Australian Government

Australian Transaction Reports and Analysis Centre

Australian Government

Attorney-General's Department

Consideration of possible enhancements to the requirements for customer due diligence

Discussion paper

May 2013

Table of contents

Table of contents **2**
Glossary of terms **3**
Purpose of this paper **4**
Structure of the paper 5
Consultation process 5
Next steps 6
Part 1 ..... **7**
Introduction **7**
Government policy on AML/CTF 9
What is customer due diligence (CDD)? 10
Why reform? – Potential areas of cost and benefit 11
Keeping up with evolving threats 11
Keeping Australian businesses competitive on the global economic stage 12
Industry practice – toward an enhanced understanding of risks 14
Part 2 ..... **15**
Summary of potential reforms **15**
Ownership and control 15
Situations where a customer is acting on behalf of a person 15
Settlor of a trust 16
Enhanced customer due diligence and politically exposed persons (PEPs) 16
Purpose of business relationship 16
CDD records 16
Part 3 ..... **30**
Options to minimise regulatory burden associated with the potential reforms **30**
Exemptions for low-risk situations 30
Customer self-attestation 31
Reliance on third-party due diligence 31
Supporting infrastructure 32
Simplified due diligence (SDD) 32
Transitional arrangements 33
Attachment 1: FATF Recommendation 10 – Customer Due Diligence **34**
CUSTOMER DUE DILIGENCE AND RECORD KEEPING 34
10. Customer due diligence 34
INTERPRETIVE NOTE TO RECOMMENDATION 10 (CUSTOMER DUE DILIGENCE) 35
A. CUSTOMER DUE DILIGENCE AND TIPPING OFF 35
B. CDD – PERSONS ACTING ON BEHALF OF A CUSTOMER 35
C. CDD FOR LEGAL PERSONS AND ARRANGEMENTS 36
D. CDD FOR BENEFICIARIES OF LIFE INSURANCE POLICIES 37
E. RELIANCE ON IDENTIFICATION AND VERIFICATION ALREADY PERFORMED 37
F. TIMING OF VERIFICATION 38
G. EXISTING CUSTOMERS 38
H. RISK-BASED APPROACH 38

Glossary of terms

Term	Definition
Anti-money laundering and counter-terrorism financing (AML/CTF) regime	The *Financial Transaction Reports Act 1988* (FTR Act), *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act), *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No.1)* (AML/CTF Rules), Regulations and guidance, including the supervisory systems.
Beneficial ownership and control	The natural person who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It includes those persons who exercise effective control over a legal person or arrangement.
Customer due diligence (CDD) measures	Measures taken to know and understand a customer and related beneficial owner(s), including the identification and verification of their identity.
Financial Action Task Force (FATF)	The Financial Action Task Force is the key international inter-governmental body that sets and monitors the implementation of the international standards for anti-money laundering, counter-terrorism financing and combating the financing of the proliferation of global weapons of mass destruction.
Legal arrangement	A FATF term which refers to a trust or other similar legal arrangement.
Legal person	A FATF term which refers to any entity other than a natural person that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include a company, body corporate, foundation, partnership, or association and other relevantly similar entity.
Money laundering	Money laundering is the processes by which the criminal origins of the proceeds of crime are concealed, and the proceeds of crime can be spent or invested in the legitimate economy.
Politically exposed persons (PEPs)	Politically exposed persons are individuals who occupy, or have occupied, prominent public positions, including prominent positions in international organisations, both within and outside Australia (or their close family or associates).
Reporting entities	The businesses on which the AML/CTF regime places regulatory obligations because the businesses provide designated services.
Third-party reliance	The AML/CTF Act allows reporting entities to rely on the customer due diligence checks performed by some other businesses, where a range of conditions are met.
Terrorism financing	The financing of terrorist acts, and of terrorists and terrorist organisations.

Purpose of this paper

The purpose of this paper is to seek stakeholder views on current industry practice and the need for, and costs and benefits of, amendments to Australia's anti-money laundering and counter-terrorism financing (AML/CTF) customer due diligence (CDD) regime.

Money laundering is the lifeblood of organised crime and is a significant risk to Australia's prosperity. Organised crime costs the Australian economy more than $15 billion per year. Money laundering is a transnational crime that threatens the integrity of our financial system and funds criminal activity, including terrorism, which impacts on community safety and wellbeing. Australia is a founding member of the Financial Action Task Force (FATF) which sets the international standards on combating money laundering and the financing of terrorism through the FATF Recommendations. The FATF plays an important role in ensuring that an internationally coordinated approach prevents criminals from exploiting vulnerabilities arising from differences between the laws of different jurisdictions.

In February 2012, the FATF released revised international standards on AML/CTF that clarