respect to the money laundering risks posed by PEPs ($Z=13.9$; $p \leq 0.0001$) and between those from the alternative remittance and banking sectors ($Z=-6.214$; $p \leq 0.0001$). This could, arguably, be explained on the basis that those in the

Box 1 Australian money laundering cases

The recently prosecuted money laundering cases in Australia summarised below offer some insight into the types of high-risk customers that the regulated business sectors may encounter.

A Ansari v R H Ansari v R (2007) 70 NSWLR 89; *Ansari v The Queen* [2010] HCA 18; *Regina v Z* [2006] NSWCCA 342

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 a man known as 'Z' in October 2003. The Ansaris then arranged for another person, 'H' to collect the money and deposit it on their behalf between October 2003 and May 2004. 'H' deposited $1,952,107 in amounts of less than $10,000 during that period. Via Exchange Point, the Ansari's moved illicit funds around within their country of origin without leaving any transaction records with a remittance service provider in that country.

The Crown alleged that the Ansaris knew that the funds would be deposited in amounts 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)).

Defendant 'Z' was an Israeli national who pleaded guilty to money laundering and drugs charges in 2004. Z's role was to deposit the proceeds from drug sales with Exchange Point and in 2004, Z advised the Ansaris that a deposit would be for more than $2m and would require more steps than the previous laundering activities. Z and a Belgian national, 'K' were arrested for possessing commercial quantities of MDMA. A statement later made by Z indicated he was employed by a Romanian national, 'R', to move money from Australia and he delivered more than $2m to Exchange Point on his first trip in 2003. R offered Z $10,000 in 2004 to undertake the same kind of laundering activities as those undertaken in 2003.The Ansari's appealed their sentences to the NSW Court of Appeal, which dismissed the appeals and affirmed the terms of imprisonment for the money laundering offences for which they were found guilty.

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

Huang and Siu each pleaded guilty to offences under the FTR Act (s 31(1)) and of money laundering under the Criminal Code (s 400.3(1)). Huang was paid $30,000 by his employer for remitting $3,088,311 to Hong Kong and China in 335 separate transactions in 2003. Huang used a branch of one of two major Australian banks to complete the transactions. He believed he was remitting legitimately gained funds that were being transferred offshore to evade Australian taxes. Siu believed the money to be the proceeds of an illegal fishing operation. Siu conducted 59 transactions, also through the same large Australian banks, between May and July 2003 to remit a total of $556,400. Siu was paid around $3,000 for his participation.

Trang Thi Phuong Nguyen 2010

In 2010, Nguyen pleaded guilty to money laundering for transactions she conducted between November 2007 and January 2008. Nguyen divided funds totalling $1.9m into accounts with balances of less than $10,000 and remitted the funds to individuals in Vietnam using false names (ACC 2010).

Long Thanh Money Transfer Company 2009

Seven people employed by the Long Thanh Money Transfer Company were convicted of money laundering in 2009. The individuals involved in the remittance businesses received sentences for laundering up to $68m (ACC 2009a). Three other defendants were convicted in October 2009 (ACC 2009b) for laundering sums of $9m, $5.5m and $4m respectively.

Nhon Anh Khuu and Chi Vien Duong 2009

Khuu and Duong defrauded the Australian Taxation Office (ATO) of $1.7m and $2.2m by creating an artificial network of subcontractors to disguise the nature of a labour hire business from the ATO, as well as receiving goods as payment for labour that were later sold. The defendants pleaded guilty to charges of defrauding the Commonwealth, obtaining property by deception, dishonesty causing a risk of a loss to the Commonwealth and dealing funds intended to become the instruments of crime.

Prchal, Raffaut, Rojas and Smetana 2008

Raffaut prepared amended tax returns containing false details for Prchal in 2001 and 2002, resulting in the ATO refunding Prchal $35,038.87. Raffaut then obtained the details of other tax payers and he and Prchal recruited Rojas to present those details to tax agents in order to obtain refunds from the ATO. Smetana was recruited to supply bank account details to receive the payments from the ATO. Smetana received eight percent of the total payment; Rojas received $200–250 per day for his role. The ATO paid $262,580.23 into Smetana's three accounts. The group claimed a further $162,121.89 that the ATO did not pay out. Smetana was convicted of recklessly dealing with the proceeds of crime to the value of $100,000 or more (CDPP 2009).

banking and remittance sectors would be more likely to encounter and hence form views about foreign PEPs than those in the gambling sector. Confirmation of this would, however, require further research. It should be noted that the majority of respondents within the gambling sector were from small business clubs and pubs, and that larger gambling sector entities such as casinos, may have a different view on the risks posed by PEPs.

The different perceptions of the level of risk of customers present in different industry sectors could also be due, in part, to the nature of the customer bases of these businesses. The large proportion of respondents from the gambling sector who perceived that individuals posed risks of money laundering (41.2%), as opposed to domestic companies (8.5%), reflects the customers of these businesses—gambling businesses generally only having individuals as customers. The interview data further confirmed this finding. Proprietors of pubs that have gaming machines considered that high levels of risk surround patrons who spend large sums at venues with multiple gaming. Domestic companies were, obviously, not involved in such activities.

Respondents were also asked to predict what they perceived as emerging money laundering risks to their businesses for the period from 1 July 2009 to 30 June 2011 (see Table 7). The unprompted response of approximately one-third of respondents (32.8%) was that they expected their businesses to face no money laundering risks in the two years to 30 June 2011. A further 18.7 percent of respondents expected there to be low risk or for risk of money laundering to decrease during that period. A much smaller proportion of respondents (1.5%) anticipated that risk of money laundering would increase.

Respondents from the cash delivery service sector were most likely to believe that there would be no money laundering risk for their businesses in the two years to 30 June 2011 (43.9%), while a further 21.1 percent anticipated that such risk would be low or would decrease. Respondents from the securities and derivatives sector were least likely to believe that there would be no money laundering risk to their businesses in the two years to 30 June 2011 (21.1%), although 25.4 percent of these businesses also anticipated that risks would be low or decrease during the ensuing two year period.

Apart from those who considered that their business faced no risks of money laundering or low or decreasing risks in the two years to 30 June 2011, gambling was the most commonly identified money

Table 6 Customers perceived to hold the greatest risks of money laundering

Customer type	n	%[a]
Individuals—foreign residents	1,670	39.9
Individuals—Australian residents	1,556	37.2
Registered foreign companies	932	22.3
Politically exposed persons	921	22.0
Foreign government bodies	638	15.2
Charities and not-for-profit organisations	545	13.0
Domestic companies	484	11.6
Partnerships	363	8.7
Trustees	360	8.6
Incorporated and unincorporated associations	351	8.4
Registered cooperatives	202	4.8
Domestic government bodies	168	4.0
Don't know	1,529	36.5
None selected	168	4.0

a: Respondents were able to select more than response; therefore, percentages do not total 100

Source: AIC AML/CTF Australian businesses survey [computer file]

laundering risk, selected by 288 respondents, although most of these (n=272) were from the gambling sector themselves. Most of the 2.7 percent (n=111) of respondents who nominated money transfers or foreign exchange as posing money laundering risks in the two years to 30 June 2011 (see Table 7) were also sector specific. The foreign exchange sector had the highest proportion of respondents who selected foreign exchange or money transfers as being a risk (13.8% of that sector's respondents). A statistically significant difference was found between the mean results for foreign exchange businesses and the next business category that identified foreign exchange as a high risk (7.9% of the 'other' category), in terms of foreign exchange being a money laundering risk in the ensuing two years to 30 June 2011 ($Z=-2.855$; $p \leq 0.004$). In summary, respondents from the foreign exchange sector were most likely to nominate money transfers or foreign exchange as a money laundering risk, as might be expected.

Changes in perceived money laundering risks

Survey respondents

Survey respondents were asked to consider the level of money laundering risk their business had been exposed to in the financial year prior to 30 June 2009 and how they perceived the level of risk may alter in the ensuing two year period to 30 June 2011. The findings are shown in Table 8.

The majority (97.8%) of survey respondents perceived the level of money laundering risk to their businesses in the year to 30 June 2009 to be low. A similarly high proportion of respondents (93.6%) expected the risk of money laundering faced by their businesses to remain the same in the two year period to 30 June 2011. These findings were obtained in 2009 from surveyed businesses and may not accord with the understanding of risk levels held by law enforcement agencies and regulators such as AUSTRAC (2011c) and the Australian Crime Commission (2011).

Table 7 Areas of perceived money laundering risk to 30 June 2011

Potential money laundering risk	n	%[a]
No perceived risks	1,375	32.8
Low risks/decreasing risks	785	18.7
Risks perceived to increase	62	1.5
Money transfer/foreign exchange	111	2.7
Gambling	288	6.9
New/unknown clients	88	2.1
Generic money laundering/proceeds of crime risks	45	1.1
Fraud	52	1.2
Drugs	45	1.1
Identity-related issues	45	1.1
Use of cash	33	0.8
Financial services	34	0.8
Superannuation	20	0.5
Internal fraud/staff issues	22	0.5
Tax evasion	19	0.5
Other	118	2.8
Don't know	190	4.5
No response	1,061	25.3

a: Respondents were able to select more than response; therefore, percentages do not total 100

Source: AIC AML/CTF Australian businesses survey [computer file]

Interviews

Interviewed participants explained in more detail why they perceived that their businesses currently faced few risks of ML/TF and why they thought these low levels of risk were unlikely to change in the foreseeable future. The customer profile of their business, stringent practices for acquiring new customers and KYC procedures, having few new customers, business size and the nature of their industries were the key reasons cited by the interview participants for the perception that they had very low or non-existent risks of ML/TF to their businesses (eg see Box 2).

Some interviewees took the view that money laundering and terrorism financing did not pose any risk to their businesses because of the nature of the industry in which they operated. For example, one interviewee from the funds management industry was unaware of any instances of funds managers who had been involved in ML/TF, although it is theoretically possible that funds managers could be involved in assisting money laundering activities unwittingly. Those from the gambling sector, predominantly owners of pubs and clubs that operated gaming machines, viewed the legislation as being necessary for financial institutions but considered it to be superfluous for a pub or club.

The small business owners who were interviewed each referred to the size of their businesses as the main reason why risks of money laundering and financing of terrorism were low. These individuals stressed that the size of their customer base allowed them to know their existing customers personally, effectively minimising risks to their businesses. The interview participants from the gambling sector provided a common example of how the size of their businesses might insulate them against risks of ML/TF. Gaming machines allow the possibility of placing large sums of money into each machine and having that money paid back out. A customer's capacity to do so in a venue with few machines, while remaining unnoticed by staff, would be exceedingly low. A larger venue with many more machines could offer, in the opinion of the interviewee, a more genuine opportunity for this to take place as the staff would be less likely to be able to monitor all of the gaming machines effectively. One interviewee observed that previously unknown customers in a small pub were immediately noticed by staff and some customers were inclined to monitor the behaviour of each other carefully—often in order to see which machines were likely to pay dividends more than others. The interviewee felt that this kind of environment almost completely removed the ability for anyone in the establishment to do anything untoward without attracting attention.

One interviewee noted that the cash-based nature of the hotel industry afforded a far greater opportunity to launder illicitly-gained funds than did the use of gaming machines. It was thought that hotels offered opportunities to co-mingle the proceeds of crime with legitimate turnover by discounting stock to increase the turnover of the business; or by adding false levels of stock into the stock monitoring system. One interviewee noted that the ability to co-mingle funds in a cash business was not tied singularly to the hotel industry—it had little to do with gaming facilities and more to do with the cash-intensive nature of businesses in general.

The risks identified by interviewees were very industry specific; or tied to the specific services offered by some businesses. For example, some of the risks posed to commercial banks were thought to arise from the remittance services and trade financing products they do business with. One interviewee explained that a bank's inability to verify the presence, absence, quantity, or price of commodities exposed it to risk that it may have provided finance for something entirely different than that represented and the money may have been paid back to the bank to develop a financial trail for it. The goods financed by a bank arrive at their destination port, money is exchanged and the transaction documents arrive weeks after a transaction has taken place. The transactions take place long before the bank's documentation arrives; it is not possible to examine the actual delivery even if the bank wanted to, or had the expertise to do so. The process becomes even more complex where the bank has provided financing for trade between two countries other than Australia.

Risks identified by an interviewee based on the Gold Coast concerned the location of the business. The director of this firm considered that the Gold Coast was a target for criminals testing out various scams. This director highlighted that the risks of doing

Table 8 Changing perceptions of money laundering risks

Risks to 30 June 2009			Risks from 1 July 2009 to 30 June 2011		
Current risk level	n	%	Expected change to risks	n	%
Low	3,785	97.8	Increase	128	4.0
Medium	76	2.0	Remain the same	2,991	93.6
High	9	0.2	Decrease	78	2.4

Source: AIC AML/CTF Australian businesses survey [computer file]

business in this location were increased by the highly transitory population and the absence of any industry apart from tourism.

The interviewee from the money-changing and remittance service business held a different view of the tourist-orientated location of his business. He viewed the customer base of tourists, cruise ship employees and migrant workers as posing a lower risk of becoming involved in ML/TF than a more diverse customer base that the same kind of business in a metropolitan location might attract. He did note that the only potential risk areas within the business stemmed from the remittance services he provided to migrant workers, but stressed that the identification requirements and transaction information needed to complete the transfer through the network he utilised eliminated those risks. Alternative remittance providers may, however, be subject to enhanced risks owing to close kinship or cultural ties with their customers, which may lead to subtle pressures to comply with high-risk requests. Smaller businesses, regardless of sector, also face capacity constraints in putting risk identification and mitigation programs in place. A regional pub owner agreed with the utility of the AML/CTF regime in metropolitan areas but did not see any risks of ML/TF to her business due to its location in a country town with a population of less than 10,000 people; she had never seen any evidence of either taking place and did not expect this to change in the next two years.

Interviewees highlighted the fact that opaque transactions within their businesses created a potential risk area for exposure to ML/TF. One interviewee expressed concern about the role of other financial institutions as intermediaries in the transactions made with his business. Borrower clients, for example, are able to make cash deposits in a branch of a major bank to service a loan. The mortgage company, in these instances, remained unaware if those payments were made as large cash payments. The mortgage company has had to rely on the bank to perform the appropriate due diligence in these situations. The opaque transactions identified by an interviewee in the mutual banking industry encompassed internet banking services, where the business has a decreasing amount of contact with customers, and in the capacity for account holders to nominate third-party signatories or power of attorney access to accounts. This left the business unsure about who was transacting through the account.

Perceptions of terrorism financing risks

Survey respondents were asked to consider the potential risks to their business of becoming involved in a transaction tied to the financing of terrorism in some way. All survey participants were asked to identify the customer types that they considered would pose the highest risk of becoming involved in the financing of terrorism and the types of terrorism financing risks that their businesses might face in the two year period to 30 June 2011. The survey sought to document the level of terrorism financing risks perceived by regulated businesses in the 2008–09 financial year and to document how regulated businesses expected those risks to alter in the forthcoming two year period. The study also documented the views of regulated businesses on the best strategies for reducing risks of terrorism financing. It should be noted that accurate intelligence on terrorism financing risks is not widely known among the community generally and few people in Australia could be expected to have the same level of understanding of risk levels as law enforcement and security agencies.

Table 9 shows the views of survey respondents as to the types of customers they perceived to hold the greatest risks of being involved in the financing of terrorism during the financial year 2008–09, selected from a predetermined list of customer types. It was found that more than 36.1 percent (n=1,511) of respondents believed that individuals posed the greatest risk, followed by PEPs (24.7%).

These results were significantly different according to the business sector the respondents occupied (χ^2=35.8, df=8, $p \leq 0.0001$). Comparing mean results for the highest perceived risk customer types, it was found that there was a statistically significant difference between the proportion of respondents who considered that individuals presented the highest risk of financing of terrorism and those who considered that PEPs presented the highest risk, with respondents across the entire sample perceiving risks from individuals to be the greatest (Z=11.31, $p \leq 0.0001$).

Changes in perceived financing of terrorism risks

Table 10 shows the views of respondents on the types of terrorism financing risks they considered would affect their businesses over the two year period to 30 June 2011, selected from a predetermined list of risk categories (see Box 3 for known Australian terrorism financing cases). The majority of respondents (57.9%) were of the view that their business would face no risks, or low risks, of terrorism financing in the two years to 30 June 2011. Approximately six percent of respondents did not know whether such risks existed or they were unable to predict the level of risk. Comparing mean results for response categories of no risk/low risk and don't know/can't predict the risk, it was found that there was a statistically significant difference between the proportion of respondents who considered that there were no/low risk of financing of terrorism and those who did not know or could not predict the risks for the two years to 30 June 2011 (Z=51.21, $p \leq 0.0001$).

The results were significantly different according to the business sector respondents occupied (χ^2=98.1, df=8, $p \leq 0.0001$). A Cramér's V of 0.16 indicated that there was a weak level of association between respondents' perceptions of risk and the business sector they occupied. The proportion of respondents from different business sectors who perceived no or low risk of terrorism financing ranged between 65.9 percent for financial services businesses to 40.4 percent of foreign exchange businesses.

Table 11 shows the views of respondents on the level of terrorism financing risks they considered have affected their business in the year 2008–09 and how the level of risk would change over the two year period to 30 June 2011. Almost all respondents (99.5%) considered there to be a low level of terrorism financing risk to their business in the year to 30 June 2009 and almost all (95.3%) anticipated that the level of risk would not change during the two years to 30 June 2011. The 17 respondents who considered that terrorism financing risks were

Box 2 Business perceptions of money laundering risks

The customer profile of a cash delivery business

All of the cash delivery business customers were well-known companies and entities that the public are familiar with; their customers did not include any individuals. A NSW Government department, with 900 sites that were serviced by the cash delivery business where all of the cash collected was in the form of coins, was a typical example of a client. All of the cash delivery business customers were based in Australia and no customer had ever requested that their funds be sent offshore.

Screening new customers in a private mortgage company

The private mortgage company held views on specific kinds of borrower clients that might pose higher risks of illicit dealings. These views were formed on the basis of the location that the business operates from. The company would not lend funds for some property development ventures or to other borrowers that they assumed may be likely to be involved in organised crime. The company had, unwittingly, loaned funds to borrowers to pay proceeds of crime warrants in the past. The company ameliorated the risks associated with these customers by clarifying the nature of the offence with the prospective borrower's lawyer and witnessing proof of the nature of the matter. Banks, faced with the same kind of loan application, have the capacity to request details of the debt, whereas a private mortgage lender does not have the same powers.

Source: Cash delivery business and private mortgage company representative, personal communication, November 2009

medium in 2008–09 were spread across the gambling (n=6), banking (n=4), alternative remittance (n=2), foreign exchange (n=2), managed funds and superannuation (n=1), and other (n=1) business sectors. The two respondents who considered risks to be high were both from the gambling sector.

Perceived effectiveness of anti-money laundering/ counter-terrorism financing measures

Respondents were also asked to identify the countermeasures that they considered would be most effective in minimising ML/TF risks to their businesses.

Anti-money laundering measures

Table 12 presents the results for anti-money laundering measures grouped into 17 categories. The most commonly identified measures that respondents considered to be effective in minimising money laundering related to customer identification and due diligence (14.6%). Considerably fewer respondents viewed transaction monitoring (6.4%) or reporting (2.9%) as effective countermeasures.

The large 'no response' rate, compared with the limited positive response rates given for each of the suggested risk mitigation measures listed in Table 12, maybe due to a lack of understanding of the utility of the risk mitigation measures proposed, a lack of understanding regarding the differential functions of the risk mitigation measures and/or a level of indifference to the effectiveness of any or all of these measures. In turn, this may be because respondents came largely from small or micro businesses that do not always have extensive AML/CTF compliance measures in place. However, the majority of respondents, irrespective of the sector they represented, did use basic compliance measures and most believed these were effective in minimising ML/TF risks faced by their business (see next section). Alternatively, views may have been influenced by the educative resources available to entities at the early stages of implementation of AML/CTF regulatory obligations, which have been described as possibly being limited in both sector specificity and accessibility (eg see Bricknell et al. 2011 and Choo et al. forthcoming).

The extent to which respondents nominated customer due diligence as the most effective strategy against money laundering varied significantly according to the respondent's business sector (χ^2=124.2, df=8, $p \leq 0.0001$), although a Cramér's V of 0.18 indicated that there was only

Table 9 Customers perceived to hold the greatest risk of terrorism financing

Type of customer	n	%
Individuals	1,511	36.1
Domestic and foreign companies	837	20.0
Charities and not-for-profit organisations	500	11.9
Partnerships	303	7.2
Registered cooperatives	200	4.8
Politically exposed persons	1,035	24.7
Foreign government bodies	815	19.5
Incorporated and unincorporated associations	366	8.7
Trustees	289	6.9
Domestic government bodies	174	4.2
Don't know	1,898	45.3
No response	138	3.3

Note: Respondents were able to select more than response; therefore, percentages do not total 100

Source: AIC AML/CTF Australian businesses survey [computer file]

a weak level of association between respondents' identification of effective anti-money laundering measures and the business sector they occupied. Fewer gambling sector respondents (10.9%) nominated customer due diligence as the most effective countermeasure to money laundering than respondents from the banking (19.4%) or managed funds/superannuation (24%) sectors. Comparing mean results for responses from gambling sector respondents with those from the banking sector, it was found that there was a statistically significant difference between the proportion of respondents who identified customer due diligence as an effective anti-money laundering measure ($Z=14.18$, $p \leq 0.0001$). Similarly, there was a statistically significant difference between the proportion of respondents from the gambling sector who identified customer due diligence as an effective anti-money laundering measure and those in the managed funds and superannuation sectors ($Z=12.35$, $p \leq 0.0001$).

Approximately 11 percent of respondents stated that there were low risks, or no risks associated with money laundering and that, accordingly, they did not see the need for any countermeasures. The extent to which respondents stated that there were no risks of money laundering to their businesses and accordingly, no anti-money laundering measures were needed, varied significantly according to the respondent's business sector ($\chi^2=44.5$, df=8, $p \leq 0.0001$), although a Cramér's V of 0.18 indicated that there was only a weak level of association present. Cash delivery services was the sector most likely to indicate that no risks were present and that no measures were necessary to address money laundering (19.3%). Only 4.7 percent of respondents from the alternative remittance sector considered there to be no risks and no countermeasures required. Comparing mean results for responses from gambling sector respondents (13.4%) with those from the banking sector (10.2%), it was found that there was a statistically significant difference between the proportion of respondents who indicated that their businesses faced no risks or low risks of money laundering ($Z=-19.7$, $p \leq 0.0001$), with gambling sector respondents being more likely to indicate an absence of risk than those from the banking sector.

Counter-terrorism financing measures

Respondents were also asked to identify the countermeasures that they considered would be most effective in minimising financing of terrorism risks to their businesses. Table 13 presents these results grouped in 12 categories. Respondents most commonly indicated that no countermeasures were necessary, or they had no suggestions as to the measures required (36.4%). The proportions of each sector who indicated that no measures were

Table 10 Perceived terrorism financing risks to business to 30 June 2011

Perceived terrorism financing risk	n	%
No risk/low risk	2,425	57.9
Money transfer/foreign exchange	70	1.7
Gambling	48	1.2
Increased business/new customers/new products	27	0.6
Unknown customers/investors/services	26	0.6
Identity fraud/other fraud	21	0.5
Cash	8	0.2
Charities	3	0.1
Other	451	10.7
Don't know/can't predict	241	5.8
No response	912	21.8

Note: Respondents were able to select more than response; therefore, percentages do not total 100

Source: AIC AML/CTF Australian businesses survey [computer file]

Box 3 Australian terrorism financing cases

Very few defendants have been charged with terrorism financing offences in Australia (see Smith, McCusker & Walters 2010). The case of Vinayagamoorthy does not provide any great insight into the potential covert use of the Australian financial system for the purposes of providing financing to terrorist organisations or for terrorist actions. The prosecution contended that the defendants generated funds by selling stolen car parts and made personal donations to a group pool of funds. The judgements in this case did not explicitly describe whether any of these funds entered the financial system, remained as cash, or were simply spent on goods or services.

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 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 three defendants collected funds from the Tamil community in Australia through the Tamil coordinating committee, the TCCE, and provided them to the LTTE between 2002 and 2005. The court accepted that the defendants were motivated, in part, by a desire to assist the Tamil community in Sri Lanka. 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 ANB 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 convicted of attempting to intentionally make funds available to a terrorist organisation pursuant to s 102.6(1) of the Criminal Code. 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. Applications for leave to appeal against conviction and sentence were lodged by all the defendants and were heard by the Victorian Court of Appeal in March 2010. On 25 October 2010 the Court delivered judgement. The convictions recorded against each of the defendants with respect to the principal offences were upheld although other convictions for possessing a thing connected with preparations for a terrorist act were overturned. The defendants were resentenced. Applications for special leave to appeal to the High Court of Australia by three of the defendants were refused (CDPP 2011: 71).

Table 11 Perceptions of the level of terrorism financing risks to businesses

Risks to 30 June 2009			Risks from 1 July 2009 to 30 June 2011		
Current risk level	n	%	Expected change to risks	n	%
Low	3,522	99.5	Increase	84	2.8
Medium	17	0.5	Remain the same	2,822	95.3
High	2	0.1	Decrease	55	1.9
Total	3,541		Total	2,961	

Note: Percentages may not total 100 due to rounding

Source: AIC AML/CTF Australian businesses survey [computer file]

necessary or that they had no relevant suggestions ranged from more than 40 percent of respondents from the securities and derivatives sector to 24.4 percent from the financial services sector. The extent to which respondents stated that there were no counter-terrorism financing measures needed or that they had no relevant suggestions regarding counter-measures, varied significantly according to the respondent's business sector (χ^2=41.0, df=8, p≤0.0001), with a Cramér's V of 0.10 indicating a weak level of association being present.

The most commonly identified measures that respondents considered to be effective in minimising terrorism financing related to customer identification and due diligence (9.5%) and as noted above, 14.6 percent of respondents suggested that this was also an effective countermeasure for money laundering risks. Only 1.7 percent of respondents considered that identity checks, use of watch lists, criminal background checks and other institutional checks would be effective counter-terrorism financing measures. Comparing mean results from respondents who indicated that no measures were needed and those who indicated that customer due diligence was the most effective counter-terrorism financing measure, it was found that there was a statistically significant difference between these two groups of respondents (Z=29.3, p≤0.0001).

On the whole, KYC procedures were considered to be effective in countering both money laundering and financing of terrorism risks, possibly because these are widely known and used already by many businesses. Many respondents, however, had no suggestions concerning effective countermeasures owing to the perceived very low levels of risk that they faced. Again, reasons surrounding the lack of understanding of utility, a lack of understanding of the differential purposes of the measures and/or indifference to the regime may explain the limited positive responses received to the risk mitigation measures proposed.

Table 12 Measures most effective in minimising money laundering risks to business

Risk mitigation measure	n	%
KYC/customer ID/more customer ID/ID card	611	14.6
Staff training/vigilance/awareness	450	10.7
In house/existing procedures/no change needed	401	9.6
Ongoing monitoring/vigilance/observation	311	7.4
Transaction monitoring	269	6.4
Limit transactions (such as by size)	123	2.9
Reporting	120	2.9
Compliance/increase compliance/AUSTRAC or AML/CTF Act measures are fine	101	2.4
Intelligence sharing/ID verifying database/list of high-risk customers	80	1.9
Software	69	1.7
Need information/training/typologies from AUSTRAC	60	1.4
Update/assess procedures/improvement	41	1.0
Other legislation/regulation already covers it	31	0.7
General public awareness	39	1.0
Other	168	4.0
Don't know	297	7.1
Low risks/no risks/need nothing at all	478	11.4
No response	1,279	30.5

Note: Respondents were able to select more than response; therefore, percentages do not total 100

Source: AIC AML/CTF Australian businesses survey [computer file]

Table 13 Effective measures for minimising terrorism financing

Risk mitigation measure	n	%
Due diligence/Know your customer	396	9.5
Education and training	286	6.8
Following in-house policies and procedures	268	6.4
Transaction monitoring	214	5.1
Awareness/observation/vigilance	149	3.6
Better communication with government, law enforcement and other agencies	117	2.8
Reporting suspect transactions/individuals/instructions	102	2.4
Existing legislation, policies, procedures	101	2.4
Limiting services (such as no cheques, no cash out)	72	1.7
Identity checks/watch lists/criminal checks/institution checks	71	1.7
Other	1,248	29.7
No measures needed/no suggestions	1,526	36.4

Note: Respondents were able to select more than response; therefore, percentages do not total 100

Source: AIC AML/CTF Australian businesses survey [computer file]

Compliance measures

In Australia, as noted above, reporting entities that provide designated services are required to comply with various AML/CTF obligations including filing financial transaction reports such as threshold reports to AUSTRAC, performing risk-based customer identification procedures and monitoring customer transactions, establishing and maintaining an AML/CTF program, maintaining customer and transaction records, reporting on the level of compliance with the regime and nominating a compliance officer to AUSTRAC. A risk-based system has been developed in Australia where entities are required to assess the risks associated with specific customers and transactions, and to determine how to mitigate that risk by meeting the obligations under the Act. Reporting entities are able to adjust the level of due diligence associated with each customer and transaction according to their risk level, as well as to consider the level of risk posed by their different operations. Accordingly, regulated businesses may have different AML/CTF programs in place and act differently from one another in fulfilling their obligations under the legislation.

Each business must conduct a risk assessment of its customers, the services it provides and the methods it uses to deliver them, any foreign jurisdictions it deals with and any additional risks stemming from permanent foreign offices (AUSTRAC 2008). The customer identification, enhanced due diligence and ongoing due diligence, transaction monitoring and reporting requirements are tied to the business' evaluation of the risks posed by its customers and operations. Compliance beyond these measures involves record keeping and staff screening obligations. Businesses in Australia are also required to submit an annual compliance report to the regulator detailing their compliance activities (AUSTRAC 2009b).

AUSTRAC (2009c) has noted that authorised deposit-taking institutions (ADIs) and investment banks are comfortable with AML/CTF compliance requirements. Smaller ADIs and non-ADI lenders, smaller financial service providers, smaller gambling and bullion entities, and money service businesses may find the processes of conducting risk assessments and implementing risk-based programs more problematic.

In the absence of other Australian surveys dealing with questions of compliance, it is appropriate to review the results of some overseas studies. Survey data from the United Kingdom in 2007 have found generally high levels of compliance with AML/CTF risk assessment requirements and follow-up procedures. Almost all of the MLROs surveyed in the United Kingdom in 2007 had undertaken a formal risk assessment of their business, although

14 percent had not developed a strategic response to the risks identified in this process. A further two percent of this group of MLROs were unsure if a response had been developed (PricewaterhouseCoopers 2007). The businesses within PricewaterhouseCoopers' sample that had experienced problems implementing a risk-based approach to the United Kingdom's AML/CTF regime reported concerns about time constraints, resourcing demands and difficulties altering existing processes. In another survey of Indian financial services businesses undertaken by KPMG (India) (2009), Indian businesses with AML/CTF requirements reported a similar level of compliance to those in the United Kingdom for some aspects of the regime, with close to 90 percent of respondents reporting having used a risk-based approach to customer due diligence when opening new accounts in 2009 and a further eight percent of businesses considered doing so (KPMG (India) 2009).

Previous studies have, however, suggested that reporting entities have not fared as well in the process of implementing effective procedures for transacting with PEPs, a class of customers identified by FATF as having high levels of risk in terms of ML/TF (Choo 2010 and references cited therein; see also the AICs review of international developments in Walters et al. 2012). Previous surveys of regulated businesses have found that identifying PEPs and their associates, and ameliorating the risks posed by PEPs, remain problematic. More than 70 percent of the MLROs surveyed in 2001 (Gill & Taylor 2004) considered the United Kingdom's regulations insufficient to identify the links between PEPs and their family members and associates. By 2007, just under half of surveyed MLROs in the United Kingdom did not have a list of PEPs for use through all areas of their business (PricewaterhouseCoopers 2007). By 2009, more than half of KPMG's sample of Indian financial services businesses had implemented procedures for identifying PEPs. Of those with PEP identification procedures, 56 percent used a purchased list as well as internal lists to identify the relevant, while a further 36 percent used a purchased list alone (KPMG (India) 2009). A majority of Tier One banks reported performing enhanced due diligence for PEPs opening accounts and 70 percent of this sample reported conducting ongoing transaction monitoring for PEPs. The authors of this report note that, in the absence of a universally accepted definition, the measures applied by these banks are unlikely to be uniform (KPMG International 2007).

Anti-money laundering/ counter-terrorism financing procedures used

In the present survey, respondents were asked to indicate the extent to which they complied with the basic requirements of the AML/CTF regime in Australia. The participants were asked which of three core AML/CTF measures their businesses undertook (pre-employment screening of staff, ongoing customer due diligence for current customers and KYC procedures for new customers). They were also asked to indicate what additional AML/CTF measures their businesses employed. The data shown in Tables 14, 15 and 16 show that the proportion of businesses that conducted pre-employment screening, KYC processes for new customers and ongoing customer due diligence for existing customers varied according to the business sector they occupied. Rates of non-compliance with the three nominated AML/CTF requirements across the entire sample also differed for each of the three AML/CTF requirements examined. Approximately one-quarter (23.5%) of all respondents did not conduct pre-employment staff screening at all (see Table 14), while 15.4 percent did not carry out ongoing due diligence for existing customers (see Table 15), and 19.8 percent did not conduct KYC procedures for new customers (see Table 16).

The majority of participants from all business sectors (more than 75%) reported screening prospective staff, although the data in Table 14 show variable compliance rates according to business sector. Businesses in the managed funds and superannuation sector reported the highest pre-employment screening compliance rates (90.8%). Alternative remittance sector businesses and businesses in the 'other' sector category reported the lowest rates of compliance with pre-employment screening (65.5% and 63.6% respectively). These results were significantly different according to the business sector

respondents occupied (χ^2=125.6, df=8, p≤0.0001). A Cramér's V of 0.18 indicated that there was a weak level of association between use of pre-employment screening and the business sector they occupied.

A statistically significant relationship was also found between levels of compliance with the requirement to conduct ongoing due diligence for existing customers and the business sector respondents occupied (χ^2=49.863, df=8, p=0.000; Cramér's V=0.113) (χ^2=49.9, df=8, p≤0.0001). A Cramér's V of 0.11 indicated that there was a weak level of association between these variables. Financial services sector respondents were most likely to report conducting ongoing due diligence for existing customers (92.7%), while those in the category of 'other businesses' were least likely to conduct due diligence (77.2%; see Table 15). Comparing mean results for these two groups, it was found that there was a statistically significant difference between respondents from the financial services sector and those in the 'other businesses' category who reported complying with ongoing due diligence requirements (Z=-7.4, p≤0.0001). Generally, however, all respondents reported very high levels of compliance with ongoing due diligence obligations under the legislation.

In relation to compliance with KYC requirements, it was found that over 80 percent of respondents reported using such procedures for new customers (see Table 16). Compliance with these requirements differed significantly across business sectors (χ^2=122.1, df=8, p≤0.0001), although a Cramér's V of 0.18 indicated only a weak level of association between KYC compliance and sector. The highest levels of KYC compliance for new customers existed in the managed funds/superannuation sector (92.8%) and the financial services sector (92.7%). Lowest levels of compliance with KYC procedures for new customers were reported in the gambling (75.7%) and foreign exchange sectors (79.3%). Comparing mean results for the managed funds/superannuation sector and respondents in the category of 'other businesses', it was found that there was a statistically significant difference between the proportion of respondents who reported complying with statutory KYC requirements in these two sector groups (Z=1.4, p≤0.0001).

Comparing mean results for responses from respondents concerning non-compliance with staff screening and KYC processes, it was found that there was a statistically significant difference between these two groups (t=-3.1; df=8358.6; p≤0.002). There was also a statistically significant difference between use of staff screening and ongoing due diligence procedures for new customers (t=-8.6; df=8209.5, p≤0.0001), and also for the use of KYC processes and ongoing customer due diligence (t=5.5; df=8297.4; p≤0.0001). Overall, reporting entities were most likely to have complied with ongoing customer due diligence requirements and were more likely to have complied with KYC requirements than pre-employment staff screening.

Additional anti-money laundering procedures identified by respondents that were not part of the measures listed included:

- record keeping, monitoring and reporting (n=47; 1.2% of respondents);
- general compliance with the AML/CTF regime (n=67; 1.6%);
- training and professional development (n=38; 0.9%);
- limiting risks by placing restrictions on transactions (n=18; 0.4%); and
- stating that the customers and staff are personally known to the business, making KYC unnecessary (n=12; 0.3%).

Overall, it appears that high proportions of businesses complied with the risk-management procedures specified in the AML/CTF Act 2006 (Cth) and other processes designed to minimise money laundering risks.

Anti-money laundering/ counter-terrorism financing software

Prior international research

As background to the results of the present Australian survey, it is useful to consider the results of previous overseas studies that have reported the varying degrees to which AML/CTF-specific software has

Table 14 Pre-employment screening, by business sector

Business sector	Conducts screening		Does not conduct screening	
	n	%	n	%
Managed funds/superannuation (n=346)	314	90.8	32	9.3
Banking (n=304)	251	82.6	53	17.4
Financial services (n=164)	141	86.0	23	14.0
Securities and derivatives (n=114)	103	90.4	11	9.7
Gambling (n=2,184)	1,669	76.4	515	23.6
Foreign exchange (n=203)	148	72.9	55	27.1
Cash delivery (n=57)	51	89.5	6	10.5
ARS (n=192)	122	65.5	70	35.0
Other businesses (n=360)	229	63.6	131	39.3
Total (n=4,189)	3,028	76.5	896	23.5

Source: AIC AML/CTF Australian businesses survey [computer file]

Table 15 Ongoing due diligence for existing customers, by business sector

Business sector	Conducts due diligence		Does not conduct due diligence	
	n	%	n	%
Managed funds/superannuation (n=346)	314	90.8	32	9.3
Banking (n=304)	274	90.1	30	9.9
Financial services (n=164)	152	92.7	12	7.3
Securities and derivatives (n=114)	104	91.2	10	8.8
Gambling (n=2,184)	1,810	82.9	374	17.1
Foreign exchange (n=203)	171	84.2	32	15.8
Cash delivery (n=57)	50	87.7	7	12.3
ARS (n=192)	165	85.9	27	14.1
Other businesses (n=360)	278	77.2	82	22.8
Total (n=3,924)	3,318	84.6	606	15.4

Source: AIC AML/CTF Australian businesses survey [computer file]

Table 16 Know-your-customer requirements for new customers, by business sector

Business sector	Conducts KYC		Does not conduct KYC	
	n	%	n	%
Managed funds/superannuation (n=346)	3,321	92.8	25	7.2
Banking (n=304)	272	89.5	32	10.5
Financial services (n=164)	152	92.7	12	7.3
Securities and derivatives (n=114)	103	90.4	11	9.7
Gambling (n=2,184)	1,653	75.7	531	24.3
Foreign exchange (n=203)	161	79.3	42	20.7
Cash delivery (n=57)	51	89.5	6	10.5
ARS (n=192)	169	88.0	23	12.0
Other businesses (n=360)	266	73.9	94	26.1
Total (n=3,924)	3,148	80.2	776	19.8

Source: AIC AML/CTF Australian businesses survey [computer file]

been used by businesses in connection with their discharge of AML/CTF legislative obligations. For example, 34 percent of the Tier One banks surveyed by PricewaterhouseCoopers in its 2007 survey in the United Kingdom, monitored transactions electronically and of these, 29 percent purchased the software from a third-party provider (PricewaterhouseCoopers 2007). Within this group, fewer smaller companies used automated monitoring than did larger firms. A quarter of companies that employed fewer than 100 staff had automated transaction monitoring systems in place, while almost double this proportion (42%) of companies with more than 100 employees did so.

Another study found that half of the US-based life insurance companies surveyed by Ernst & Young (2007) had AML/CTF systems dependant, to some extent, on automated services. The companies that had automated their AML/CTF programs predominantly used systems developed in-house, with approximately 35 percent purchasing software instead of developing it. This group of companies nominated human resources expenditure as the most costly area of their AML/CTF electronic systems. Approximately 30 percent of respondents spent between US$250,000 and US$1m on human resources management and all of the companies surveyed spent less than US$250,000 on software and hardware combined.

In the United Kingdom, one-third of MLRO's surveyed in 2007 (PricewaterhouseCoopers 2007) stated that their companies needed to improve their AML/CTF systems. They specifically identified the need to enhance or automate their transaction monitoring procedures and to improve staff training. They also indicated that an electronic identification, or an electronic means of certifying identity, would improve their systems. In a survey of financial services businesses in India undertaken by KPMG in 2009, the majority of those surveyed monitored sanctions lists as part of their transaction monitoring programs, with more than 40 percent of these businesses using software specifically designed for this purpose (KPMG India 2009).

A case study involving a Luxembourg private bank's AML/CTF software selection process showed the predominant considerations of the bank for system flexibility, accuracy, service and follow-up procedures for flagged transactions when selecting appropriate systems. The central concern of the bank prior to making software decisions was that any automated transaction monitoring system should be fit-for-purpose in terms of the bank's regulatory obligations, business operations, potential expansion plans and resources (Veyder 2003).

Survey results

The present AML/CTF Australian business survey sought to document the proportion of survey participants who used software of differing kinds to assist with Australian AML/CTF requirements compliance. The responses refer to software and other systems specifics that were available or used by respondent businesses at the time of the survey in 2009 and hence do not reflect improvements to either that may have occurred subsequent to the survey period.

In 2009, approximately 24 percent (n=1,044) of respondents indicated that they used some software for AML/CTF compliance purposes. The tools that respondents identified included commercial software packages that are designed to address AML/CTF and other compliance or financial crime risks (eg World-Check, Norkom (0.3%) and Complinet/ Complispace) or more general software (eg Mantas, SAS, Ultradata and Ultracs, Veda, Quicken, MYOB, RIA and Microsoft Excel). Overall, use of individual software packages of either category was very low (less than 1% for most packages identified).

World-Check was the commercial software product most commonly used by respondents (2.7%). The data in Table 17 show that 10.3 percent of the managed funds/superannuation and 12.9 percent securities and derivatives reporting entities used World-Check software, while the proportions of gambling and 'other' sector businesses that used this product were below one percent.

A higher proportion of businesses reported using products developed in-house, or products developed by an industry body than licensed software from a commercial provider. These included in-house developed software (10.2%) and internal Australia Post software (2.8%). Some businesses reported using internet searching or other search functions such as Factiva (0.7%), the AUSTRAC website (0.5%), general internet usage (0.2%); and

a further 0.2 percent used other unspecified electronic procedures. Banking (23.7%) and financial services businesses (19.5%) were the sectors with the highest proportions of respondents developing and using in-house AML/CTF software.

More than 60 percent (n=2,564) of respondents reported not using any AML/CTF software tools in the 12 month period to 30 June 2009 (see Figure 1). These results showed significant differences according to the business sector respondents occupied (χ^2=408.1, df=8, $p \leq 0.0001$). A Cramér's V of 0.32 indicated that there was, however, only a weak level of association between not using AML/CTF software and the business sector respondents occupied. The business sector least likely to report using AML/CTF software was the gambling sector, with almost three-quarters of respondents indicating that they did not use this software (73.7%). This is most likely due to the high proportion of small business clubs and pubs in the sector. By contrast, those in the foreign exchange sector were most likely to use AML/CTF software—only 29.6 percent indicating that they did not use software in the 12 month period to 30 June 2009.

Interviews

Two interview participants from the banking sector reported using software to augment their customer identification and transaction monitoring processes. One banking respondent noted that he used World-Check on a pay-per-use basis, rather than paying an annual licence fee of $10,000 per year. Transactions were also monitored manually using spreadsheets. The interviewee indicated that his bank was examining the feasibility of implementing a larger system to monitor transactions in the future.

One mutual financial services association interviewee reported using Orion, a commercial financial and accounting software product, to monitor Visa transactions and used an Orion add-on to conduct AML/CTF transaction monitoring. Orion software is able to identify suspicious transactions based on the parameters that the user has defined in advance. These parameters are set by the compliance officer and were determined by the nature of the customers and the relevant AUSTRAC AML/CTF risk indicators. The system identified and flagged unusual transactions that should be examined further by the compliance officer (Financial services association representative, personal communication, November 2009).

Know-your-customer processes

KYC requirements—such as customer identification and enhanced due diligence measures, including the identification of beneficial owners of customers—pose various challenges for regulated businesses seeking to implement AML/CTF measures. In Europe,

Table 17 World-Check software users, by business sector

Business sector	Users of World-Check from this sector (n)	Users of World-Check from this sector (%)	% of World-Check users from the sector
Managed funds and superannuation	36	10.3	33.3
Banking	24	7.9	22.2
Financial services	6	3.7	5.5
Securities and derivatives	15	12.9	13.9
Gambling	17	0.8	15.7
Foreign exchange	4	2.0	3.7
Cash delivery services	2	3.5	1.9
Alternative remittance services	3	1.6	2.8
Other	1	0.3	0.9
All sectors	108	2.8	100.0

Note: Percentages may not total 100 due to rounding

Source: AIC AML/CTF Australian businesses survey [computer file]

the majority of the sample of Eastern European financial institutions that responded to Ernst & Young's survey on the implementation of the European Union's Third Anti-Money Laundering Directive, anticipated challenges meeting the Directive's KYC requirements (Ernst & Young 2007). Identifying the economic activities of customers and identifying PEPs were the areas that posed the greatest challenges. In another survey conducted in 2001, more than 60 percent of the MLROs surveyed anticipated difficulties in identifying the beneficial owners of assets (Gill & Taylor 2004).

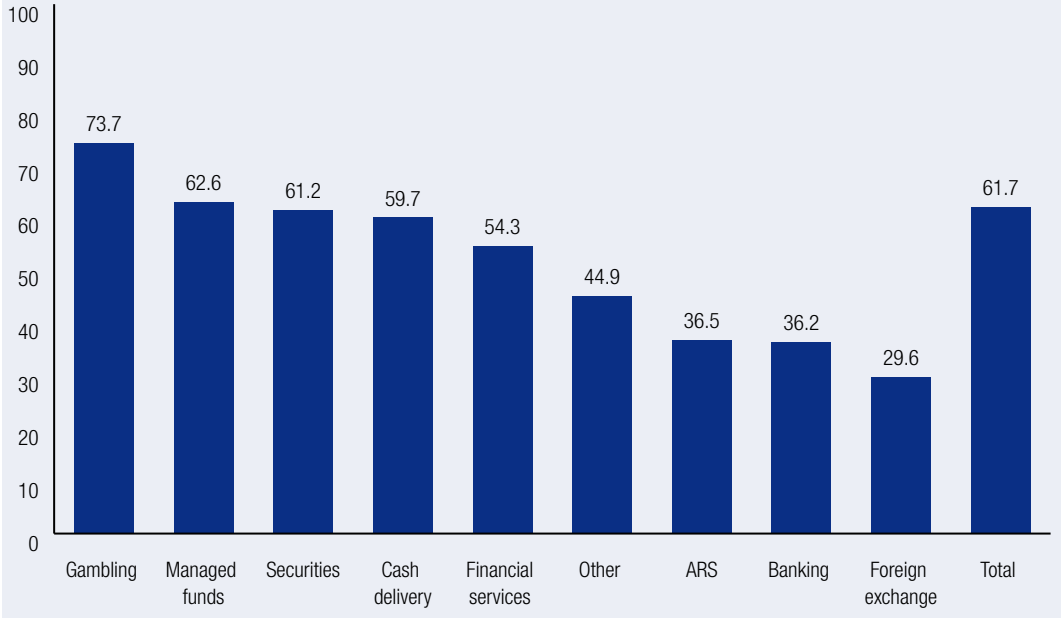
Know-your-customer confidence

Survey respondents were asked to indicate how confident they were in identifying each of the following categories of customers:

- domestic companies;
- registered foreign companies;
- trustees;
- partnerships;
- incorporated and unincorporated associations;
- registered cooperatives;
- domestic government bodies;
- foreign government bodies;
- charities or not-for-profit organisations;
- PEPs; and
- individuals, including sole traders.

Figure 2 presents results combining the percentage of businesses that were *very confident* and *confident*, compared with those that were *neutral* and those that were *not confident* or *not at all confident*, for each customer type. The highest levels of confidence were reported for being able to identify individuals (86.1%) and domestic companies (84.5%). Very few respondents reported not being confident (2.4%) when identifying individuals. The highest levels of lack of confidence in identifying customers concerned the identification of foreign government bodies (24.2%), PEPs (22.4%) and foreign-registered companies (21.4%). The obvious impediments to undertaking appropriate scrutiny of overseas-based organisations and individuals are the likely reasons for the low levels of confidence expressed by respondents when responding to this question.

Figure 1 Regulated businesses that did not use AML/CTF software in 12 month period to 30 June 2009, by business sector (%)



Source: AIC AML/CTF Survey Stata file

Figure 3 shows more detailed information on the confidence different business sectors have in identifying foreign registered companies. Businesses in the foreign exchange (37%) and gambling (26.7%) sectors reported generally little or no confidence in their identification of foreign registered businesses, while those in the securities and managed funds/ superannuation sectors had much higher levels of confidence.

Figure 4 shows levels of confidence reported by businesses from various sectors in identifying PEPs. Respondents from the alternative remittance (15.6%), foreign exchange (15.2%) and 'other' business categories (16.4%) reported having little or no confidence in their ability to identify PEPs. Those from the securities sector showed the highest levels of confidence in identifying PEPs—47.9 percent having some confidence and 22.5 percent being extremely confident in so doing.

Know-your-customer processes

The survey also asked respondents to identify the extent to which their businesses used manual as opposed to software-based processes to conduct customer due diligence, or some blend of the two. Figure 5 shows that 49 percent of the respondents reported using only manual processes and just over one-fifth (22%) used a mix of manual and software-based processes.

These results differed significantly according to the business sector respondents occupied (χ^2=721.6, df=40, $p \leq 0.0001$). A Cramér's V of 0.19 indicated that there was a weak level of association between respondents' use of differing due diligence processes and the business sector they occupied. Those in the gambling sector were most likely to use only manual due diligence processes (61%), while manual processes were least often used by banks (22.9%).

A statistically significant relationship was also present between the type of due diligence processes used and use of AML/CTF software (χ^2=924.9, df=5, $p \leq 0.0001$, Cramér's V=0.47). A number of businesses that reported using AML/CTF software also reported using only manual processes in relation to customer due diligence (n=209, 10.3%), perhaps because software was used principally for transaction reporting rather than due diligence activities.

A proportion of respondents from each of the sectors reported having no customer due diligence procedures in place. Just over 10 percent (10.2%) of gambling sector businesses reported having no customer due diligence procedures in place, while 11.6 percent of 'other' businesses had no such procedures. Nine percent of cash delivery businesses also had no procedures in place.

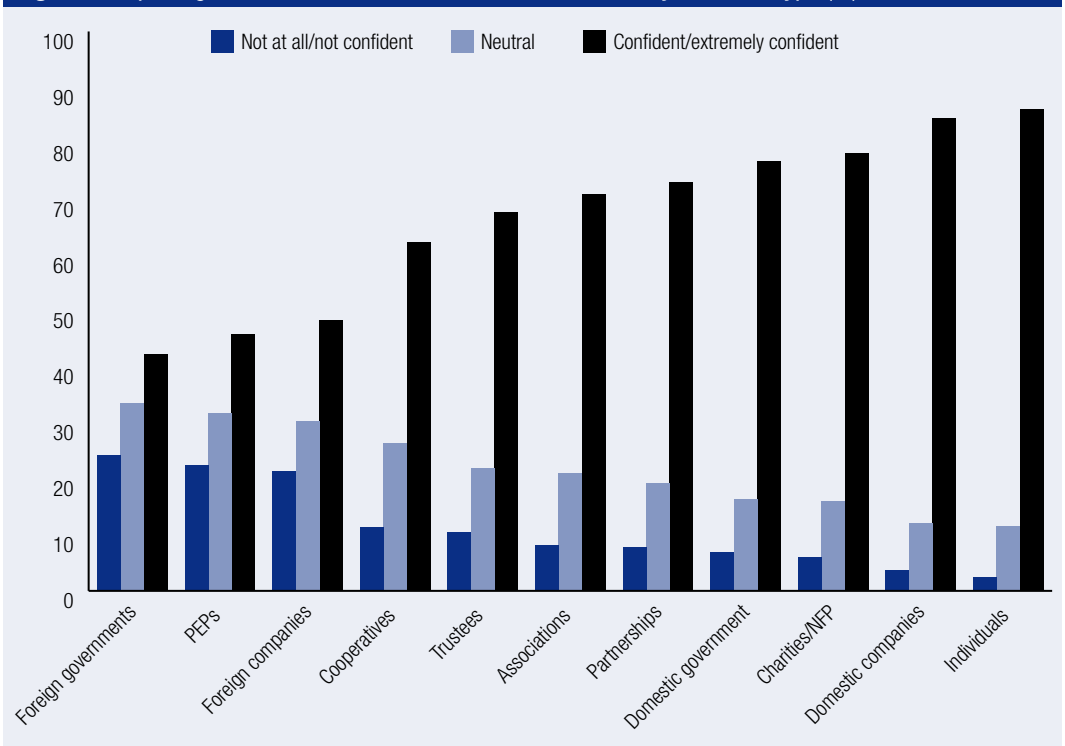
Views of interviewees on customer due diligence

Interview participants confirmed that the way businesses approached customer identification and due diligence was very industry specific. Interviewees from the gambling sector predominantly worked in small businesses that derived most of their income from work as hoteliers, while operating some gaming machines. Interviewees explained that hotels are not obliged to conduct formal identification processes for their customer base who simply purchase drinks or meals over the bar or who unsuccessfully play gaming machines, reflecting the results of the survey that showed that this sector used few formal due diligence processes. One club's representative indicated that the club collected basic information about customers who were not members of the club, although this information was not recorded anywhere other than on the entry form that was completed at the door. Similarly, there were no restrictions on who may become a member or who may be signed in as a guest. That club documented the customer's basic demographic information upon paying out a win of more than $200 and for wins of more than $1,000, the club required patrons to supply two types of government-issued identification before issuing a cheque.

One interviewee from a pub provided an example of the difficulties present in seeking information from customers (see Box 4)

By contrast, an interviewee from a private equity company's current investment fund had a total of 12 investor companies, each of which were already regulated by the Australian Prudential Regulation Authority or the Australian Securities and Investments Commission (ASIC). The company also undertook its own extensive customer due diligence processes that included examination of the investors' reputation

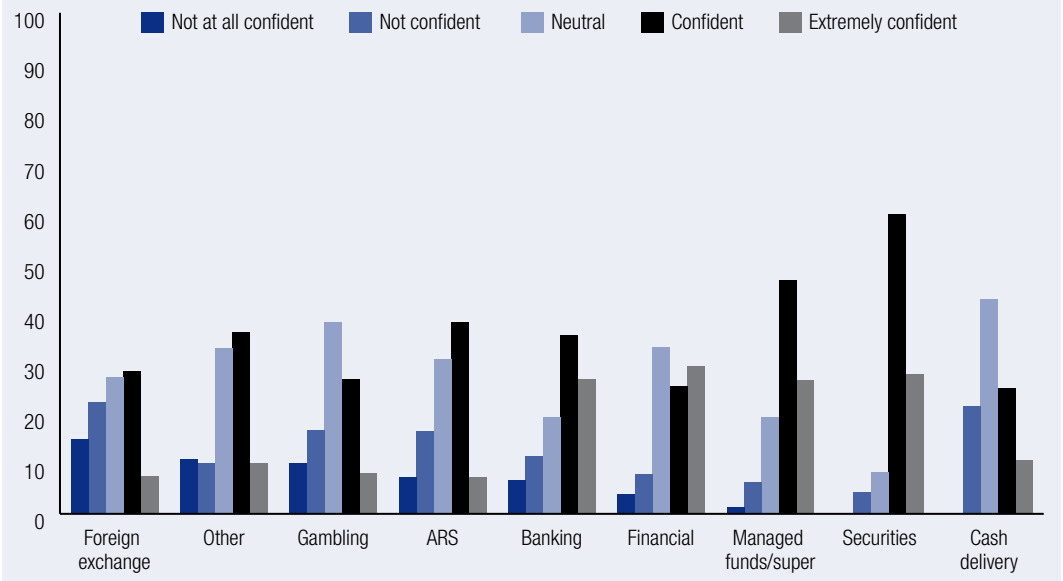
Figure 2 Reporting entities' customer identification confidence, by customer type (%)



Note: NFP= not for profit

Source: AIC AML/CTF Australian businesses survey [computer file]

Figure 3 Confidence in identifying foreign registered companies, by sector (%)



Source: AIC AML/CTF Australian businesses survey [computer file]

and capacity to meet its financial commitments throughout the forthcoming decade.

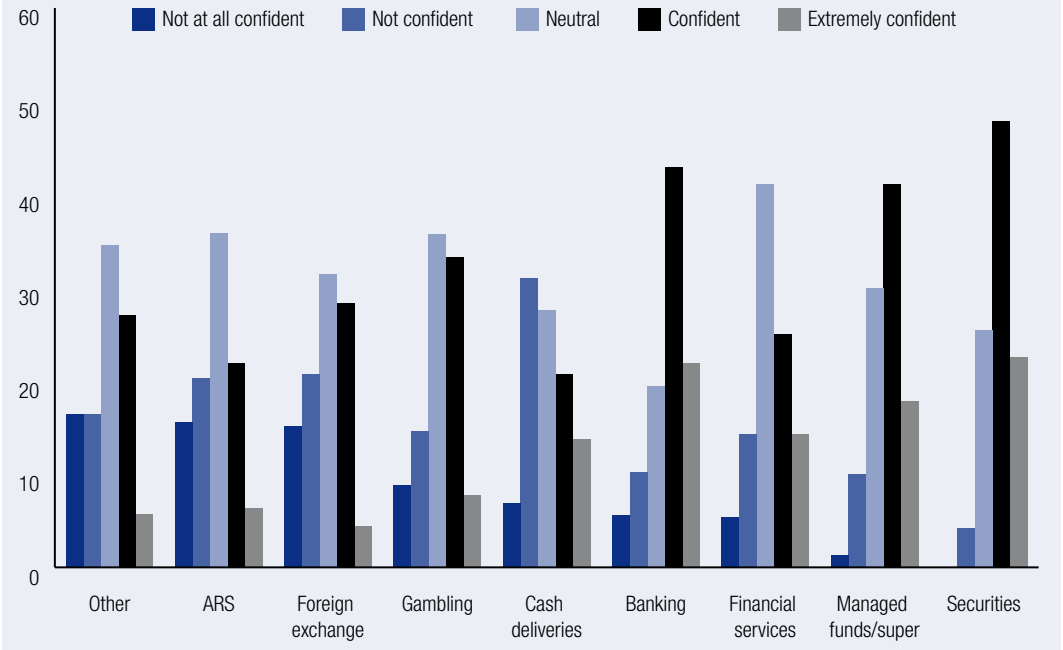
Similarly, an interviewee from a commercial bank indicated that the bank employed a risk matrix that identified a clear hierarchy of management available to staff for advice or assistance. All new corporate clients were subject to a rudimentary check on the ASIC website to verify the identification of the directors and any relevant licences. All potential clients were checked against the Attorney-General's Department and Department of Foreign Affairs and Trade watch lists, and checked against World-Check's database of PEPs.

One interviewee from a cash delivery business indicated that he had always taken a very conservative risk-management approach to accepting new clients. The company did not deal with unknown businesses and conducted stringent assessment of any potential new clients, which encompassed a comprehensive overview of their business practices, the company's reputation, potential lost revenue and questions of personal safety for employees. Any potential clients that failed to take on the risk management recommendations identified in the assessment process were declined. All new clients, and existing clients at the time AML/CTF preventative measures were introduced, were checked against ASIC databases. The business had a lot of face-to-face contact with its clients and required its clients to notify them when a new staff member starts.

Another interviewee who worked with a private mortgage company indicated that he found it difficult to find good borrowers, which made it difficult to invest the funds coming into the business (see Box 5).

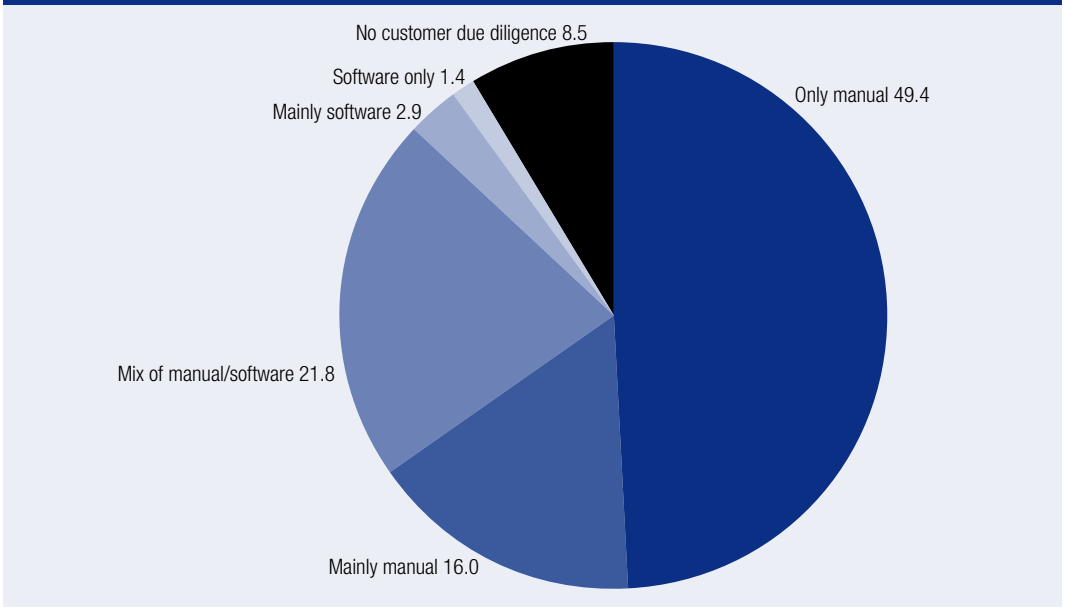
In another instance recounted by a finance company interviewee, a borrower's application for finance for a kebab shop exemplified the enhanced due diligence measures of the lender. The lender had reservations about the loan because of the nature of business and some issues with the proposed guarantors for the loan. The lender investigated the proposal further, had the applicants detail the history of similar businesses they owned and made separate enquiries about the applicants to the broker and lawyer involved in the transaction. The lender obtained a certificate of a witness from the solicitor for the mortgage documents, had the guarantors verify the identity of the borrowers and ensured that the guarantors had received independent advice. All

Figure 4 Confidence in identifying politically exposed persons, by sector (%)



Source: AIC AML/CTF Australian businesses survey [computer file]

Figure 5 Current customer due diligence processes (%)



Source: AIC AML/CTF Australian businesses survey [computer file]

clients were subject to a credit ratings agency check to uncover patterns such as 'clear outs' that might indicate where a person has repeatedly run away from their debt. The reasons for clear outs varied from family case law to something more sinister.

The mortgage company interviewee also noted that new investors providing funds for borrowers could only invest after being referred to the private mortgage company by an existing investor. The company regularly received calls from people seeking to invest funds with their company. They were exceedingly cautious about taking new investors as they found it difficult to invest the funds they already had. The credit manager would meet with a potential new investor to get to know them and would conduct a 100 point identity check at that stage. The investor would then receive a product disclosure statement and the 100 point check would be completed. The company considered it good practice to trial new investors by investing a small amount of money, around $25,000. Most investors disclosed where their funds originated. The mortgage company considered KYC practices important to reduce the risk for their company and to ensure the continuation of positive working relationships.

Confidence in customer due diligence assessments performed by other businesses—survey results

Section 38 of the AML/CTF Act 2006 (Cth) allows reporting entities to rely on customer identification procedures undertaken by another reporting entity carried out in accordance with the legislation and regulations. The aim of this is to reduce the burden on regulated businesses and to streamline the identification procedures required in certain specified circumstances. The Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 No.1 (Part 7.2) restricts reporting entities' use of customer identification conducted by another business to licensed financial advisors and members of designated business groups where:

- the first reporting entity (the entity identifying the customer) makes arrangements for the customer to receive a designated service by a second reporting entity;
- the second reporting entity obtains a record of the identification record made by the first reporting entity or has made arrangements to access the records of the first entity; and

- the second reporting entity has determined it appropriate to rely on the identification undertaken by the first reporting entity, having considered the money laundering and terrorism financing risks posed by providing a designated service to the customer.

Reporting entities that rely on identification procedures completed by another reporting entity, or by an agent, retain their accountability for accurately identifying their customers (AUSTRAC 2010b). Confidence in the customer due diligence procedures conducted by another business, in this context, is a crucial factor in determining whether reporting entities will ever share information in this way.

Respondents to the present survey were asked to indicate their levels of confidence in the customer due diligence assessments conducted by other businesses using the same Likert scale as described previously (ie *not at all confident, not confident, neutral, confident, extremely confident*). Respondents were specifically asked to consider customer due diligence conducted by financial planners, accountants, lawyers and other financial institutions, and were able to nominate other types of businesses. The professional sector businesses were included despite the fact that they did not fall within the legislation. Confidence ratings for the customer due diligence undertaken by each of these four selected business types were condensed into *not at all confident/not confident*, *neutral* and *confident/extremely confident* in order to simplify the results (see Table 18).

Generally, there was a lower level of confidence in customer identification processes undertaken by financial planners as opposed to accountants, lawyers, or other financial institutions. Comparing mean results for responses from respondents concerning confidence in identification undertaken by financial planners and financial institutions, it was found that there was a statistically significant difference between these two groups ($t=-9.1$; $df=2415.2$; $p \leq 0.0001$).

Financial institutions were the only business sector included in this question that had AML/CTF regulatory responsibilities and yet more respondents felt confident or extremely confident in customer identification completed by accountants (76.7%). The confidence rating between accountants and financial institutions was statistically significant ($t=3.2$; $df=3092.4$; $p \leq 0.002$), indicating that more

Box 4 Difficulties in seeking information from customers

The pub had some bikies in a few months ago—they were passing through on their way elsewhere. The group played the pokies and drank without any issues. Those playing the pokies made some sizeable bets and received payouts of $100–200 from the TAB. Their behaviour was not suspicious in any way; anyone making bets of $500 is going to be paid out larger amounts than someone making smaller bets. The hotel staff found it very hard to ask the bikies for identification for the payouts. One of them yelled out his driver's licence number and the staff had to tell him the licence needed to be sighted. It was certainly uncomfortable for the staff member and the publican considered the situation to be possibly dangerous. Telling customers that they need identification information for compliance might be okay for some businesses but is certainly difficult for pokies. The bikies were very obvious and the owner was aware of them constantly. If the bikies had only been in the pub for a short time and gotten large payouts then the owner would have called the police. (Publican, personal communication, October 2009).

Box 5 Difficulties in finding good borrowers

Brokers acted as intermediaries for locating borrowers. The brokers the company worked with were well-known to the credit manager but not to the employees. The company also considered referrals for borrowers from some banks and mortgage brokers. The most common thing clients were seeking was non-confirmative finance. The process for establishing a new borrower was very detailed. Borrowers outlined their scenario and supplied supporting documentation and the mortgage company provided application packs including the Corporation Act, financial services licence, money laundering brochure and identification requirements. The broker then attends to the borrower and returns the information to the mortgage company. The private mortgage company would then send the mortgage document out to the borrower. The borrower was required to sign the documents in front of a justice of the peace, who declared that signatures were witnessed, verified the identity of the borrower and confirmed that they consented to signing the application. A case of mortgage fraud using false identification in the same state compelled the mortgage company to undertake more stringent identity checks. The lenders, in this case, may not have been paid out despite an insurance fund for these situations. The private mortgage company, from then on, maintained a checklist of documentation for every file and all employees had access to these files for monitoring (Mortgage company, personal communication, October 2009).

confidence existed in the processes undertaken by accountants than financial institutions. A higher percentage of respondents also expressed confidence in the due diligence processes of lawyers (73.4%) than other financial institutions (71.1%), although this was not statistically significant (t=2.4; df=3132.1; $p \geq 0.016$). A significant difference was found between levels of confidence in due diligence undertaken by accountants as opposed to lawyers (t=2.421; df=3132.13; $p=0.016$).

The data in Figure 6 show the marked differences that existed across business sectors in respect of their level of confidence in relying on customer due diligence procedures performed by financial planners. Those in the cash delivery services sector had the least confidence in relying on due diligence assessments made by financial planners (18.8%), while respondents from the securities and derivatives sector were generally confident or extremely confident in customer due diligence assessments conducted by financial planners (76.9%).

As is apparent from Figure 7, the banking sector showed the highest proportion (11.5%) of businesses that reported low levels of confidence in relying on the processes conducted by accountants. By contrast, more than 86 percent of financial services sector respondents were confident or extremely confident in the due diligence procedures conducted by accountants.

In relation to levels of confidence in due diligence undertaken by those in the legal sector, Figure 8 shows that the financial services sector respondents had the highest levels of confidence (83.9%), while only 64.5 percent of the banking sector, 60 percent of foreign exchange businesses and 51.1 percent of alternative remittance dealers were confident or extremely confident in replying on due diligence undertaken by lawyers.

Transaction monitoring and reporting

Both the FTR Act and the AML/CTF Act 2006 (Cth) currently require that reporting entities provide a number of financial transaction reports to AUSTRAC. A substantial change in reporting to AUSTRAC took place on 12 December 2008 when the reporting requirements of the AML/CTF Act 2006 (Cth) came into effect. The reporting requirements oblige entities providing one or more 'designated services' under the AML/CTF Act 2006 (Cth) to submit certain reports to AUSTRAC. These include the following (AUSTRAC 2010).

Under the AML/CTF Act 2006 (Cth), reporting entities must submit SMRs if, at any time while dealing with a customer, the entity forms a reasonable suspicion that the matter may be related to an offence (not just a ML/TF offence), tax evasion, or the proceeds of crime. Entities must submit SMRs to AUSTRAC within three days of forming the suspicion (or within 24 hours for matters related to financing of terrorism suspicions). For many reporting entities, SMRs have progressively replaced suspicious transaction reports, which fall under the FTR Act.

Under the AML/CTF Act 2006 (Cth), if a reporting entity provides a designated service to a customer that involves the transfer of physical currency (or e-currency) of $10,000 or more (or the foreign currency equivalent), that entity must submit a TTR to AUSTRAC. For many reporting entities, TTRs have replaced significant cash transaction reports, which fall under the FTR Act. Entities must submit TTRs to AUSTRAC within 10 days of the transaction.

Under the AML/CTF Act 2006 (Cth), if a reporting entity sends or receives an instruction to or from a foreign country to transfer money or property, that entity must submit an international funds transfer instruction (IFTI) report. IFTI reports were also required to be submitted under the FTR Act. Entities must submit IFTIs to AUSTRAC within 10 days of the transfer.

Under the AML/CTF Act 2006 (Cth), cross-border movement of physical currency (CBM-PC) reports are submitted when currency (coin or paper money) worth $10,000 (or the foreign equivalent) or more is carried, mailed or shipped into or out of Australia. When a person carries currency of $10,000 or more into or out of Australia, a CBM-PC report must be completed at the first customs examination area upon entry into Australia or before leaving Australia. When a person mails or ships currency of $10,000 or more into or out of Australia, a CBM-PC report must be submitted within five business days of the currency being received in Australia or at any time

before the currency is sent out of Australia. On 12 December 2006, CBM-PC reports replaced international currency transfer reports, which fall under the FTR Act.

Under the AML/CTF Act 2006 (Cth), cross-border movement of bearer negotiable instrument reports must be completed by persons entering or leaving Australia who are carrying bearer negotiable instruments (such as travellers cheques, cheques or money orders) of any amount, if asked by a customs or police officer to complete such a report. This aspect of the reporting regime is examined by Smith and Walker (2010).

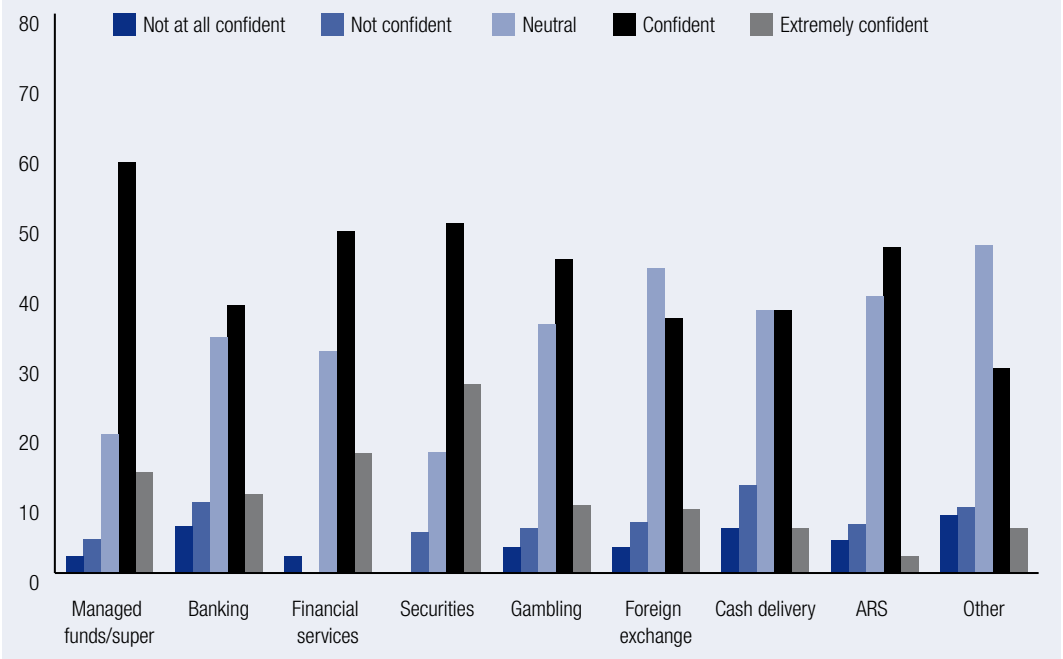
Finally, a reporting entity must give an annual report to AUSTRAC regarding its compliance with the AML/CTF Act 2006 (Cth) (ss 47–48). The first such report was due on 31 March 2008. The AML/CTF compliance report obligations apply to any person or entity that provides designated services. Reporting entities were encouraged to enrol via AUSTRAC Online, an internet-based information portal for reporting entities launched in December 2007. AUSTRAC Online streamlined the enrolment process for new entities and provided a simple and efficient means for entities to submit their compliance reports. By the end of the reporting year, more than 10,000 entities had enrolled via AUSTRAC Online

Table 18 Respondents' confidence in know-your-customer procedures undertaken by another business (%)

	Confidence rating		
Sector performing KYC	Not at all/not confident	Neutral	Confident/extremely confident
Financial planners	10.8	33.3	55.9
Accountants	5.0	18.3	76.7
Lawyers	5.6	21.0	73.4
Other financial institutions	5.5	23.4	71.1

Source: AIC AML/CTF Australian businesses survey [computer file]

Figure 6 Confidence in relying on customer due diligence conducted by financial planners, by sector (%)



Source: AIC AML/CTF Australian businesses survey [computer file]

and approximately 7,500 AML/CTF compliance reports had been submitted (AUSTRAC 2008). At 30 June 2011, a total of 18,484 entities were enrolled with AUSTRAC Online (AUSTRAC 2011).

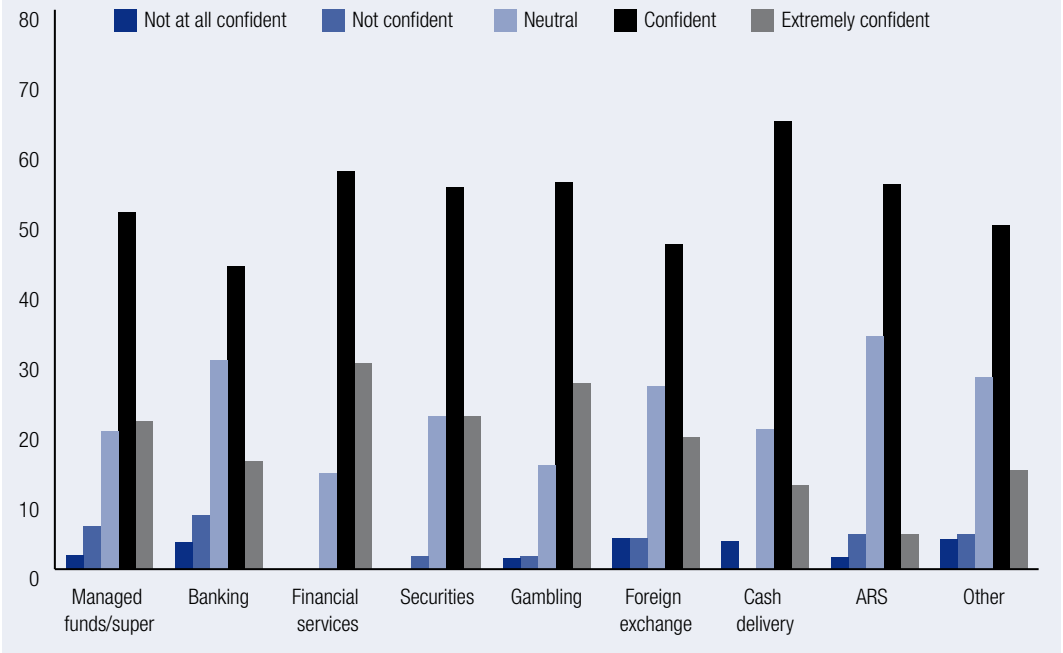
In Australia, the pattern of suspicious transaction/matter reporting to AUSTRAC has been one of general increase between 1994–95 and 2010–11, although these increases were more pronounced from 2003–04 onwards. A substantial increase between 2008–09 and 2009–10 was followed by a slight reduction in 2010–11 (see Figure 9).

The increased number of reports submitted to AUSTRAC is unlikely to be the direct result of an increase in the number of suspicious transactions performed by designated entities on behalf of their customers. Instead, it is likely to be attributed to the tightening of the AML/CTF regime (in the wake of the 11 September 2001 and other terrorist attacks), a legislative-driven increase in the number of reporting entities, an increase in the size of some regulated sectors, increased publicity by AUSTRAC of the requirements of the regime and a period of defensive reporting influenced by the securing of convictions against high profile financial institutions in the United States and the United Kingdom for failing to adequately maintain AML/CTF compliance systems (Smith et al. forthcoming).

Perceptions of the effectiveness of transaction monitoring—survey results

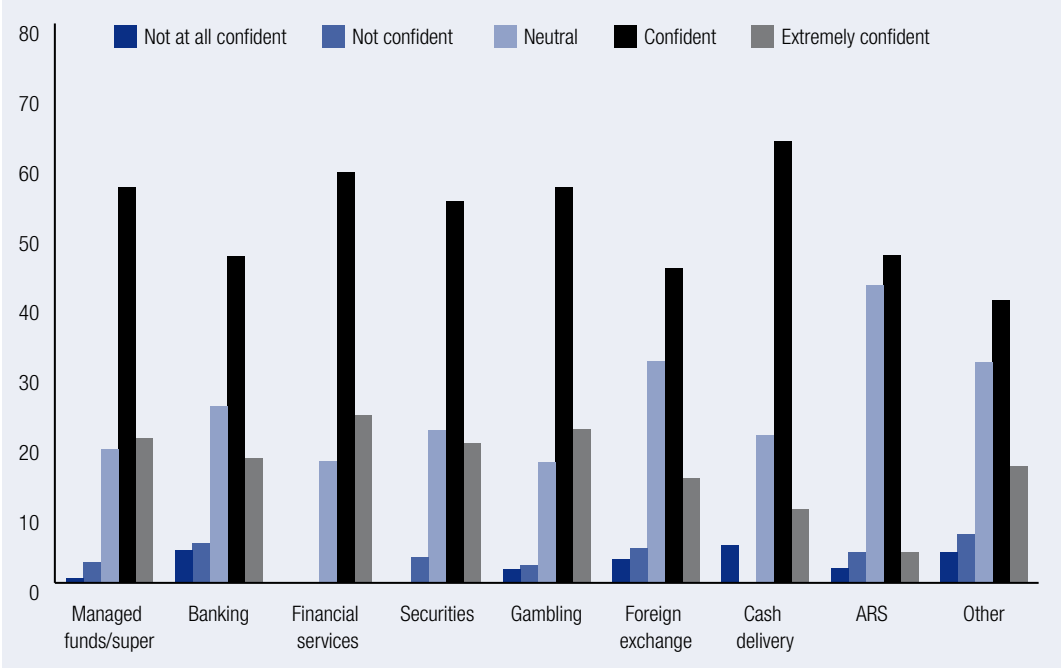
The AML/CTF regime requires reporting entities to monitor transactions of customers in order to identify both threshold transactions as well as suspicious matters and have regard to complex, unusual large transactions and unusual patterns of transactions, which have no apparent economic or visible lawful purpose (Chapter 15, AML/CTF Rules Instrument 2007 (No 1)). The survey sought the views of participants on the ability of their business to monitor transactions, the methods used to monitor transactions and the procedures likely to be the most effective in monitoring transactions. Respondents were specifically asked to indicate their views on the extent to which their business was effective in identifying each of a variety of types of financial transaction. Respondents were also asked to indicate their perceptions of the effectiveness of

Figure 7 Confidence in relying on customer due diligence conducted by accountants, by sector (%)



Source: AIC AML/CTF Australian businesses survey [computer file]

Figure 8 Confidence in relying on customer due diligence conducted by lawyers, by sector (%)



Source: AIC AML/CTF Australian businesses survey [computer file]

transaction monitoring in terms of identifying cash transactions equal to or more than $10,000, suspicious transactions of less than $10,000, suspicious transactions of more than $10,000, transactions involving PEPs and suspicious transactions to overseas countries. The perceptions of respondents on the effectiveness of transaction monitoring for each of these transaction types are presented in Figure 10.

Almost 95 percent of respondents considered their transaction monitoring procedures to be effective, or very effective, at identifying cash transactions of $10,000 or more. Smaller proportions of respondents considered their procedures to be very effective, or effective, at identifying transactions involving PEPs (51.2%) or at identifying suspicious transactions made to overseas countries (77.4%).

Comparing mean results for responses concerning the effectiveness of identifying transactions involving PEPs and suspicious transactions to other countries, it was found that there was a statistically significant difference between these two groups (t=-12.3; df=3429.5; $p \leq 0.0001$); that is, respondents viewed their ability to identify transactions involving PEPs as being significantly less effective than their ability to identify suspicious transactions to other countries. The foreign exchange sector was the sector that believed it was least effective in identifying transactions involving PEPs (19.1% believing processes to be either ineffective or very ineffective).

Respondents also differed significantly in terms of their perceived effectiveness in identifying suspicious transactions of less than $10,000 as opposed to those of more than $10,000 (t=-11.2; df=6077.3; $p \leq 0.0001$). Overall, respondents were less confident in their ability to identify suspicious transactions of less than $10,000 than suspicious transactions of more than $10,000.

Automated transaction monitoring

Respondents were also asked to indicate whether their transaction monitoring activities were manual, using some automated software-based system, a mixture of both, or whether no monitoring was undertaken. The data in Figure 11 show that more than half (58.2%) of respondents reported using only manual, or mainly manual, transaction monitoring

processes in their businesses. A small percentage of businesses (7.8%) reported using predominantly software-based transaction monitoring processes.

Table 19 presents statistics on the transaction monitoring processes used by respondents according to their business sector. It was found that transaction monitoring software was most often used in the foreign exchange sector (23.4%) with those in the gambling (67.9%) and securities and derivatives sectors (68.1%) most often using manual processes for transaction monitoring. Almost six percent (5.7%) of respondents, mostly from the gambling sector, indicated that they used no transaction monitoring processes. This accords with the results presented in Figure 1 that showed that respondents from the gambling sector were the least likely to use AML/CTF software generally.

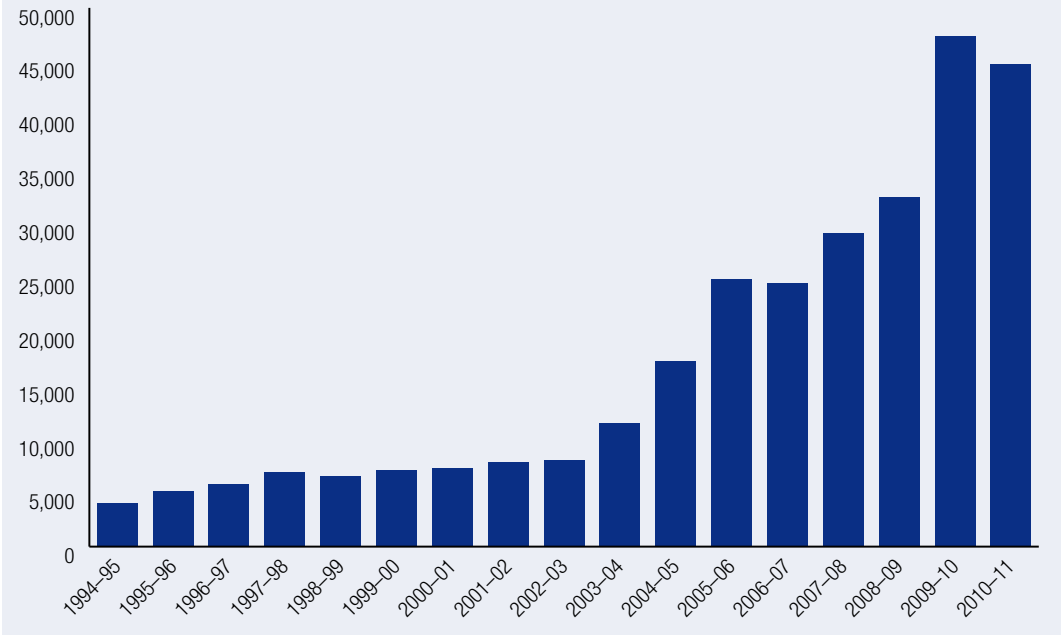
Perceptions of the effectiveness of transaction monitoring procedures

An attempt was also made in the survey to gauge perceptions about the effectiveness of various types of transaction monitoring procedures. Grouping the responses into three categories of *very effective/effective*, *neutral* and *very ineffective/ineffective*, Figure 12 presents the assessments for five types of transaction monitoring methods—anti-money laundering software, external third parties (such as consultants), external audit, internal audit and internal staff-based methods.

It was found that the majority of respondents (92.9%) indicated that using internal staff to identify transactions was an effective or very effective method of transaction monitoring. Internal auditing was also considered to be effective or very effective for 85.3 percent of respondents. Somewhat fewer respondents (77%) indicated that using external third parties, or using external audit (78%), to identify transactions were effective or very effective methods of transaction monitoring. The effectiveness ratings shown in Figure 12 also indicated that just over one half of respondents (58.1%) perceived that AML/CTF software was an effective or very effective means of monitoring transactions.

Respondents from the banking (82.2%), securities and derivatives (84%), and alternative remittance services (80%) sectors were most likely to view transaction monitoring using AML/CTF software as effective or very effective. Fewer respondents (38.4%) from the gambling sector, by contrast,

Figure 9 Suspicious transaction/matter reports received by AUSTRAC, 1994–95 to 2010–11 (n)



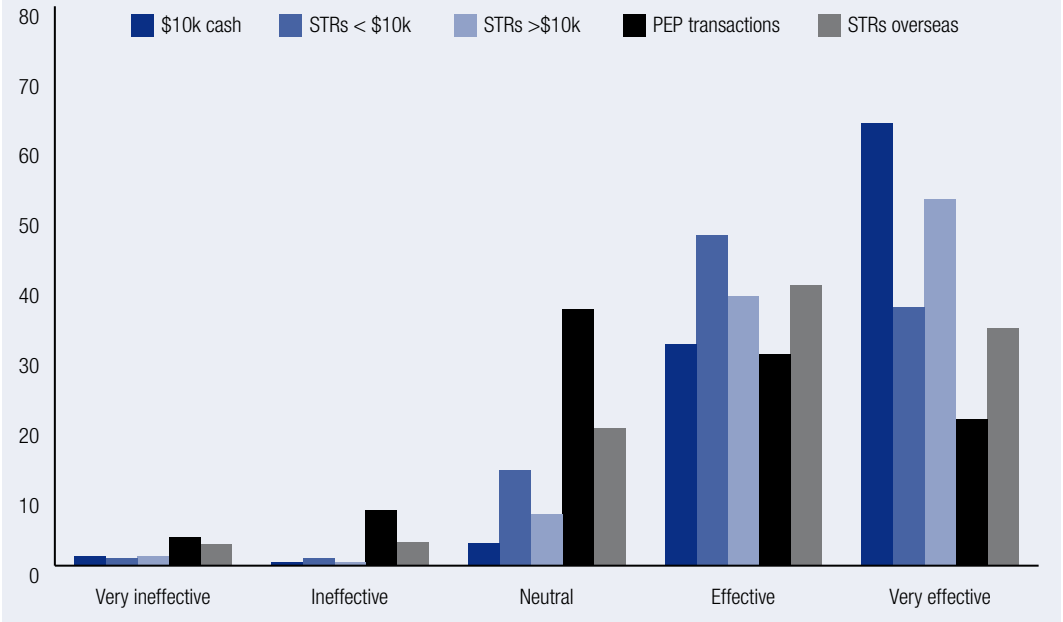
Sources: AUSTRAC annual reports 1994–95 to 2010–11

viewed AML/CTF software as effective or very effective. Those from the gambling sector were also most likely to say that they did not use any AML/CTF software for any aspect of compliance. There is no indication, however, of whether gambling businesses did not use AML/CTF software because of its perceived ineffectiveness, or simply if the perception of ineffectiveness stems from a lack of exposure to using software. It could also be the case that respondents from the gambling sector considered that AML/CTF software was too expensive or not well-suited to the compliance needs of the sector.

Responses of interviewees

Interviewees were asked to provide information on the procedures they used that were relevant to the identification of suspicious transactions undertaken by their customers. Many of these procedures were used for credit control and fraud reduction reasons, rather than specifically for anti-money laundering purposes, although they were also of benefit in detecting suspicious transactions for AML/CTF purposes as well. One interviewee from a pub, for example, explained that the pub had TAB facilities as well as gaming machines and that the TAB monitored the bets placed in the pub. The TAB set a betting threshold of $200, beyond which the pub owners needed to place the bet with the TAB. The TAB would contact the pub to get some identification information of the punters on any bets they had questions about. One of the pub's regular customers frequently placed large bets at the pub and the pub's owners knew that the man supported himself through gambling. This punter placed a bet of $1,000 and the TAB called to verify it when he placed it and again the day after. The owner witnessed one customer winning $10,000 within the first three months that the owner had been in the pub; another won $1,800 during the same period. Each of these winners had their details recorded prior to receiving their winnings, although the owners knew them quite well and saw them often. The pub had procedures for placing large bets so that the staff could do so and the system worked well for the TAB facilities. The owners had no idea of what amounts of cash were going into the pokies by a single user though, as each machine gave a figure

Figure 10 Perceptions of the effectiveness of transaction monitoring for different types of transactions (%)

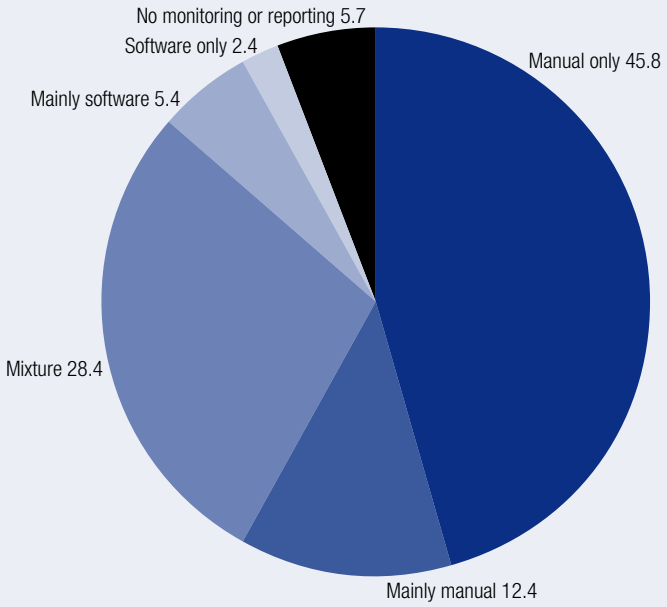


Source: AIC AML/CTF Australian businesses survey [computer file]

at the end of the day but did not log the amounts placed by each user or in a single session. Lots of big punters played the pokies and tended to favour some machines; the pub owners could usually tell who had been using a machine upon clearing it out at the end of the day.

Another interviewee who worked with a cash delivery company indicated that all cash pickups came with a receipt indicating the amount of money that a machine should be holding. Any pickups that approached $10,000, or cumulatively reached $10,000, were recorded in a spreadsheet. The risk-management system involved a recording system for all guards in the field to document everything and this information was recorded in the office. All of the company's staff, including the

Figure 11 Manual and automated transaction monitoring processes across business sectors (%)



Note: Percentages may not total 100 due to rounding

Source: AIC AML/CTF Australian businesses survey [computer file]

Table 19 Each business sector using manual, software-based, or mixed transaction monitoring processes (%)

Business sector	Only/mainly manual	Only/mainly software	Mixture	No monitoring
Foreign exchange	32.0	23.4	42.3	2.0
Banking	35.2	11.6	50.5	2.7
Alternative remittance services	49.5	14.4	33.0	3.2
Financial services	52.4	8.5	37.2	1.8
Cash delivery services	54.4	7.0	33.3	5.2
Managed funds/superannuation	54.8	6.1	37.0	2.0
Gambling	67.9	3.5	21.4	7.2
Securities and derivatives	68.1	2.7	25.7	3.5
Other	42.1	21.1	30.2	6.5

Source: AIC AML/CTF Australian businesses survey [computer file]

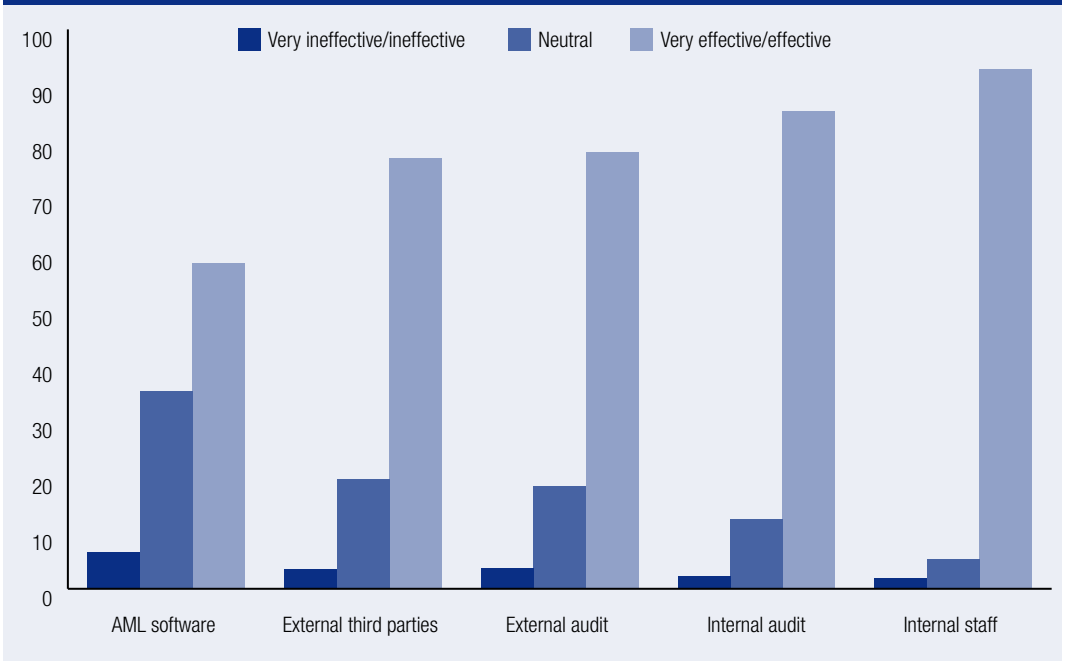
guards and office staff dealing with the cash once it had been collected, were trained in AML/CTF reporting requirements. All of the guards were aware of the cash transaction reporting requirements and the office employees were aware of all of the reporting requirements as well. The company conducted an AML/CTF component within its induction process for new staff and held a monthly meeting intended for staff to ask questions and identify further training needs.

Identifying suspicious transactions—survey results

Respondents were asked to indicate whether their business 'had identified any suspect transactions over the 12 month period ending 30 June 2009' (ie the 2008–09 financial year). The question asked about 'suspect transactions' which was the terminology used at the time, rather than the term used in the current legislation, 'suspicious matters'. There is a possibility that some respondents might not have provided a positive response to these questions where they were unable to identify a suspect transaction as relating either to money laundering or financing of terrorism, where the distinction between the two categories was unclear. However, because so few transactions concerned financing of terrorism, this problem is likely to have minimal impact.

A total of 181 respondents indicated that their business had identified a suspected money laundering transaction. At least five businesses from each business sector identified at least one transaction suspected of being linked to money laundering. More than 80 percent of the businesses that reported identifying suspect transactions

Figure 12 Perceptions of the effectiveness of transaction monitoring procedures (%)



Source: AIC AML/CTF Australian businesses survey [computer file]

identified 10 transactions or less. The low numbers of suspicious transactions that businesses in the AML/CTF Australian businesses survey identified are consistent with the reported numbers of suspect transactions in other surveys. Ninety percent of regulated businesses surveyed in the United Kingdom in 2007 reported 100 suspicious transactions or less in a year (PricewaterhouseCoopers 2007). The largest proportion of the group (58%) reported six or less transactions per year, compared with one percent of the sample that reported 500 transactions or more. The Indian financial services businesses surveyed by KPMG in 2009 showed a similar pattern, with 56 percent of respondents filing less than five reports and 12 percent reporting more than 20 transactions in a year (KPMG (India) 2009).

Figure 13 shows the percentage of suspect transactions that were reported by entities in varying sectors grouped according to five categories of volume—10 or less suspect transactions, 50 or less, 100 or less, 500 or less, or more than 500 suspect transactions. For example, 100 percent of respondents that reported over 500 suspect transactions in the year to 30 June 2009 came from the banking sector (1 bank). However, only 22 percent of entities that reported 10 or less suspect transactions came from the banking sector. Businesses within the banking sector identified 33 percent of all of the transactions suspected of involving money laundering reported in the survey.

Thirteen survey respondents identified a transaction suspected of involving the financing of terrorism in the same period. At least one business from each sector identified at least one transaction it suspected of being linked to the financing of terrorism. The banking sector was also the reporting sector that identified the largest volume of transactions that were thought to involve the financing of terrorism. The number of suspected terrorism financing transactions was, however, much smaller at only four.

Under- and over-reporting

The present study sought the views of participants on under- and over-reporting of suspicious matters by seeking their responses to a series of statements suggesting situations in which under- or over-reporting might occur.

Under-reporting—survey results

Survey respondents were asked if they *agreed*, *strongly agreed*, *disagreed*, or *strongly disagreed* that failing to report a suspicious transaction to AUSTRAC was justifiable in situations where:

- reporting was not required by law;
- they perceived reporting to be of no use;
- reporting would result in lost business;
- reporting would alienate customers; and
- there was a fear of reprisals.

Accordingly, if respondents agreed with these statements, it was considered likely that they would fail to report matters to AUSTRAC that could potentially have involved money laundering or financing of terrorism.

The results presented in Figure 14 were grouped into three categories relating to general agreement with the statements, neutrality, or disagreement. It was found that almost 80 percent of respondents disagreed, or strongly disagreed that failing to report was justifiable where reporting might result in a loss of business (79.8%) or alienate customers (78.5%). A third of respondents agreed or strongly agreed that failing to report a suspicious transaction was justifiable where reporting was not required by law and 13.3 percent of respondents agreed that failure to report was justifiable where reporting was perceived to be of no use.

The results relating to the statement ‘under-reporting is justifiable when it is not required by law’ were significantly different according to the business sector respondents occupied (χ^2=40.4, df=16, $p \leq 0.001$). A Cramér’s V of 0.07 indicated that there was a weak level of association between respondents’ views regarding the justifiability of non-reporting ‘when not required by law’ and the business sector they occupied. Similarly, the results relating to the statement ‘under-reporting is justifiable when it is of no use’ were significantly different according to the business sector respondents occupied (χ^2=68.1, df=16, $p \leq 0.0001$). A Cramér’s V of 0.10 indicated that there was a weak level of association between respondents’ views regarding the justifiability of non-reporting ‘when it is of no use’ and the business sector they occupied.

The data presented in Figure 15 show that the banking, cash delivery services and financial services sectors were most likely to disagree with the statement that failing to report 'when it is not required by law' was justifiable. Businesses from the securities and derivatives sector were most likely to agree that failing to report in these circumstances was justifiable.

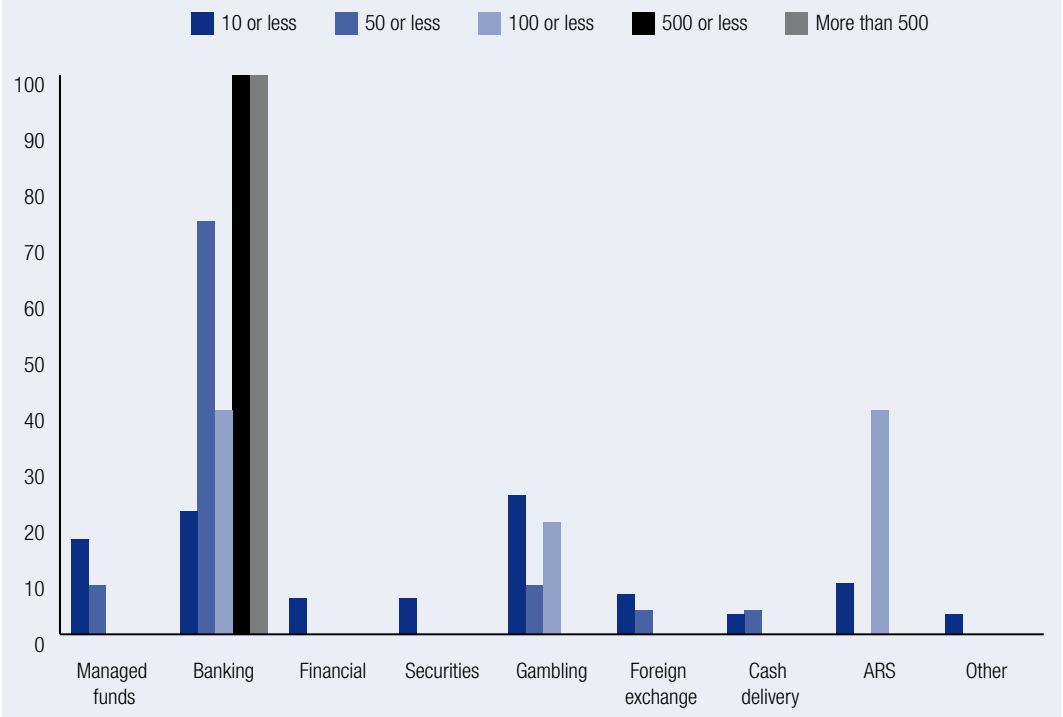
The banking, managed funds/superannuation and financial services sectors were also most likely to disagree or strongly disagree that failing to report a transaction in circumstances in which reporting 'would be of no use' is justifiable, as the data in Figure 16 show. Those in the gambling sector were most likely to agree that failure to report in these circumstances would be justifiable.

The results were also analysed in terms of the type of transaction monitoring procedures that respondents used—namely, manual, through the use of software, a mixture of both, or none. Statistically significant relationships were found between the transaction monitoring procedures businesses used and their views on under-reporting suspicious transactions. Figure 17 presents the results for the statement that failure to report is justifiable when reporting is not required by law.

These results were significantly different according to the business sector respondents occupied (χ^2=41.5, df=10, $p \leq 0.0001$). A Cramér's V of 0.07 indicated that there was a weak level of association between the views of respondents concerning the justifiability of reporting when not required to do so by law and the transaction monitoring procedures they used. Businesses without any monitoring procedures were more likely than other businesses to agree that electing not to report suspicious transactions when required to do so by law was justifiable.

A statistically significant, but weak relationship was also found between the way in which businesses monitored transactions and their views on failing to report when reporting was perceived to be useless (χ^2=32.6, df=10, $p \leq 0.001$; Cramér's V=0.07). Businesses without any transaction monitoring processes were most likely to agree that failing to

Figure 13 Suspect transactions reported in the year to 30 June 2009, by business sector and volume reported (%)



Source: AIC AML/CTF Australian businesses survey [computer file]

report if the business considered that doing so would be useless was justifiable (53.2%). Businesses with a mixture of automated and manual monitoring procedures were most likely to disagree or strongly disagree with this statement (74.6%). Figure 18 shows respondents' views as to the justifiability of failing to report where reporting was perceived to be of no use, according to the transaction monitoring procedures which are used.

A statistically significant, but weak, relationship was also found between views concerning the justifiability of failing to report where this could alienate customers and the type of transaction monitoring procedures used (χ^2=46.6, df=10, $p \leq 0.001$, Cramér's V=0.08). Respondents without any transaction monitoring procedures were more likely than other businesses to agree or strongly agree that not reporting in these circumstances was justifiable.

Over-reporting—survey results

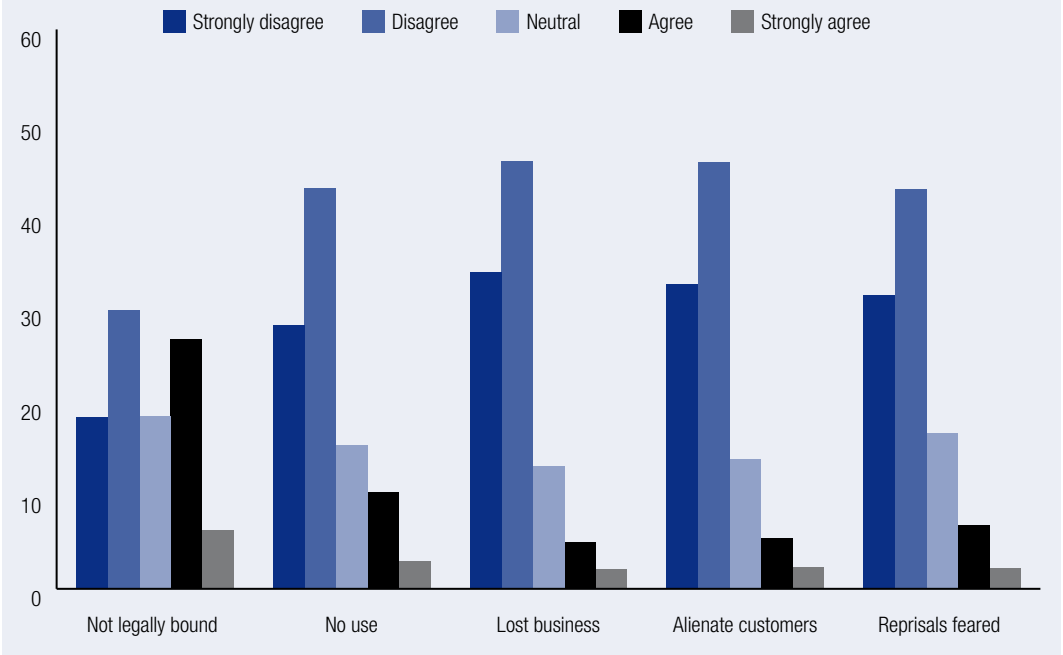
With respect to attitudes towards over-reporting of suspicious transactions, respondents were asked to indicate whether they believed reporting more suspicious transactions to AUSTRAC than strictly necessary was justifiable in the following circumstances:

- when the business was not sure what the transaction involved ('unsure of transaction');
- when there was heightened staff awareness/ understanding of AML issues ('staff awareness');
- when electronic/automated transaction monitoring made reporting easy ('electronic monitoring');
- to avoid the imposition of penalties for failing to comply ('avoid penalties'); and
- to ensure the business' level of reporting was comparable with that of other businesses in the same sector ('report volumes').

The views of respondents on over-reporting in these circumstances are shown in Figure 19, with results grouped in three categories of general agreement, neutrality and general disagreement.

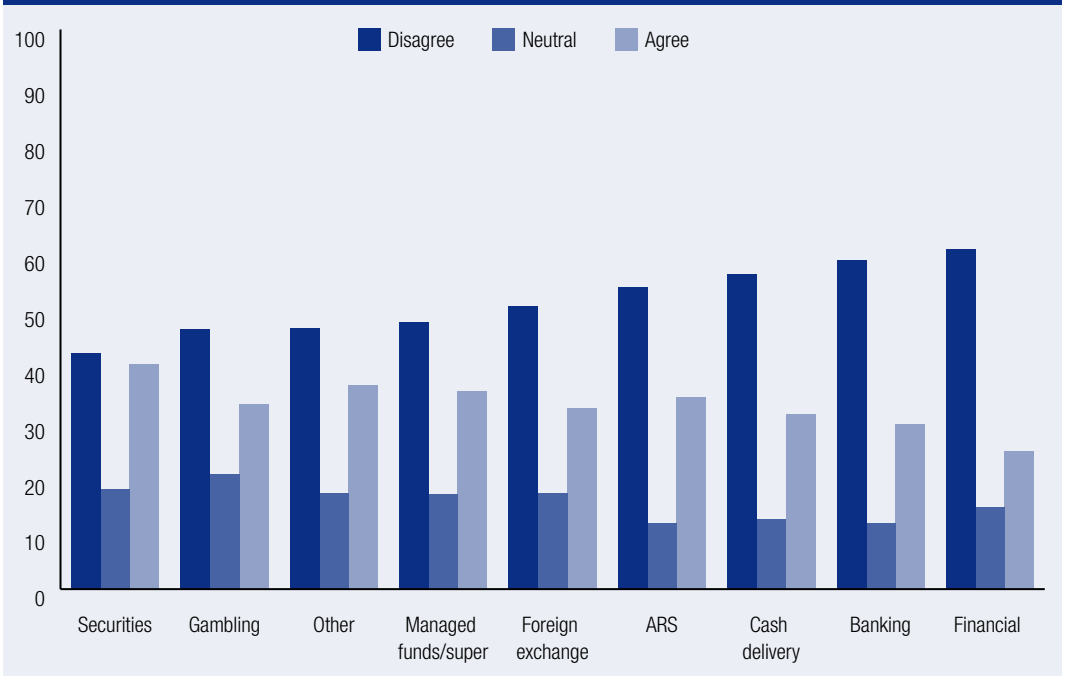
A majority of respondents agreed or strongly agreed (70.4%) that over-reporting was justifiable where the business was unsure of what a transaction involved. A total of 58.3 percent of businesses also agreed or strongly agreed that over-reporting in order to avoid penalties for non-compliance was justifiable and

Figure 14 Justifications for failing to report suspicious transactions



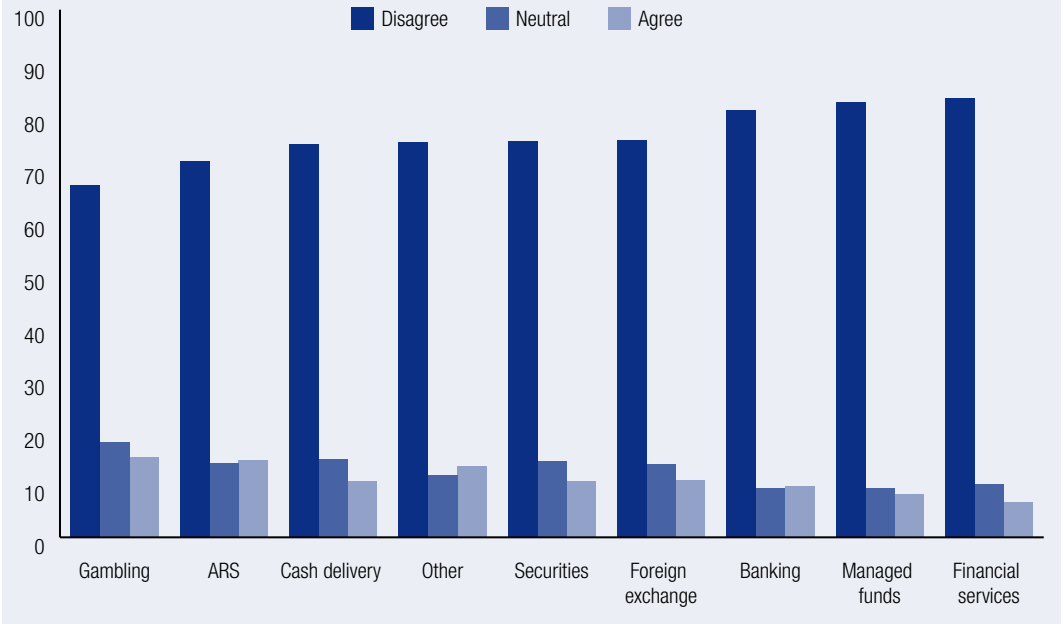
Source: AIC AML/CTF Australian businesses survey [computer file]

Figure 15 Justifiability of failing to report a suspicious transaction when it is not mandatory, by business sector (%)



Source: AIC AML/CTF Australian businesses survey [computer file]

Figure 16 Justifiability of failing to report a suspicious transaction when reporting is perceived to be of no use, by business sector (%)



Source: AIC AML/CTF Australian businesses survey [computer file]

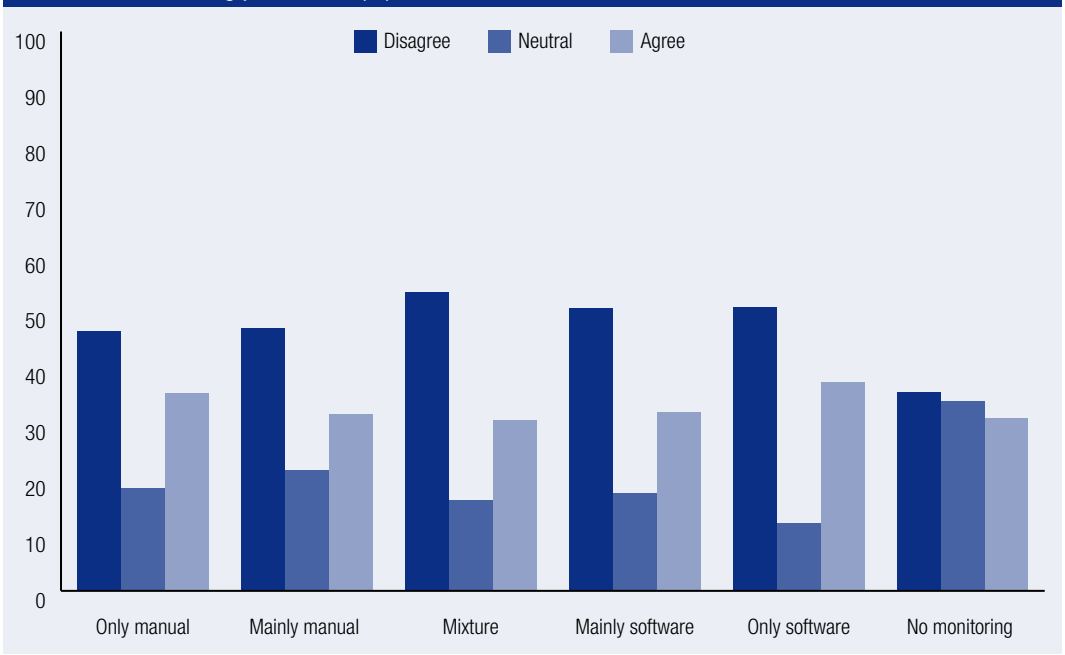
46 percent agreed or strongly agreed that it was justifiable to ensure that the business' level of reporting was comparable with that of other businesses in the same sector.

The results concerning over-reporting in circumstances in which the business was unsure of the nature of the transaction were significantly associated with the business sector from which respondents came (χ^2=42.6, df=16, $p\leq$0.0001). A Cramér's V of 0.08 indicated that there was a weak level of association between respondents' views as to over-reporting in these circumstances and the business sector they occupied. Businesses classified as 'other' (78.2%), those from the managed funds and superannuation sector (74.3%), and the foreign exchange sector (73.6%) were most likely to agree or strongly agree that over-reporting was justifiable in these circumstances. Those from the securities and derivatives (62.1%) and cash delivery services (59.1%) sectors were least likely to agree that this was justifiable.

The business sector of the respondent was also significantly associated with their response to over-reporting to avoid penalties for non-compliance (χ^2=57.64 df=32, $p\leq$0.004, Cramér's V=0.07). Businesses from the banking and cash delivery sectors were the least likely to consider that over-reporting would be justifiable in order to avoid fines for non-compliance, while businesses classified as 'other' were the most likely to agree that over-reporting in these circumstances would be justifiable.

Banking businesses were also the least likely to agree that over-reporting would be justifiable in order to ensure that the bank's level of reporting would be comparable with that of other banks. Those from the foreign exchange and cash delivery sectors were most likely to agree that over-reporting in these circumstances would be justifiable. A statistically significant relationship was found between the business sector respondents occupied and their view on over-reporting in order to ensure that their level of reporting would be comparable with that of comparable businesses in the same sector (χ^2=102.3, df=16, $p\leq$0.0001). A Cramér's V of 0.13 indicated that there was a weak level of association between these views and the business sector they occupied.

Figure 17 Justifiability of failing to report a suspicious transaction when it is not mandatory, by transaction monitoring procedures (%)



Source: AIC AML/CTF Australian businesses survey [computer file]

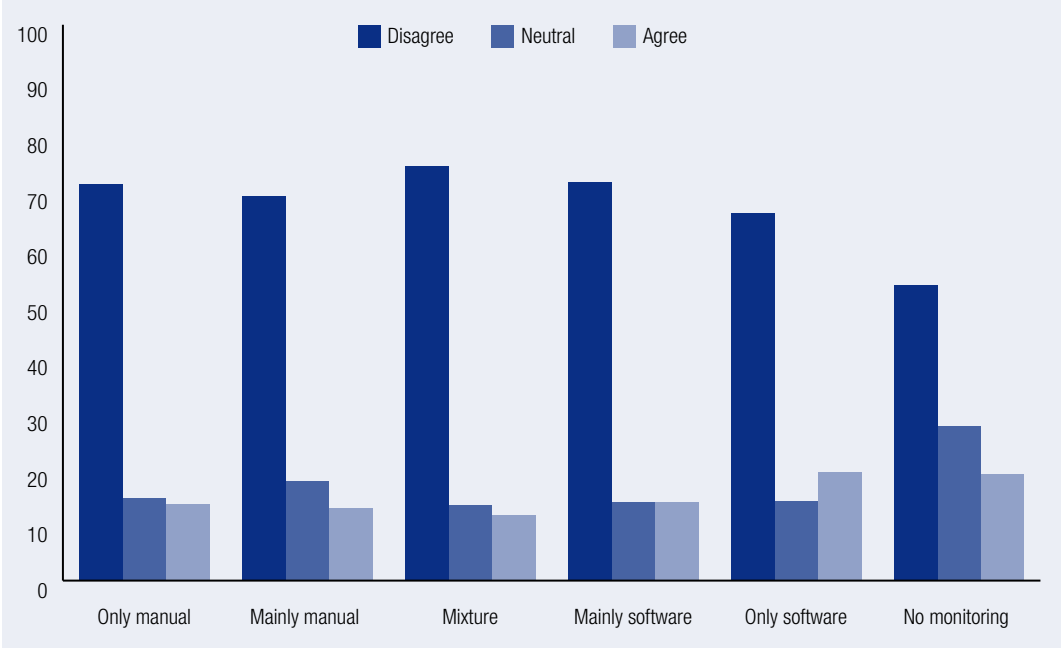
Statistically significant, but weak relationships were also found between business sector and views as to the justifiability of over-reporting where automated transaction monitoring makes reporting easier (χ^2=149.8 df=16, p≤0.0001, Cramér's V=0.16) and as a consequence of heightened staff awareness (χ^2=68.8 df=16, p≤0.0001, Cramér's V=0.10). Businesses that provided foreign exchange services were the most likely to agree that over-reporting would be justifiable where automated transaction monitoring made reporting easy, while banking sector businesses were the least likely to agree with this statement. Alternative remittance businesses were the most likely to consider that over-reporting was justifiable because of heightened staff awareness.

An analysis was also undertaken of the views of respondents as to over-reporting and their use of AML/CTF software. Statistically significant, but weak, relationships were found between the use of AML/CTF software and responses:

- to over reporting in order to avoid penalties for non-compliance (χ^2=20.7 df=4, p≤0.0001, Cramér's V=0.08);
- to ensure comparable reporting numbers (χ^2=32.7 df=2, p≤0.001, Cramér's V=0.10);
- when staff have a heightened awareness (χ^2=8.6 df=2, p≤0.013, Cramér's V=0.05); and
- where software makes reporting easy (χ^2=38.5 df=2, p≤0.0001, Cramér's V=0.1).

Businesses that used AML/CTF software were less likely than those businesses without AML/CTF software to agree or strongly agree that over-reporting would be justifiable in order to avoid penalties, to ensure comparable reporting numbers with other businesses in the same sector, or because of heightened staff awareness. Businesses with AML/CTF software (28.7%) were more likely than businesses without software (19.8%) to disagree or strongly disagree that over-reporting would be justifiable where software made it easy to report. It seems, therefore, that there are a number of circumstances in which businesses from certain sectors would be willing to engage in both under-reporting and over-reporting of suspicious transactions to AUSTRAC, based largely on commercial reasons.

Figure 18 Justifiability of failing to report a suspicious transaction when reporting is perceived to be of no use, by transaction monitoring procedures (%)



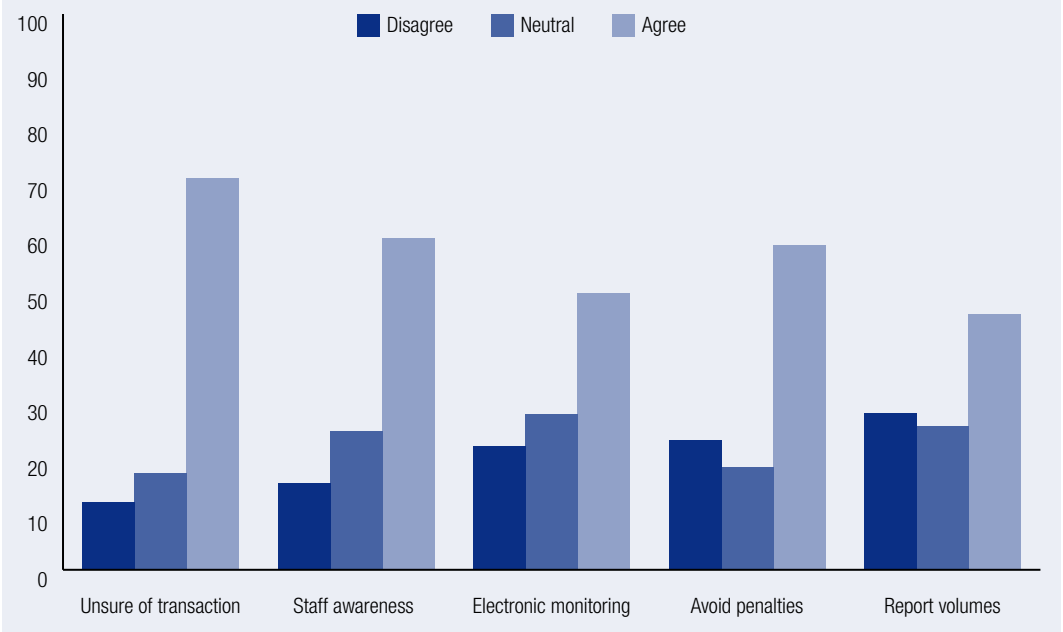
Source: AIC AML/CTF Australian businesses survey [computer file]

Views of interviewees regarding risk management

Although only a small number of individuals agreed to participate in follow-up interviews, a number of relevant issues were raised that help understand how reporting entities undertake risk management in connection with AML/CTF compliance. Some interviewees, for example, reported limiting the types of products, services, or transactions that they might otherwise offer, primarily in order to reduce risks of financial loss to their businesses but with the subsidiary aim of reducing risks of any involvement in any illicit financial transactions. The private mortgage lender who participated in an interview indicated that risks of loss were minimised by limiting loans made to non-Australian residents for residential properties. The lender would not lend any funds for 'off the plan' property purchases to any borrowers and would only lend up to 70 percent of the value of a property. The business aimed to safeguard itself against risks that may be associated with non-resident borrowers by conducting enhanced due diligence on those clients. The enhanced due diligence procedures the mortgage lender conducted included investigating whether the client had Foreign Investment Review Board approval, documenting their reasons for being in Australia, using their identification and profile to verify the client's legitimacy and witnessing evidence of the funds available to them in Australia. Generally, these clients would need to have status as a permanent or temporary resident in order to borrow funds.

Other interviewees described risk management activities that were supplementary to customer identification and transaction monitoring. The interviewee from the mutual banking business indicated that its risk management procedures had been revised following the introduction of the AML/CTF Act 2006 (Cth). The risk management system at the time of interview included the development of a risk management framework, the creation of a staff library for AML/CTF documents, random file auditing conducted every two months and tracking risks within a database system. The program required all supervisors and managers to undergo risk checks each month and the top 10 risks were then reported to the board. A key aspect of the risk management system was the establishment of an internal fraud unit, consisting of the compliance officer, an information technology officer and the finance manager, which was

Figure 19 Justifiability of reporting more transactions than necessary, by circumstances (%)



Source: AIC AML/CTF Australian businesses survey [computer file]

deliberately established as a hierarchical system for examining reports of suspicious transactions.

The mutual banking business also performed police records checks with the Australian Federal Police and a bankruptcy check via the Australian Prudential Regulation Authority and ASIC disqualification registers, prior to employing new staff members. All staff members made an AML/CTF declaration as part of their annual performance review and were required to declare any convictions recorded against them in the previous 12 month period. Staff members were also trained annually with AUSTRAC materials and any sites with a poor compliance performance in the auditing process received additional training. The business also sought to educate customers on the risks associated with their personal accounts.

By contrast, the two money exchange and remittance businesses interviewed did not carry out substantial changes to the ways in which they identified customers and handled business records following the commencement of reporting obligations. The businesses had an identification database, although this predated the AML/CTF Act 2006 (Cth) requirements. All customers were identified, usually with a passport, and the business did not undertake additional identification procedures beyond this unless the transaction was in excess of $10,000. In these cases, the forms for a large cash transaction were also completed within four or five days. The owner considered the KYC principles to be sufficient for a small business in its current location.

Two interviewees reported considering specific risk-management procedures for terrorism financing separately to the procedures employed for money laundering. The mutual bank used its transaction monitoring software to do a monthly search of its customer database against names of the Department of Foreign Affairs and Trade (DFAT) watch list. The issues associated with this list, such as duplicated names or alternate spellings, meant that the business did not follow up any partial matches and only examined any complete matches between their customers and the list. The private mortgage lender, by comparison, did not use the DFAT or Attorney-General's proscribed persons lists at all. The company secretary was confident that any persons on those lists would not apply for a loan in their own name and he doubted that he would be able to deduce whether a customer was applying for a loan on behalf of an individual on those lists.

Compliance costs associated with the anti-money laundering/counter-terrorism financing regime

The present study sought to assess the financial and other costs associated with conducting the AML/CTF regime in Australia. Unfortunately, difficulties were encountered by participants in quantifying precisely the costs of implementing AML/CTF regulations. Previous surveys of regulated businesses overseas have also emphasised the difficulties associated with quantifying the costs of AML/CTF regimes. For example, in the United Kingdom, more than 80 percent of MLROs surveyed by PricewaterhouseCoopers were unable to determine their company's expenditure on AML/CTF in 2006 (PricewaterhouseCoopers 2007). This was partly due to the way compliance systems have been designed, which often do not permit costs specifically associated with AML/CTF compliance to be disaggregated from overall business compliance costs generally. Few reporting entities in Australia have previously provided estimates of the actual cost of AML/CTF implementation. Some banking businesses have declined to do so, citing commercial confidentiality and Sathye (2008) has suggested that accounting practices may render the calculation of separate costs for AML/CTF compliance impossible to ascertain. Hence, the present AML/CTF Australian businesses survey is unique in providing some of the first quantitative estimates of implementation and compliance costs that have been published in Australia.

Despite the fact that the business environment and regulatory systems differ in some overseas countries from those that exist in Australia, it is appropriate to look to some international research to understand the difficulties that arose in attempting to quantify compliance costs and the effectiveness of the regime in the current study. Although most of the MLROs surveyed by PricewaterhouseCoopers in the United Kingdom in 2007 were unable to quantify the costs associated with AML/CTF compliance precisely, approximately 80 percent of the sample considered that the regime had delivered no benefits to their businesses when taking into consideration the level of cost involved (PricewaterhouseCoopers 2007); and one-third of MLROs surveyed in 2001 believed that the costs of AML/CTF outweighed any benefits of the regime (Gill & Taylor 2004). The views of businesses on the expense of AML/CTF in this study were tied to the business sector of the respondents and were also linked to the size of the business in question. Approximately 67 percent of banks did not consider AML/CTF too costly for the risks involved, whereas more than 70 percent of building societies and 68 percent of insurance companies stated that the regime was too expensive for those risks. Almost half of this sample of MLROs, who also performed another role in their company, considered the regime too expensive. By comparison, only a quarter of full-time MLROs considered the

regime to be too expensive. Gill and Taylor (2004) suggested that the more favourable view of full-time MLROs stems from their employment in the banking sector. MLROs with concurrent roles may also be more likely to work in a smaller business and this may also have influenced their views on the balance of costs of AML/CTF for the risks involved.

The results of previous overseas surveys have found relatively large increases in AML/CTF compliance costs since the regime has been implemented. The Tier One banks surveyed by KPMG (International 2007), for example, reported an average increase of more than 50 percent for AML/CTF compliance costs between 2004 and 2007. Similarly, more than three-quarters of the regulated businesses surveyed by KPMG in India in 2009 anticipated an increase in their AML/CTF compliance costs in the three years to 2012. These businesses identified automated transaction monitoring, retrospective transaction review and transaction monitoring as the most expensive aspects of compliance. More than 90 percent of the Indian sample forecast that their transaction monitoring systems would need more resources because of the complex implementation process, ongoing costs and reviewing false positives. Just over 75 percent of these businesses anticipated that their total costs for all AML/CTF compliance would increase in the three years to 2012 (KPMG (India) 2009). KPMG's 2007 Tier One (by capitalisation) banks also reported human resources and transaction monitoring to be the most expensive aspects of AML/CTF compliance (KPMG International 2007).

Current costs of compliance and anticipated changes

The survey sought to document both the nature and amount of the costs expended by respondent businesses in complying with the AML/CTF requirements during the preceding 12 month period ending 30 June 2009. The survey also canvassed the expectations of participants regarding the changes to their AML/CTF compliance costs in the two years to 30 June 2011. Because regulated businesses are well-placed to identify opportunities for reducing their compliance costs, the survey also asked for views on potential cost saving measures.

Cost estimates are somewhat difficult to calculate as initial implementation costs can often be high where new systems are created and software purchased, while savings can be made in subsequent years as systems are refined and inefficiencies eradicated. Subsequent years may, however, have ongoing maintenance costs and regular staff training overheads. Costs can also vary as businesses change their operations or move into new markets—particularly those that entail business transactions with potentially high-risk customers located overseas. As this survey was completed shortly after the full implementation of the AML/CTF Act 2006 (Cth), the costs data presented below refer to a period when entities were actively making system changes in response to new compliance obligations. It is possible that for some entities these changes required substantial expenditure while for others, only minimal investment was needed. The findings described below refer to expenditure as estimated for this timeframe, which may or may not have continued into the current period. In addition, as noted above, it is sometimes also difficult for AML/CTF compliance costs to be disaggregated completely from general corporate compliance and risk management costs. This is reflected by some respondents to the present survey being unable to qualify the costs of AML/CTF specifically.

The survey began by asking respondents to estimate the approximate cost to their business of complying with the AML/CTF regime over the 12 month period ending 30 June 2009. Figure 20 shows that expenditure estimates for all of the survey respondents ranged from $0 to $60m for the period in question. One-fifth (21%) of respondents stated that their business did not incur any AML/CTF compliance costs in the period to 30 June 2009. When costs were incurred, the mean expenditure per business was $57,580, with a median cost of $1,000. Almost two-thirds of the respondents (63%) estimated that their business' expenditure on AML/CTF compliance was more than $1 and less than $10,000.

In terms of the sector respondents occupied, at least some respondents from each sector reported having no expenditure on AML/CTF compliance.

Almost 40 percent of businesses classified as 'other' reported no AML/CTF compliance expenditure, while only four percent of managed funds and superannuation sector respondents reported no such expenditure. The results in Table 20 show the average and range of reported AML/CTF costs within each business sector. Businesses from the securities and derivatives sector had the highest mean annual compliance costs at close to $300,000 for the 2008–09 year. The sectors that reported the least mean expenditure on anti-money laundering compliance were the foreign exchange sector, the gambling sector and those classified as 'other' businesses.

Comparing categories of expenditure on AML/CTF compliance (see Figure 20) with categories of annual business turnover (see Table 3), a statistically significant, but weak relationship was found (χ^2=327.8, df=25, $p \leq 0.0001$; Cramér's V=0.23). Similarly, comparing categories of expenditure on AML/CTF compliance (see Figure 20) with categories of the number of full-time equivalent employees (see Table 2), a statistically significant, but weak relationship was found (χ^2=802.1, df=30, $p \leq 0.0001$; Cramér's V=0.23).

Figure 21 shows the percentage of businesses in each sector whose expenditure on AML/CTF compliance was grouped into five categories (in addition to those who reported zero expenditure). As expected, respondents from the managed funds/superannuation, banking and securities sectors spent the highest amounts on AML/CTF compliance, while those from the gambling, foreign exchange and 'other' sectors spent the least. Over 50 percent of managed funds businesses spent in excess of $10,000, while only 4.3 percent of those in the gambling sector spent in excess of $10,000. Approximately one-quarter (25.5%) of cash delivery businesses spent between $1 and $500. The highest expenditure on AML/CTF compliance costs were reported by one respondent with 850 full-time equivalent employees from the securities and derivatives sector who spent $60m in the year 2008–09. The highest spend in the banking sector was one business that spent $36.2m for the year (see Table 20).

Respondents were also asked to arrange various types of compliance costs in rank order from most costly to least costly. The aspects ranked were:

- AML/CTF training and professional development;
- AML/CTF staff recruitment;
- AML/CTF staff salaries;
- AML/CTF monitoring software establishment costs;
- AML/CTF monitoring software recurrent costs; and
- AML/CTF external consultancy costs.

Respondents were also able to provide a rank order for additional items of compliance expenditure and these were also rated from the most costly item to least costly. Table 21 presents summary statistics for respondents' rankings of the most costly aspects of AML/CTF compliance. Respondents indicated that training and professional development and staff salaries were the two most costly aspects of compliance from the prompted categories. Record keeping and customer relations were the two most costly areas of expenditure of the self-nominated categories.

Comparing mean results for responses relating to the two categories with the highest rankings (training/professional development and record keeping), it was found that there was no statistically significant difference between these two categories (t=-1.1, $p \geq 0.28$). Similarly there were no significant differences between the compliance cost mean rankings for record keeping, monitoring, and reporting and for the costs of customer relations (t=-0.407; $p \geq 0.703$); or the cost of record keeping and the costs of equipment and administration (t=-1.809; $p \geq 0.080$), or for each of the unprompted compliance cost areas supplied by survey respondents.

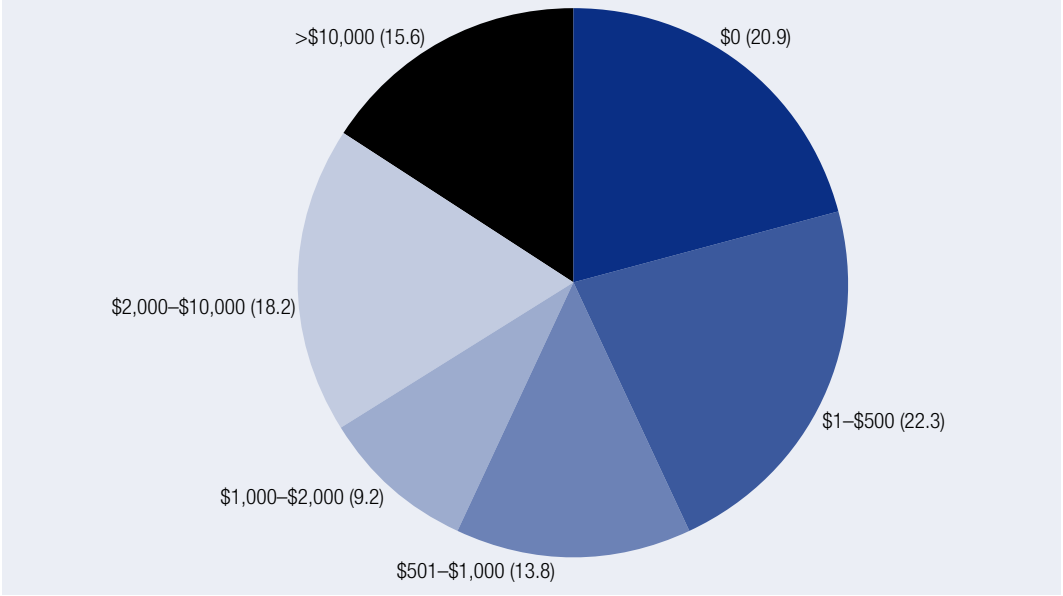
Respondents were also asked to indicate the extent to which they expected their AML/CTF compliance costs would change in the two year period ending 30 June 2011 and if so, what was the area of greatest increase or decrease. More than two-thirds of respondents (67.7%) expected the AML/CTF compliance costs to their businesses to remain the same in the two year period to 30 June 2011. Few businesses (5.5%) anticipated those costs falling while a little over a quarter of respondents (26.8%) anticipated that their AML/CTF costs would increase (see Tables 29 and 30 regarding anticipated increases in compliance areas). Figure 22 shows the responses from businesses in the various sectors concerning the likelihood of costs of compliance changing in the

ensuing two years to 30 June 2011. The largest proportions of almost all sectors expected compliance costs to remain the same. The alternative remittance sector (47.8%), cash delivery services (43.2%) and the securities and derivatives (42%) sectors were those with the largest proportion of businesses anticipating an increase in compliance costs. The gambling and foreign exchange sectors both had approximately 75 percent of respondents expecting the costs of compliance to remain the same in the two years to 30 June 2011.

The size of the expected increases and decreases in compliance costs to 30 June 2011, for those respondents anticipating a change, are presented in Table 22. Approximately 70 percent of the proportion of respondents expecting a shift in compliance costs also expected those costs to rise by up to 50 percent. A much smaller proportion (12.9%) anticipated an increase in AML/CTF costs of more than 50 percent.

Table 23 shows how these anticipated changes in AML/CTF compliance expenditure differed according

Figure 20 Estimated compliance costs from all respondents for the year to 30 June 2009 (%)



Source: AIC AML/CTF Australian businesses survey [computer file]

Table 20 AML/CTF compliance expenditure across sectors

Sector	Mean ($)	Median	Range
Gambling	$10,848	$500	$0–$12,000,000
Banking	$198,156	$2,100	$0–$36,200,000
Managed funds and superannuation	$52,201	$6,000	$0–$3,000,000
Financial services	$26,721	$1,000	$0–$3,016,500
Securities and derivatives	$291,037	$1,000	$0–$60,000,000
Foreign exchange	$7,979	$375	$0–$550,000
Cash delivery	$12,801	$500	$0–$550,000
ARS	$12,003	$1,000	$0–$550,000
Other	$8,349	$250	$0–$550,000
All sectors	$57,580	$1,000	$0–$60,000,000

Source: AIC AML/CTF Australian businesses survey [computer file]

to the business sector respondents occupied. Of those anticipating an increase in compliance costs, the financial services sector comprised the largest proportion of businesses that expected costs to increase by more than 50 percent. The managed funds and superannuation sector comprised the largest proportion of businesses anticipating a fall in compliance costs of more than 50 percent.

Respondents who reported expecting AML/CTF compliance costs to their business to increase or decrease in the two years to 30 June 2011 also nominated the area of expenditure likely to show the greatest change. The largest proportion of respondents (39.5%) anticipating either an increase or decrease in costs nominated AML/CTF staff training and professional development as the area likely to show the greatest change. AML/CTF staff recruitment was the cost compliance area nominated by the smallest proportion of respondents anticipating change (1.8%) as being most likely to show the greatest impact on costs.

The results presented in Table 24 and Table 25 show that respondents who expected an increase in AML/CTF costs identified different areas of change to businesses who anticipated a decrease in costs.

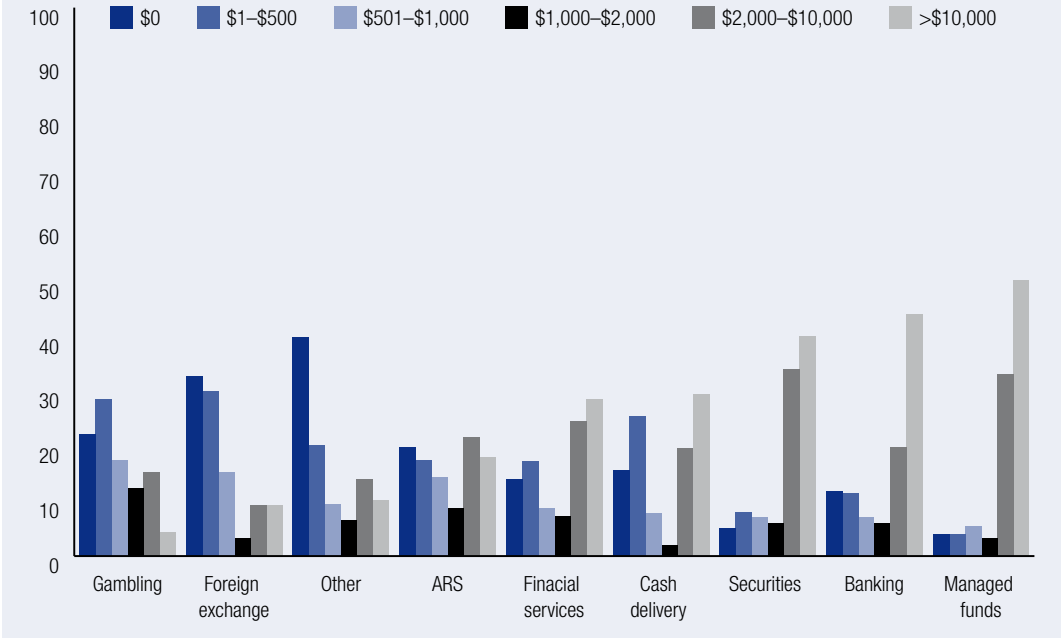
Just over 43 percent (43.2%) of respondents who expected an increase thought that training and professional development would be the area of expenditure most likely to change. An additional fifth of respondents (20.4%) expected that AML/CTF staff salaries would be the area of the greatest cost increase to 30 June 2011.

Approximately 30 percent of businesses who anticipated a decrease in costs in the period to 30 June 2011 identified the use of external consultants to be the area of greatest change. Fewer businesses (22.7%) expected staff training and professional development to have the greatest impact on costs although this was similar to the proportion of businesses that anticipated an increase in staff salaries (20%).

Respondents were also asked to indicate how the costs to their businesses of complying with the AML/CTF regime could be reduced. The prompted alternatives were:

- avoiding duplicated compliance procedures;
- sharing data and information with other businesses;
- streamlining account opening procedures;

Figure 21 Compliance cost categories for the year to 30 June 2009, by business sector (%)



Source: AIC AML/CTF Australian businesses survey [computer file]

- developing AML/CTF software in-house;
- reducing their reliance on outsourced expertise; and
- greater sharing of typology data and software by AUSTRAC.

From Table 26 it is apparent that the largest proportion of respondents (34.2%) indicated that AML/CTF costs could be reduced by not duplicating compliance procedures.

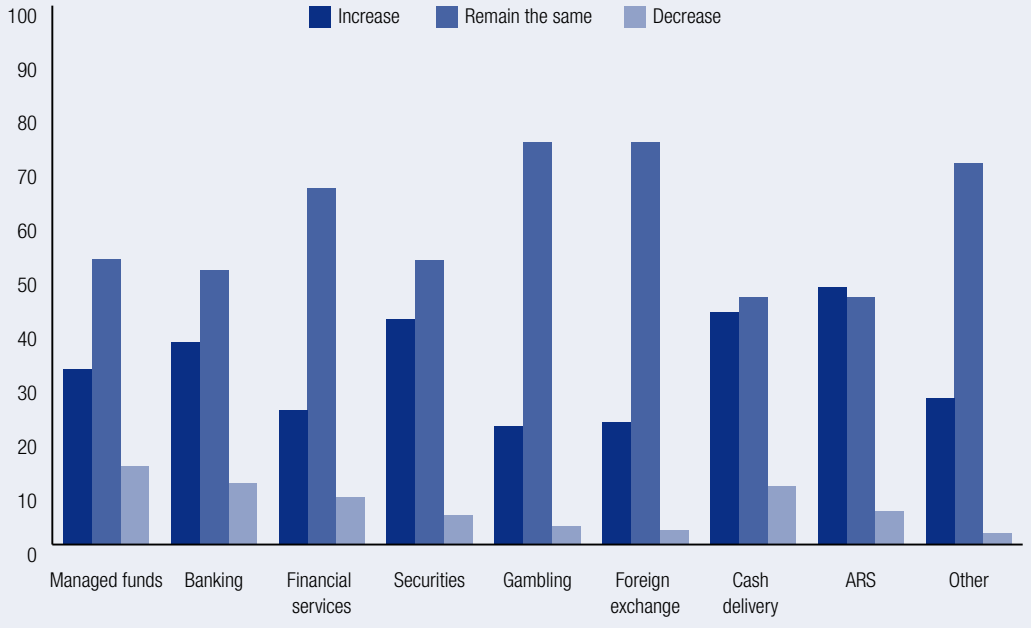
Tests of association demonstrated a statistically significant, but weak relationship between the compliance cost expectations of respondents and their views on reducing costs by avoiding duplicated compliance procedures (χ^2=28.0, df=2, $p \leq 0.0001$,

Table 21 Most costly compliance components

Compliance aspect	Mean ranking	Median ranking	Standard deviation
Prompted responses			
Training/professional development	2.19	2	1.5
Staff recruitment	3.62	3	1.5
Staff salaries	2.68	2	1.5
Monitoring software establishment	3.73	4	1.4
Software recurrent	4.52	5	1.4
External consultancy	4.11	5	2.0
Unprompted responses			
Record keeping/monitoring/reporting	1.91	1	1.5
Equipment/admin costs	2.81	3	2.0
Customer relations	2.40	1	2.6

Source: AIC AML/CTF Australian businesses survey [computer file]

Figure 22 Estimated movements in compliance costs to 30 June 2011, by business sector (%)



Source: AIC AML/CTF Australian businesses survey [computer file]

Cramér's V=0.10). Those who anticipated an increase in their compliance costs were more likely to agree that those costs could be reduced by avoiding any duplication in procedures.

Respondents who anticipated an increase in costs also indicated that greater sharing of typology data and software by AUSTRAC would reduce their costs, although the survey did not specify what that data or software might be. Tests of association showed that the relationship between anticipated cost movements and greater sharing of typology data and software by AUSTRAC was statistically significant (χ^2=68.7, df=2, $p \leq 0.0001$, Cramér's V=0.15). The association between expected compliance costs and the belief that data sharing with other businesses would reduce costs was also statistically significant (χ^2=9.9, df=2, $p \leq 0.007$, Cramér's V=0.06). Participants who anticipated cost increases to 30 June 2011 were also more likely to agree that data sharing with other businesses would reduce their compliance costs.

Interviewees' views of compliance costs

The views expressed by interviewees on the costs and utility of the AML/CTF regime showed a mixture of support for the aims of the regime and difficulties in its application. One interviewee anticipated that, in 2006 when the regime was introduced, compliance costs would be onerous, but later found that compliance was relatively simple and that existing compliance programs or other risk management processes were able to be adapted to suit the new requirements. The positive experiences of one small business with respect to compliance and the ability of existing risk management practices to be integrated into AML/CTF compliance activities, led

Table 22 Anticipated shifts in AML/CTF compliance costs

Direction of change	Extent of change	Index	
		n	%
Anticipated reduction in costs	<50%	59	6.5
	>50%	96	10.5
Anticipated increase in costs	<50%	639	70.1
	>50%	118	12.9

Source: AIC AML/CTF Australian businesses survey [computer file]

Table 23 Anticipated movements in AML/CTF costs to 30 June 2011, by business sector (%)[a]

Business sector	Anticipating decreased costs		Anticipating increased costs		Total
	Decrease by more than 50%	Decrease by less than 50%	Increase by less than 50%	Increase by more than 50%	
Managed funds/super	18.5	12.6	63.0	5.9	100.0
Banking	14.6	8.1	70.9	6.4	100.0
Foreign exchange	3.7	7.4	77.8	11.1	100.0
Securities/derivatives	7.0	4.7	76.7	11.6	100.0
Cash delivery service	10.0	10.0	65.0	15.0	100.0
Gambling	10.0	3.8	71.1	15.1	100.0
Alternative remittance	5.1	5.1	74.6	15.3	100.0
Other	5.4	1.8	75.0	17.9	100.1[b]
Financial services	10.0	15.0	47.5	27.5	100.0

a: Percentages are of those respondents who anticipated a change in costs

b: Percentages may not total 100 due to rounding

Source: AIC AML/CTF Australian businesses survey [computer file]

the Managing Director to believe that those businesses that had difficulties in complying with the AML/CTF regime probably had inadequate risk management procedures in place prior to 2006 and that the introduction of the AML/CTF legislation simply exacerbated the problem for them. Another interviewee noted that although the AML/CTF compliance costs had been very great for her business, the additional benefits that it provided in terms of enhanced risk management made it more than worthwhile. Even if the current legislative requirements were abolished, she would still seek to maintain the system that had been introduced.

For interviewees employed in compliance roles within their organisations, filing the annual compliance report was not felt to be challenging. The picture that emerged from the interviews was that for those with a professional understanding of compliance, or with existing exposure to compliance obligations other than the AML/CTF regime, compliance was not overly difficult. Those without this experience, particularly those from the gambling and alternative remittance sectors, indicated that they found it difficult to understand the entire range of their reporting obligations and where they encountered problems, found it difficult to obtain clear and simple advice. A major concern identified by interviewees from small businesses related to the often legalistic language used by the regulator in providing information and advice. The gambling sector was the industry sector that interviewees perceived the AML/CTF regime as being too onerous for, in view of the risks present in Australia. By comparison, however, one interviewee who was a securities dealer and an Australian Financial Services Licence holder prior to the 2006 AML/CTF reforms, indicated that AML/CTF compliance for his business was so simple that it was pointless. This interviewee took

Table 24 Anticipated increase to costs to 30 June 2011, by compliance area (%)

AML/CTF compliance expense area	%
AML/CTF training and professional development	43.2
AML/CTF staff recruitment	1.9
AML/CTF staff salaries	20.4
AML/CTF software establishment costs	12.7
AML/CTF software ongoing costs	6.3
External consultants	12.5
Other	2.9

Note: Percentages may not total 100 due to rounding

Source: AIC AML/CTF Australian businesses survey [computer file]

Table 25 Anticipated decrease to costs to 30 June 2011, by compliance area (%)

AML/CTF compliance expense	%
AML/CTF training and professional development	22.7
AML/CTF staff recruitment	1.3
AML/CTF staff salaries	20.0
AML/CTF software establishment costs	18.0
AML/CTF software ongoing costs	0.0
External consultants	29.3
Other	6.0
n/a	2.7
Total	100.0

Source: AIC AML/CTF Australian businesses survey [computer file]

the view that the other compliance obligations for his business, managed by ASIC, were far more arduous. He further noted that the information and templates that ASIC provided were accessible and helpful.

Some interviewees expressed that they had considerable difficulties understanding the regime and knowing how to comply with the legislation. It should be noted that these interviews were conducted in 2009, shortly after full implementation of the 2006 legislation. The actual financial cost of compliance was seen as being less of a problem for some compared with the time and effort required to understand the compliance requirements for small businesses unfamiliar with money laundering and financial crime. Interviewees from the small business sector, in particular, indicated that they found it difficult to obtain advice on how to implement a compliance program that was appropriate for their business sector. The annual compliance report was difficult for some interviewees, although less of a problem for more experienced compliance officers.

Most interviewees found accurate quantification of the costs of complying with the AML/CTF regime for the year to 30 June 2009 difficult. Particular issues arose because AML/CTF compliance costs often were embedded within more general corporate compliance and risk management costs. The reported expenditure was likely to have been affected by the size of businesses, although interviewees suggested that the estimates provided by businesses with multiple types of compliance obligations were probably not solely related to AML/CTF compliance. The interviewees who were able to indicate a dollar amount for their AML/CTF compliance costs for the 2008–09 financial year drew on the fixed costs of software, staff and external consultants to arrive at an estimate, although they noted that the time spent on compliance was difficult to quantify.

The representative from the mutual banking business reported that the business spent approximately $60,000 in the year to 30 June 2009 on AML/CTF compliance. The software component of this figure was $1,500 per month during that period and the remaining portion was for the salary of the compliance officer. The business intended to enhance the software package that it used for risk monitoring and tracking but also noted the impossibility of determining the amount of staff time required to establish the AML/CTF program. The representative from the private equity investor firm, by contrast, paid $25,000 to engage solicitors to prepare an AML/CTF policy but noted that the remaining costs of compliance were negligible as they were subsumed within general risk management and corporate governance activities. The private mortgage provider approached several legal firms to provide the same service to their business and decided, in view of the high price of outsourcing, to develop an AML/CTF compliance regime in-house. This interviewee found the process challenging because of an absence of clarity in the guidelines he used.

Staff costs, record keeping and customer relations were considered to be the most costly components of AML/CTF compliance, with staffing also being identified as an area in which costs are likely to increase. However, this was not the case for all interviewees. One interviewee expected AML/CTF costs to be quite high when he first examined the requirements but subsequently found that his business did not need to hire any new staff in order to become compliant. The resulting costs for implementing an AML/CTF program for this business, as a consequence, were quite low.

Table 26 Mechanisms to reduce AML/CTF compliance costs (%)

Prompted cost reduction mechanisms	%
Avoiding duplication of procedures	34.2
Sharing data and information with other businesses	19.8
Streamline account opening	9.2
Develop AML/CTF software inhouse	10.3
Less reliance on outside experts	10.2
Sharing from AUSTRAC	20.5

Source: AIC AML/CTF Australian businesses survey [computer file]

Attitudes towards the anti-money laundering/ counter-terrorism financing regime

One of the central aims of the present study was to canvass the views of respondents concerning the necessity for, and effectiveness of, Australia's AML/CTF regime. Views were also sought on the necessity of the level of resources required for compliance with the legislation in light of the level of risk of ML/TF in Australia and accordingly, the extent to which the regime was effective in minimising risk. Finally, respondents were also invited to offer suggestions concerning possible ways the regime could be improved.

Effectiveness of the anti-money laundering/counter-terrorism regime

The present study sought to document the views of those regulated by Australia's AML/CTF regime by seeking their opinions on the regime's contribution to the deterrence of financial crime, minimisation of financial crime risks within businesses, ability to recover the proceeds of crime and promote good governance and integrity of the financial system generally. The AML/CTF regime operates within a much broader regulatory environment, so it was sometimes difficult for respondents to identify the precise extent of the contribution of the AML/CTF regime as distinct from other aspects of corporate governance. Nonetheless, the responses provided some indication of how businesses assessed some of these key aspects of the AML/CTF regulatory environment.

Respondents were asked to rate the effectiveness of the AML/CTF regime in achieving each of the following nine goals:

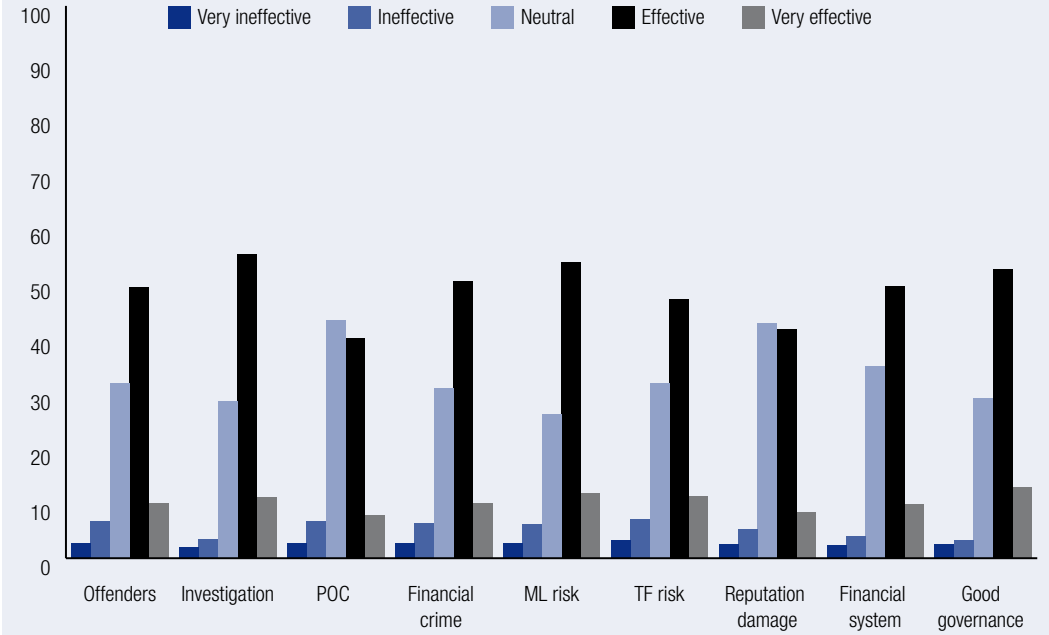
- deterring offenders from using reporting entities to facilitate crime;
- enabling regulators to investigate financial crime effectively;
- facilitating the recovery of the proceeds of crime;
- minimising risks of financial crime and identity fraud;
- minimising risks of money laundering;
- minimising risks of terrorism financing;
- minimising risks of reputational damage;
- maintaining the integrity of the financial system; and
- promoting good governance.

The views of survey participants on the ability of the AML/CTF regime to meet is goals varied quite considerably (see Figure 23). Overall, significantly more respondents viewed the regime as being effective or very effective at minimising the risk of money laundering (65.2%) compared with those who believed the regime was effective or very effective at minimising terrorism financing risks

(58.2%; t=4.7, $p \leq 0.0001$). Ten percent of respondents took the view that the aim of the AML/CTF regime to reduce risks of terrorism financing was either ineffective or very ineffective.

Table 27 presents centralised tendency results for the ratings that respondents gave the regime in meeting its nine objectives. The aim of the regime of 'enabling regulators to investigate financial crime effectively' received the highest mean effectiveness rating (3.7), as did the additional benefit of installing 'good governance practices'. The lowest effectiveness rating was given for the aim of 'facilitating the recovery of the proceeds of crime' (3.4). A statistically significant difference was found between the mean results for the highest and lowest mean rated aims of the regime (t=-2.5; df=7069.9; $p \leq 0.01$).

Figure 23 Perceptions of the AML/CTF regime's ability to meet its stated goals



Note: POC=proceeds of crime

Source: AIC AML/CTF Australian businesses survey [computer file]

Table 27 Perceptions of the effectiveness of the AML/CTF regime, by goal

Possible benefit	Mean effectiveness rating (1–5)	Median effectiveness rating (1–5)	Standard deviation
Deter offenders	3.6	4.0	0.9
Help regulators to investigate financial crime	3.7	4.0	0.8
Facilitate proceeds of crime recovery	3.4	3.0	0.8
Minimise financial crime/ID fraud risks	3.6	4.0	0.9
Minimise money laundering risks	3.7	4.0	0.9
Minimise terrorism financing risks	3.6	4.0	0.9
Minimise reputational damage risks	3.5	3.0	0.8
Financial system integrity	3.6	4.0	0.8
Good governance practices	3.7	4.0	0.8

Source: AIC AML/CTF Australian businesses survey [computer file]

Overall, survey respondents considered that the AML/CTF regime was generally effective in meeting most of its stated aims, such as deterring offenders, facilitating investigations of financial crimes and promoting good governance, and held neutral opinions regarding its effectiveness in reducing reputational risks and tracking the proceeds of crime.

Views of interviewees concerning effectiveness of the regime

Interviewees indicated that the regime was, to them, less effective in minimising risks of terrorism financing than money laundering, owing to the amounts of money involved being generally much smaller than the amounts of money that would be involved in money laundering activities.

One interviewee from the remittance sector viewed the current system of threshold reports and suspicious transaction reports as well as the general monitoring of large remittances, to be effective in identifying fraudulent transactions. One business, for example, used its transaction monitoring systems to identify several Nigerian scams that had been reported to its parent company. The parent company was able to examine the transactions in its database and to contact the customer in question to prevent the customer from being defrauded. Although the business in question was not obligated to prevent its customers from sending funds in these circumstances, it tried to discourage them from doing so.

Interviewees indicated that the regime had focused their attention on the possible impact that criminal activities could have on their operations, on their profitability, or on their corporate reputations, even if the regime could not materially change behaviour in all cases. The perceived effectiveness of the AML/CTF regime was influenced, for some, by the paper trail that law enforcement and other agencies could follow, even if it remained very difficult for banks to stop financial crimes from actually taking place. These views are reflected in the results presented in Table 32, which show that the aim of helping regulators to investigate financial crime effectively was the most highly rated aim in terms of effectiveness of the regime.

Other interviewees, from both the financial services and gambling sectors, considered that the regime was an appropriate crime risk-reduction mechanism but considered, on balance, that the inclusion of their business within the regime was inappropriate because of their perceived very low levels of risk.

Justifications for the regime

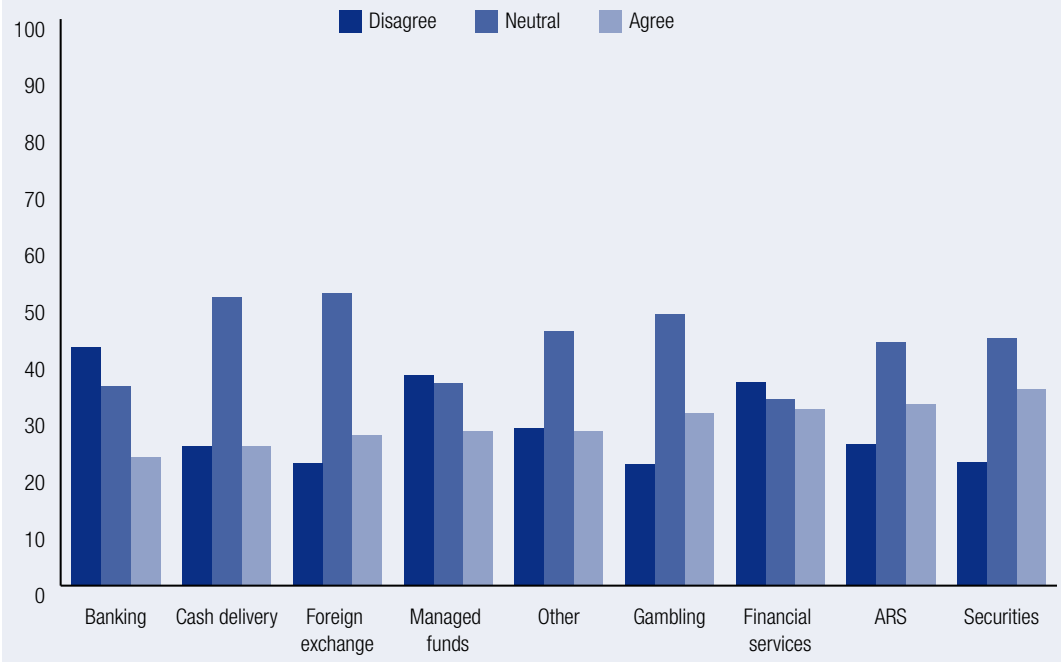
The participants in the study were also asked to provide their views on whether they considered that the costs and difficulties of the AML/CTF regime were justified, given the risks of money laundering and the financing of terrorism that were present in Australia. Specifically, participants were asked to indicate on a five-point scale the extent to which they agreed or disagreed with the statement 'In Australia, the AML/CTF regime is too onerous, given the risks' and then to provide reasons for their views.

On the scale from 1 (strongly disagree) to 5 (strongly agree), all respondents recorded a mean score of 3.8, a median score of 3.0 and a standard deviation of 1.0. The largest proportion (45.5%) of respondents neither agreed nor disagreed that the system was too onerous for the money laundering risks. The proportion of respondents who agreed with the statement (30%) was slightly higher than the proportion that did not (25.7%). These findings indicate there is no strong feeling either way about the extent to which the regime is onerous.

The results were significantly different according to the business sector respondents occupied (χ^2=108.5, df=16, $p \leq 0.0001$). A Cramér's V of 0.12 indicated that there was a weak level of association between the views of respondents for the justifications for the regime and the business sector they occupied. Those from the securities and derivatives, alternative remittance service and financial services sectors were most likely to take the view that the regime was too onerous for the perceived level of risks present (see Figure 24). Those in the banking sector were most likely to disagree that the regime was too onerous for the risks perceived to be present (42.1%).

Each respondent was also asked to provide their reasons for agreeing or disagreeing with the view that the AML/CTF regime in Australia was too onerous given the risks. From Table 28, it is apparent that the most common reason offered by businesses

Figure 24 Perceptions of the demands of compliance for the risks involved, by business sector (%)



Source: AIC AML/CTF Australian businesses survey [computer file]

Table 28 How respondents view the AML/CTF regime (%)

Reason	All businesses	'Disagreeing' businesses
Not too onerous		
Not too onerous/adequate/sufficient	3.1	7.7
Necessary/essential/important/beneficial	7.7	20.8
Safety/security/counter-terrorism	4.3	14.0
Money laundering/crime	4.6	15.0
In line with international standards	0.5	2.0
Many procedures already in place	1.4	3.5
Low risk, low burden	1.4	2.6
Too onerous		
Process is onerous/unnecessary	3.3	8.0
Business is small/reporting threshold too low	8.4	19.1
Business/area/industry is low risk	8.6	19.7
Regime time intensive/costly/work intensive	6.3	15.1
Regime complicated/hard to understand/need guidance	3.0	5.1
My business should be exempt/doesn't apply to us	1.0	3.0
Regime prescriptive/compliance too general/not specific enough	3.7	8.9
Over regulated/issues already regulated by other bodies/duplication	3.2	8.56

Source: AIC AML/CTF Australian businesses survey [computer file]

that did not view the AML/CTF requirements as being too onerous was that the regime was essential or beneficial (20.8%). A further 14 percent of businesses who disagreed that the system was too onerous shared this view for safety reasons or because of the regime's counter-terrorism aims. A small proportion of businesses that disagreed that the regime was too onerous (2.6%) suggested that the perceived low risks to their businesses meant a low burden in terms of AML/CTF compliance.

The two most common reasons that participants cited for considering the AML/CTF regime to be too onerous were the small size of their businesses or that the threshold for reporting was too low (19.1%), or that they perceived their business or industry experienced a low AML/CTF risk (19.7%).

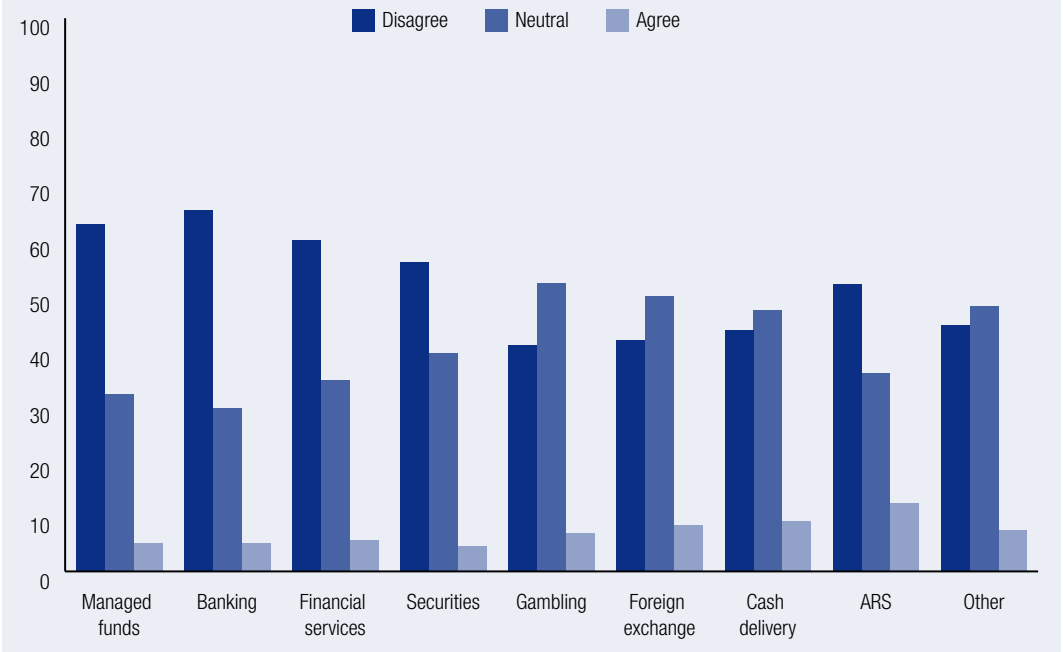
Level of business responsibility

Participants were also asked to comment on the level of responsibility for ensuring the legitimacy of their customers required by the regime. Specifically, respondents were asked to indicate on a five-point scale the extent to which they agreed or disagreed with the statement 'Not enough responsibility is placed on reporting entities to ensure probity when dealing with customers' and then to provide reasons for their views.

Just under half of respondents (46.7%) disagreed or strongly disagreed that reporting entities did not have enough responsibility to ensure probity when dealing with customers (see Figure 25). A smaller proportion (6.9%) agreed or strongly agreed that reporting entities' current responsibilities were insufficient. The largest single proportion of respondents (46.3%) provided a neutral response to the statement. Responses to this question differed significantly according to the business sector respondents occupied (χ^2=138.2, df=16, $p \leq 0.0001$). A Cramér's V of 0.14 indicated that there was a weak level of association between the views of respondents concerning their responsibility for ensuring probity of customers and the business sector they occupied.

Banking sector respondents were the most likely to disagree or strongly disagree that they did not currently have enough responsibility for ensuring

Figure 25 Perceptions of the responsibilities of business owners, by business sectors (%)



Source: AIC AML/CTF Australian businesses survey [computer file]

probity (65.4%), while respondents from the gambling sector were the least likely to disagree or strongly disagree with the statement, although still more than 40 percent disagreed or strongly disagreed with the statement. Respondents from the alternative remittance sector were most likely to agree or strongly agree that they did not have enough responsibility to ensure probity when dealing with customers (12.3%).

Respondents provided unprompted reasons for agreeing or disagreeing with the statement that reporting entities currently have enough responsibility for ensuring probity when dealing with customers and these are presented in Table 29. Almost 16 percent of respondents (15.7%) who disagreed with the statement gave their reason as being general support for the current regime or because they thought that they already had sufficient responsibility. Another 16 percent indicated that they were currently compliant or that the penalties for non-compliance were sufficiently high to ensure that adequate probity checks were made. Fewer businesses that disagreed that they did not have enough responsibility suggested that their obligations were costly and time consuming (4.5%), they were over-regulated or had too much responsibility (5.7%), or their responsibilities were too high in view of the low level of risk that was present (4.2%)

A far smaller proportion of respondents agreed or strongly agreed that they currently did not have enough responsibility to ensure probity. The largest group of these respondents formed this view because of a perception that more responsibility is needed generally, or that greater vigilance is required from some businesses (8.9%). Some respondents also expressed the view that combining the DFAT and Attorney-General's Department watch lists, and employing simpler language, would make compliance easier.

Interviewees reported experienced a number of challenges in assessing probity of their customers under the AML/CTF regime. Discrepancies between the AML/CTF regulatory requirements in different countries created problems for businesses with international operations and different standards for customer due diligence. Reporting had to be managed in each of the locations they conducted business. On a practical level, undertaking customer identification could also be difficult where customer bases included many foreign nationals whose names are not based on Roman characters. An example

Table 29 How respondents view levels of responsibility for ensuring probity (%)

Reason	All businesses	'Disagreeing' businesses
Disagreed that responsibility was insufficient		
Enough responsibility/regime is OK/generic positive	9.4	15.7
Over regulated/ too much responsibility/generic negative	3.1	5.7
Current system onerous/time consuming/costly	2.5	4.5
Obliged to comply/penalties high/currently compliant	9.2	16.2
Too much for low risk	3.5	4.2
We would do the requirements anyway	2.7	5.0
Current requirements already cover anti-money laundering	1.7	3.4
Agreed that responsibility was insufficient		
Need assistance/support/difficult to implement	1.6	4.3
System is ineffective	0.9	4.6
Needs more vigilance from some/more responsibility	1.3	8.9
Anti-money laundering is important/essential	0.8	2.5
Neutral response		
Irrelevant	0.7	1.1

Source: AIC AML/CTF Australian businesses survey [computer file]

given by one interviewee concerned the application of SWIFT transaction identification procedures that required a code to be used for Chinese character names. The resulting output was a very long code that made reporting difficult using standard forms. Most banks use SWIFT to transfer funds securely between banks.

Suggested improvements to the anti-money laundering/counter-terrorism financing regime

Survey respondents were also asked to consider how the AML/CTF regime could be improved. Survey respondents were provided with some closed questions, as well as the opportunity to provide their own suggestions for improvement (see Table 30). These findings should be read in the context that they were provided during the early stages of implementing the AML/CTF Act.

The category of improvements with which the largest proportion of respondents agreed was for AUSTRAC to provide more training courses and seminars on the regime (43.9%). These views were based on actual experience of AUSTRAC's services prior to 2009. Another third nominated the provision of more relevant typologies and case studies. The most commonly cited unprompted suggestion for improving the AML/CTF regime, nominated by 6.5 percent of respondents, was to consider business size, the extent of risks to businesses, or to consider industry-specific measures in reforming the regime.

Figure 26 shows the proportions in each business sector that responded to the three prompted responses to how regime could be improved—by AUSTRAC providing more typologies and case studies, by AUSTRAC offering more training courses and by more training and seminars being provided by industry peak bodies. Generally, there was a preference for AUSTRAC to provide more training courses, although those in the gambling and foreign exchange sectors least favoured this option. Alternative remittance providers were particularly keen on further training being provided by AUSTRAC

Table 30 Suggested improvements to the current AML/CTF regime (%)

Suggested improvements	%
Prompted responses	
More typologies/case studies from AUSTRAC	33.5
More training courses by AUSTRAC	43.9
More training/seminars by industry peak bodies	29.0
Unprompted responses	
More feedback on compliance/reporting	0.4
More case studies/typologies/examples of effectiveness	1.0
Abolish AML/CTF regime	0.6
Simplify the process/more user friendly	2.9
Consider business size/risk levels/industry specific regime	6.5
More data sharing/central data base	1.0
Stop duplication of reporting/of legislation/of requirements	0.5
More AML/CTF training/industry specific assistance	4.3
Provide software	0.3
Costs too high/provide reimbursement or concessions	0.5
Increase awareness/public information	0.3
Other	17.3
Don't know	2.4
Refused	0.2
No response	9.4

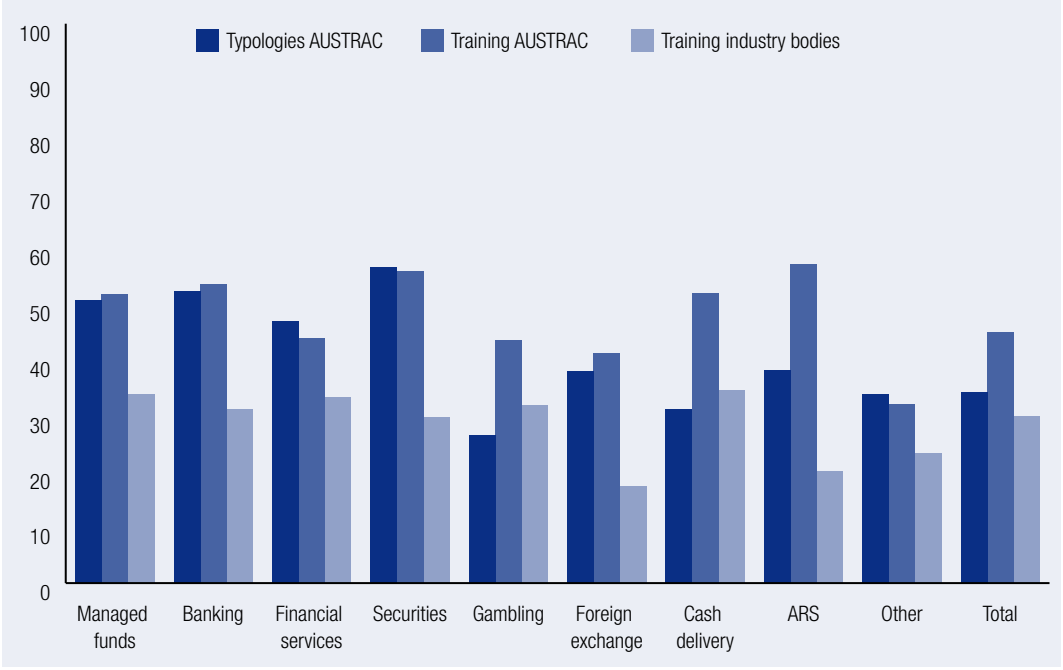
Source: AIC AML/CTF Australian businesses survey [computer file]

(a need reiterated during AIC consultations with alternative remittance providers; see Rees 2010). Those in the managed funds, financial services and cash delivery sectors also favoured the use of industry-based training because this is the form of training that is employed for other compliance regimes that they are subject to.

The results relating to each of the prompted alternative responses were significantly different according to the business sector respondents occupied in terms of the provision of more training course provided by AUSTRAC (χ^2=63.8, df=8, p≤0.0001, Cramér's V=0.10); in terms of the provision of more typologies and case studies from AUSTRAC (χ^2=188.1, df=8, p≤0.0001, Cramér's V=0.21); and in terms of the provision of training by industry peak bodies (χ^2=41.8, df=8, p≤0.0001, Cramér's V=0.10). Each of these statistics showed a weak level of association between the views of respondents as to the specified methods of improvement and the business sector they occupied.

More than half of the respondents from the managed funds and superannuation, banking and securities and derivatives sectors agreed that the current regime could be improved with more typologies and more training courses from AUSTRAC. Smaller proportions of respondents from the cash delivery (31%) and gambling sectors (26.4%) agreed that typologies and case studies provided by AUSTRAC would improve the regime. These findings illustrate to some extent the difficulties AUSTRAC faces in educating the regulated sectors, as it appears that a proportion of respondents were unaware of the typology reports and other sources of information that were available, even in mid 2009.

Figure 26 Suggested improvements to the AML/CTF regime, by business sector (%)



Source: AIC AML/CTF Australian businesses survey [computer file]

Principal findings and summary

The AML/CTF Australian business study surveyed businesses from all sectors in Australia during 2009 with AML/CTF regulatory requirements, including the gambling, banking, managed funds and superannuation, securities and derivatives, foreign exchange, alternative remittance, financial services and cash delivery sectors, and other businesses providing regulated services, such as bullion dealers. The study was the first in Australia to consider the views of reporting entities on the risks of money laundering and terrorism financing facing their businesses, their approaches to compliance, the costs of compliance the perceived effectiveness of the regime and ways in which the regime could be improved. The findings presented in this report summarise the views of regulated businesses in the phase immediately following the full implementation of the AML/CTF Act 2006 (Cth) in 2009. Further qualitative information on the perceptions of regulated businesses came from interviews undertaken with a small number of individuals who had completed the questionnaire and who were willing to undertake face-to-face interviews. Their views, although not necessarily representative of all the survey respondents, nonetheless provided some useful insights into how they understood Australia's AML/CTF regime in 2009.

Perceptions of risk

Perception of risks of money laundering

More than half of the respondents to the AML/CTF Australian businesses survey perceived the risk of their business becoming implicated in money laundering to be non-existent, or very low. The other half highlighted a diverse range of potential money laundering risks that they believed their businesses might face in the two year period to 30 June 2011. Many of these risks were tied directly to the core business of each industry sector and not to any external threat, type of customer, or type of predicate crime. The largest proportion of respondents (albeit only 5.9%) nominated gambling as the highest risk for money laundering, with the majority of these businesses being from the gambling sector themselves.

In relation to perceptions of the level of risk of money laundering to which the businesses of respondents were exposed, almost all of the survey participants (97.8%) stated that they considered their businesses were exposed to low risks of money laundering in the year to 30 June 2009. Ninety-five percent of the survey respondents anticipated that the level of risks would decrease or remain the same in the two year period to 30 June 2011. Nine businesses, from the

3,870 respondents who answered the question perceived the risks of money laundering to their businesses to be high. Most interviewees shared the view that their business faced few risks in mid 2009 and their expectation was that this situation would not change in the two year period to 30 June 2011.

Each of the business sectors surveyed in this study demonstrated different profiles in respect of who they considered to be high-risk customers, although each sector highlighted Australian and foreign individuals, PEPs and foreign companies as the four riskiest types of customers. As might be expected in a risk-based system, individual businesses assigned risk based on their own experiences. For example, respondents providing gambling services were less likely to identify PEPs as high-risk customers compared with respondents from the banking sector—although as noted above, casinos might have viewed PEPs as a higher risk than clubs and pubs—which was not able to be assessed in this survey where the results of all gambling service providers were grouped together. The perception of high risk did not include customer types that might be linked to complex business arrangements, which might be used to conceal beneficial ownership such as trusts, associations, or domestic companies.

More than one-third of survey respondents nominated individuals as high-risk customers—a larger proportion than those that identified either PEPs or foreign companies as being high risk. Businesses from the financial services sectors—such as banks and securities and derivatives businesses—were more likely to consider PEPs as high-risk customers than money service businesses or the non-financial businesses regulated in Australia. Financial services businesses were also more likely than money service businesses or non-financial businesses to consider foreign residents and foreign governments as posing higher risks as customers.

Perception of terrorism financing risks

Almost all of the study's participants (99.5%) considered the risks of terrorism financing to their businesses to be low in 2008–09 and more than 95 percent of respondents also anticipated that such risks would remain stable in the two year period to 30 June 2011. When respondents were asked to nominate the types of terrorism financing risks that their businesses might face in the two year period to 30 June 2011, just under 60 percent still indicated that their business faced little or no risks of terrorism financing. There was a relationship between business sector and perceptions of terrorism financing risk, with the proportions of respondents from different business sectors that identified no or low risks of terrorism financing ranging between 40 percent of foreign exchange businesses to 66 percent of financial services businesses. Only two participants from the entire sample reported believed high risks of terrorism financing might be affecting their businesses.

The perceptions of participants of higher risk customers also varied according to the business sector they occupied. Businesses from the financial services sector were more likely than money service businesses or non-financial businesses to select 'individuals' as higher risk customers in relation to terrorism financing.

Explaining these perceptions

The overwhelming view of survey participants was that their business faced few money laundering and terrorism financing risks. This opinion may have been based on the surveyed entities genuinely having faced few risks of either crime taking place. Alternatively, those surveyed may not have been in possession of adequate information to enable them to evaluate the level of risk that faced their business at the time. It may also be the case that the participants may have underestimated the true level of risk involved.

The current study offers some insight into the reasons why almost all of the participants in the study considered their business to be exposed to low risks of money laundering or terrorism financing. One view that emerged from the survey data was that the perception of there being very few money laundering and terrorism financing risks was directly linked to the size and core activities of the businesses involved. Smaller sized businesses felt they were insulated from ML/TF risks because owners and managers of small enterprises personally knew their customers and any new customer entering

the business would be immediately obvious to, and 'vetted' by, staff. Providing some support for this view is that almost all of the few money laundering cases that have been prosecuted in Australia that have involved small businesses have not involved unwitting involvement of personnel. Rather, these cases all involved complicit agreement by the business to participate in laundering the proceeds of crime. The Australian case examples that involved unwitting use of designated service providers had used large banks with multiple branches in order to structure deposits discreetly (see Box 1 and ACC 2011, AUSTRAC 2011b, AUSTRAC 2011c).

The feedback provided by interview participants from the gambling sector stressed that the small turnover that their businesses experienced from regulated services and the industry in which they operate were the two primary reasons for levels of money laundering risk being so low. These participants took the view that gaming machines offered little genuine opportunity to launder money or to launder large sums of money undetected. The limited opportunities afforded to any customer with the intention of laundering money would be further reduced in licensed premises that might only have one or two gaming machines. Any attempt to launder funds in such an environment would be immediately apparent.

Some of the interview participants considered that the nature of their customer base would make money laundering unlikely to occur and if it did, it would be identified. Smaller businesses, in particular, emphasised that owners and managers personally knew their customers and that any new customer entering the business would be immediately obvious to all staff and other clientele.

Another factor that may explain perceptions of low ML/TF risks was the self-described risk-averse culture of their businesses. In each case, the motivation for a highly risk-averse culture stemmed from inherent risks associated with the core activities of the business rather than from money laundering concerns. The cautious approach that these businesses adopted when dealing with new clients, combined with monitoring and modifying procedures, acted to diminish the opportunities for any clients to use their businesses to conduct illegal transactions.

It is apparent from the present research that perceptions of risk and confirmed cases of actual exploitation may not always coincide. AUSTRAC's (2010c) examination of 174 case studies and typologies published for the period 2007–10 found that money laundering offences, along with fraud offences, constituted the most prevalent form of criminal activity (26% each), while terrorism made up just one percent. The regulated industry sector most commonly used to launder money or transfer funds for the financing of terrorism—based on the sample of cases chosen in AUSTRACs typologies and case studies series—was the banking industry (45%; AUSTRAC 2010c), followed by alternative remittance services (18%) and gambling services (9%). Based on this evidence, it might be expected that representatives from these business sectors would perceive or experience a higher level of risk than other sectors in general (although it should be noted the survey in 2009 occurred in the early stages of AUSTRAC's typologies and case studies series).

However, in the current survey, the majority of survey respondents from the banking, remittance services and gambling sectors were no more likely than representatives of other surveyed industry sectors to report a higher perception money laundering or terrorism financing risk. They were also no more likely to predict an increased risk between 1 July 2009 and 30 June 2011, with the exception of providers of alternative remittance services.

In another AIC survey, respondents from law enforcement agencies considered that the risk of ML/TF to currently regulated sectors had not changed considerably since the implementation of the AML/CTF Act 2006 (Cth), although it had probably reduced for the banking sector and increased for alternative remittance service providers (Smith et al. forthcoming).

Exploring why business sectors that are implicated in confirmed cases of misuse do not have a higher risk perception might identify ways to close this gap and improve the effect of government guidance. Whether those sectors and industries regulated under AML/CTF actively use AUSTRAC and other government information to inform their risk programs could also be evaluated.

Compliance

Some relationship existed between the perceptions of reporting entities of risks and compliance activities, although there was no clear reduction in compliance from businesses that had low perceptions of risk. More than 85 percent of businesses conducted ongoing customer due diligence procedures. The compliance rate fell to 75 percent for pre-employment screening and 80 percent for KYC procedures. Relationships were found between the business sectors of participants and their likelihood of conducting each of these three compliance measures assessed in this survey. Businesses from the financial services sectors were more likely to conduct ongoing due diligence and KYC procedures than either money service businesses or non-financial businesses. Financial services businesses, such as banks, and cash delivery service providers were more likely than other participants to conduct pre-employment screening before hiring new staff.

The data revealed no statistically significant relationship between compliance with KYC requirements and the views of participants on money laundering risks to 2011. Those who perceived no money laundering risks were no less likely to comply than those who nominated some level of risk. There were relationships between respondents who nominated 'no risks' and those who conducted pre-employment screening and ongoing due diligence. Businesses that nominated 'no risks' were significantly less likely to conduct pre-employment screening and less likely to conduct ongoing due diligence.

More than 90 percent of the businesses that responded to the AML/CTF Australian businesses survey were small or micro businesses and many did not have AML/CTF regulatory obligations under the FTR Act (ie they were newly exposed to such obligations with the enactment of the AML/CTF Act 2006 (Cth)). It is arguable that within this context, some of the reporting entities surveyed experienced difficulties applying the risk-assessment procedures that formed the current basis of AML/CTF compliance in Australia. Comments from the small number of interviewees from small businesses in previously unregulated industries indicated a degree of difficulty in understanding the requirements of the regime, applying the logic of risk assessment as the basis of risk-based compliance and addressing those risks through customer due diligence and ongoing monitoring. Interviewees from industries that had previous exposure to AML/CTF regulation, other financial regulatory obligations, or extensive regulation for other areas of their business were better able to apply the concepts of a risk-based system and to identify the specific AML/CTF and other risks that their businesses might face. The relationship between the views of respondents on whether the Australian AML/CTF regime was too onerous and their business sectors might also suggest difficulties from within some industry sectors in complying with the regime.

Identifying and reporting suspicious transactions

The business sector of the participants also appeared to have an impact on the likelihood of each business identifying a suspicious matter. Banks, despite holding more restrictive views on over-reporting than other businesses, were those most likely to have identified a transaction suspected of being linked to money laundering in the year to 30 June 2009.

Most participants (70–80% depending on the scenario presented) disagreed or strongly disagreed that under-reporting of suspicious transactions to AUSTRAC was justifiable, even in situations where reporting might be thought to result in a loss of business, or where the business feared reprisals from such action. Over-reporting was also considered justifiable by the majority of respondents (50–70% depending on the scenario presented), although in each instance, the banking sector was the least likely to consider over-reporting justifiable. The results suggested that even as participants outside the banking sector were more inclined than not to report a suspicious matter, those in the banking sector were the most likely to encounter and to identify a suspicious matter.

Costs

Information on costs provided by survey respondents was also tied to, or affected by, the business sector respondents occupied. The reported compliance expenses across the entire sample ranged from no cost to $60m. The median expenditure across the entire sample was $1,000, with 57 percent of businesses reporting expenditure of $1,000 or less on AML/CTF compliance. Managed funds and superannuation businesses reported the highest median AML/CTF compliance costs at $6,000. Businesses from the foreign exchange sector and those classified as 'other' reported median costs below $500.

Approximately two-thirds of the sample expected their compliance costs to remain the same in the two year period to 30 June 2011. Seventy percent of participants who anticipated shifts in their compliance costs expected their expenses to increase by less than 50 percent. Participants ranked staff training and professional development, staff salaries and record keeping, monitoring and reporting as the most expensive areas of their compliance costs. The timing of the AML/CTF Australian businesses survey coincided with the period immediately after the full implementation of the AML/CTF Act 2006 (Cth) and hence some of the compliance cost estimates provided by respondents may refer to initial financial outlays that were not sustained into subsequent years. It is also possible that some of the systems changes required to address AML/CTF compliance were done in conjunction with other, general upgrades which may have temporarily inflated costs. The reported expenditure of participants for AML/CTF compliance in 2008–09 was associated with their views on whether the regime was too onerous. The likelihood of participants viewing the regime as being too onerous, however, did not directly increase with their costs. The participants who reported spending $1,000 or less were more likely to give neutral responses to the question of whether the regime was too onerous for the risks involved. Across the entire sample, around 28 percent of participants considered the regime to be too onerous, while approximately 25 percent disagreed that this was the case. Only one percent of respondents disagreed that the regime was too onerous as the low level of risk to their businesses meant compliance activities were kept to a minimum.

Attitudes towards the anti-money laundering/counter-terrorism financing regime

Participants held fairly positive views of the AML/CTF regime, despite the overwhelming perception that there were minimal risks of money laundering or terrorism financing to their businesses at the time. The survey's respondents considered the regime to be effective in deterring offenders, minimising the risks of financial crimes, minimising the risks of money laundering, minimising the risks of terrorism financing, maintaining the integrity of the financial system and promoting good governance practises. Respondents rated the regime as neither effective nor ineffective at facilitating proceeds of crime recoveries or minimising the risks of reputational damage. Those who considered the regime to be too onerous for the risks of ML/TF were also more likely to consider the regime to be less effective at minimising these risks.

Almost half of respondents agreed that the AML/CTF system would be improved if AUSTRAC were able to provide more AML/CTF training courses. Approximately one-third agreed that the system would be improved if AUSTRAC could provide more case studies and typologies. The businesses that participated in this study had a range of experiences with AUSTRAC and AUSTRAC's materials. Some businesses, predominantly those from industries with previous contact with financial and other forms of regulation, found AUSTRACs training documents integral to their employee training programs. Businesses from the financial services industries were more likely than money service businesses, or non-financial businesses, to suggest that the AML/CTF regime could be improved with more typologies and case studies being provided by AUSTRAC.

Conclusion

The AML/CTF Australian businesses survey was the first study to canvass the views of Australian regulated businesses on various aspects of complying with the AML/CTF regime. It attracted a large number of respondents drawn from all regulated sectors in

2009 and achieved an unusually high response rate for business surveys of this kind (50%). The findings provide a benchmark of how businesses in Australia understood their obligations in mid 2009, their views on the regime at the time and projections for the ensuing two years to 30 June 2011. Some of the principal findings are as follows.

Variations between business sectors in terms of compliance, costs and perceptions of risk were present throughout the results of the survey. The experience of businesses from the banking, securities and derivatives, managed funds and superannuation, and financial services sectors were quite different from those in the gambling sector, ARS providers, foreign exchange businesses, cash delivery sector and other businesses with regulatory obligations in key areas.

Generally, businesses without previous exposure to AML/CTF compliance were less likely to have used standard compliance measures and to report feeling confident in identifying suspicious transactions. Absence of prior exposure to AML/CTF compliance also led to these respondents to consider that the regime was too onerous relative to the risks present. While most respondents surveyed perceived the overall risk of money laundering or terrorism financing to their business to be low, some sectors from the newly regulated component of businesses were more likely to nominate a lower risk. The perception of the AML/CTF regime as being too onerous was less likely, however, to be associated with the costs involved. Most businesses reported spending $1,000 or less on AML/CTF compliance and the businesses from some of the newly integrated sectors spent even less.

An issue for the integrity of the system as a whole is that some of the business sectors (or some members of affected sectors) included in the regime—in order to create a more hostile environment to illicit transactions—reported experiencing difficulties in conducting risk assessments, implementing risk-appropriate measures and complying fully with the regulatory obligations in 2009. Gurung, Wijaya and Rao (2010) argued that all businesses may find interpreting and applying their AML/CTF regulatory obligations challenging, although financial institutions that had AML/CTF regulatory obligations prior to the 2006 Act were far better placed to become compliant with the current obligations because of their previous exposure to regulation in this field.

The Australian AML/CTF regime is risk based in the sense that regulated sectors are able to self-assess the ML/TF risk their business is exposed to and develop an appropriate compliance program to mitigate and manage this risks; reporting requirements are the same, irrespective of risk. While it was not entirely clear from the survey findings which components of the regime respondents found particularly onerous—the development and adherence to the business-specific risk mitigation program or compliance with mandatory reporting requirements—it is assumed from the responses that much of the difficulty was associated with the latter.

One of the core tenets of the risk-based system is to apply it appropriately to different business environments. One response to the findings may be the need to place greater emphasis on developing sector-specific education that will enable businesses to assess levels of risk more effectively and to create programs accordingly. An immediate response to assisting businesses without previous exposure to, or continuing difficulty with, AML/CTF regulatory requirements is through the provision of educational materials and training tailored to affected sectors. At the time the survey was undertaken, which coincided with the initial implementation of the AML/CTF Act 2006 (Cth), respondents suggested that sector-specific educative and training initiatives would assist them in better understanding and assessing the risk environment in which they operated, a central component of the risk-based AML/CTF system. The delivery of sector-specific education has been recommended in other AIC research on money laundering and terrorism financing risks; for example, providers of alternative remittance services (Rees 2010), non-financial sector businesses and professions suggested for inclusion under the second tranche of reforms and non-profit organisations (Bricknell et al. 2011).

In the period since the survey, AUSTRAC has made available a more extensive range of education, training and guidance materials for regulated entities that has included:

- generic and industry-specific guidelines regarding AML/CTF obligations;
- information brochure series on program procedures;

- risk-management tools to aid small and medium sized businesses in identifying, assessing and treating risk; and
- industry-specific engagement and supervisory strategies, comprising targeted education and awareness campaigns and guidance materials with a focus on sectors that have experienced difficulty in applying a risk-based approach to implementing AML/CTF programs;

These initiatives, along with the annual publication of typology reports, should have filled at least some of the educative gap survey respondents felt existed in 2009.

Limitations

The present survey was not without its limitations. Slightly over half of the survey's respondents came from the gambling sector and these tended to be smaller businesses within that sector. Businesses from the financial services sectors, such as banks, were under-represented. This may have influenced the results in situations where analysis was conducted across the entire sample rather than comparing the outcomes between business sectors. Small and micro-businesses comprised the majority of the sample, which may also have influenced the results obtained in the study. There was no publicly available information at the time of writing on the distribution of business size within the regulated sector, to determine whether the number of smaller businesses that responded were representative of the entire regulated sector.

The data analysis uncovered some inconsistencies in how businesses from the same industry identified their primary sources of revenue in the self-reported demographic information. This was particularly problematic for businesses providing a range of services, such as a general store operating as a post office while also providing remittance services.

In addition, and despite intensive pre-testing of the survey instrument and consultation with regulators (see Challice & Eliseo 2012), the language used in the questionnaire to describe some aspects of the AML/CTF regime in Australia proved inaccessible to some survey respondents. The language adopted in the questionnaire predominantly reflected the language used by AUSTRAC and in Australian legislation concerning AML/CTF-specific terms. Some survey respondents also highlighted problems understanding some of the terms in the questionnaire in their answers to open-ended questions.

Depending on the extent of participants' difficulty in understanding some of the key terms in the survey, the results may not have captured the views of businesses recently included in the regime to an appropriate extent. Analysis of the responses of the 50 percent of participants that elected not to complete the survey suggested that non-corporate businesses, such as pubs and clubs, post offices and retailers, were over-represented in this group. More than 70 percent of those that elected to not complete the survey agreed that the regime was too onerous (Challice & Eliseo 2012).

Finally, the survey findings reported here must be taken in the context that they were collected at the early stages of implementation of the AML/CTF regime. Initial trepidation about the costs of complying with the regime, among other concerns, may or may not have been borne out in the interim period. AUSTRAC's (2010d) Supervision Strategy for 2010–11 noted the agency's intention of conducting surveys across five industry sectors to gauge how well each sector has understood and implemented its AML/CTF obligations. If these subsequent findings are made available, they could be compared with responses collected in 2009 to determine if any changes or improvements have occurred in the regulated population's response to or capacity to comply with Australia's AML/CTF regime.

Directions for future research

Future studies of the opinions held by regulated businesses in this area and the methods and costs of compliance might seek to:

- replicate the survey and interviews to document changes in the ways businesses have viewed and applied the regime since 2009;
- replicate the survey to include all regulated businesses if the AML/CTF regime is expanded to include designated non-financial businesses and professions, such as legal practitioners, accountants and real estate agents;

- replicate the study in comparable countries to highlight differences and similarities in the self-reported risk profiles of different industries in different geographic locations; and
- conduct further and more detailed interviews with those in the regulated sectors and also with representatives of law enforcement, regulators and AUSTRAC's partner agencies that make use of the reported data.

References

All URLs were correct at July 2012

Australian Crime Commission (ACC) 2011. *Organised crime in Australia*. Canberra: ACC

Australian Crime Commission (ACC) 2010. Five and a half year sentence in major money laundering case. *Media release* 25 June. Canberra: ACC

Australian Crime Commission (ACC) 2009a. Eight sentenced in Australia's biggest money laundering investigation. *Media release* 17 December. Canberra: ACC

Australian Crime Commission (ACC) 2009b. Joint taskforce targets sentenced to imprisonment for money laundering and narcotics trafficking. *Media release* 15 October. Canberra: ACC

Attorney-General's Department 2009. *Second tranche reforms*. http://www.ag.gov.au/Antimoneylaundering/Pages/SecondTrancheofReforms.aspx

AUSTRAC 2011a. *AUSTRAC annual report 2010–11*. Canberra: AUSTRAC

AUSTRAC 2011b. *AUSTRAC typologies and case studies report 2011*. Canberra: AUSTRAC

AUSTRAC 2011c. *Money laundering in Australia 2011*. Canberra: AUSTRAC

AUSTRAC 2010a. *AML/CTF compliance officers in Australia*. AUSTRAC survey series no.1. Canberra: AUSTRAC

AUSTRAC 2010b. *AUSTRAC regulatory guide*. Canberra: AUSTRAC

AUSTRAC 2010c. *AUSTRAC typologies and case studies report 2010*. Canberra: AUSTRAC. http://www.austrac.gov.au/files/typ_rpt.pdf

AUSTRAC 2010d. *AUSTRAC supervision strategy 2010–11*. Canberra: AUSTRAC

AUSTRAC 2009a. *AUSTRAC annual report 2008–09*. Canberra: AUSTRAC

AUSTRAC 2009b. *AUSTRAC supervision strategy 2008–09*. Canberra: AUSTRAC

AUSTRAC 2009c. *Compliance reports 2009*. Canberra: AUSTRAC

AUSTRAC 2008. *AML/CTF programs*. Canberra: AUSTRAC

Bricknell S, McCusker R, Rees D & Chadwick H 2011. Money laundering and terrorism financing risks to Australia non-profit organisations. *Research and Public Policy series* no 114. Canberra: Australian Institute of Criminology

Chaikin D & Sharman J 2009. *Corruption and money laundering: A symbiotic relationship*. New York: Palgrave MacMillian

Challice G & Eliseo A 2012. Anti-money laundering and counter-terrorism financing study: Methodology report. *Technical and background series* no 46. Canberra: Australian Institute of Criminology

Choo K-KR 2010. Challenges in dealing with politically exposed persons. *Trends & Issues in Crime and Criminal Justice* no. 386. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/tandi/381-400/tandi386.aspx

Choo K-KR, Smith R, Walters J & Bricknell S forthcoming. Perceptions of money laundering and financing of terrorism in the Australian legal profession. Research and Public Policy series. Canberra: Australian Institute of Criminology

Commonwealth Director of Public Prosecutions (CDPP) 2011. *Annual report 2010–11*. Canberra: CDPP

Commonwealth Director of Public Prosecutions (CDPP) 2009. *Annual report 2008–09*. Canberra: CDPP

Ernst & Young 2007. *Anti-money laundering survey for the U.S.-based life insurance industry*. New York: Ernst & Young

Financial Action Taskforce (FATF) 2012. *International standards on combating money laundering and the financing of terrorism and proliferation.* Paris: FATF

Financial Action Task Force (FATF) 2007. *Guidance on the risk-based approach to combating money laundering and the financing of terrorism: High level principles and procedures*. Paris: OECD/FATF

Financial Action Task Force (FATF) 2005. *Third mutual evaluation report on anti-money laundering and the combating of financing of terrorism: Australia*. Paris: OECD/FATF

Gill M & Taylor G 2004. Preventing money laundering or obstructing business? Financial companies' perspectives on 'know your customer' procedures. *The British Journal of Criminology* 44(4): 582–94

Gurung J, Wijaya M & Rao A 2010. AMLCTF compliance and SMEs in Australia: A case study of the prepaid card industry. *Journal of Money Laundering Control* 13 (3): 184–201

Jensen N 2005. Technology and intelligence. *Journal of Money Laundering Control* 8(3): 227–42

Kini S 2006. Recent anti-money laundering enforcement actions: Lessons to be learnt at others' expense. *Journal of Investment Compliance* 7(3): 38–43

KPMG (India) 2009 *India anti-money laundering survey*. http://www.kpmg.com/IN/en/IssuesAndInsights/ArticlesPublications/Pages/IndiaAnti-MoneyLaunderingSurvey2009.aspx

KPMG (International) 2007 *Global anti-money laundering survey 2007: How banks are facing up to the challenge*. http://us.kpmg.com/microsite/FSLibraryDotCom/docs/AML2007FULL.pdf

PricewaterhouseCoopers 2007. *United Kingdom financial services industry anti-money laundering survey*. London: PricewaterhouseCoopers

Rees D 2010. Money laundering and terrorism financing risks posed by alternative remittance in Australia. *Research and Public Policy Series* no. 106. Canberra: Australian Institute of Criminology. http://aic.gov.au/publications/current%20series/rpp/100-120/rpp106.aspx

Ross S & Hannan M 2007. Money laundering regulation and risk-based decision-making. *Journal of Money Laundering Control* 10(1): 106–15

Sathye M 2008 Estimating the cost of compliance for AMLCTF for financial institutions in Australia. *Journal of Financial Crime* 15(4): 347–63

Sharman JC 2008. Power and discourse in policy diffusion: Anti-money laundering in developing states. *International Studies Quarterly* 52: 635–56

Smith RG et al. forthcoming. Australian anti-money laundering and counter-terrorism financing review, Special Report Series. Canberra: Australian Institute of Criminology

Smith R, McCusker R & Watlers J 2010. Financing of terrorism: Risks to Australia. *Trends & Issues in Crime and Criminal Justice* no. 394. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/tandi/381-400/tandi394.aspx

Smith RG & Walker J 2010. The illegal movement of cash and bearer negotiable instruments: Typologies and regulatory responses. *Trends & Issues in Crime and Criminal Justice* no. 402. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/tandi/401-420/tandi402.aspx

Veyder F 2003. Case study: Where is the risk in transaction monitoring? *Journal of Financial Regulation and Compliance* 11(4): 323–328

Walters J et al. 2012. Anti-money laundering and counter-terrorism financing across the globe: A comparative study of regulatory action. *Research and Public Policy Series* no. 113. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/rpp/100-120/rpp113.aspx

Appendix

Appendix

The AML/CTF legislation contains a number of definitions that are important to understand for present purposes. These include the following.

Remittance services (alternative remittance services)

Services involved in transmitting money or property, including informal systems or networks outside of the formal banking sector. A remittance arrangement is between persons who are not ADIs, banks, building societies, or credit unions.

Reporting entities

All financial institutions, money service businesses and designated non-financial businesses and professions, providing the designated services outlined in s 6 of the AML/CTF Act 2006 (Cth). Reporting entities may be collectively referred to as the regulated sector.

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.

Financial institutions may be ADIs, banks, building societies, credit unions, or other persons specified in the AML/CTF Rules.

Designated non-financial businesses and professions

Businesses, outside of the financial and money service business sectors, offering a service outlined in s 6 of the AML/CTF Act. The DNFBPs identified by FATF 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.

Bullion dealers are currently the only DNFBPs providing a designated service in Australia.

Financial Intelligence Unit

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 of 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.

AIC Reports
Research and Public Policy Series 117

In Australia, legislation was introduced in 2006 that requires specified businesses to forward reports of certain financial transactions to the Australian Government agency, AUSTRAC. As part of the Australian Institute of Criminology's research in to Australia's anti-money laundering/counter-terrorism financing regime, a survey was conducted in mid 2009 of all business with reporting obligations to AUSTRAC. This report examines the findings of the survey on the perceptions of Australian businesses to the reporting regime in Australia.

Australia's national research and
knowledge centre on crime and justice

www.aic.gov.au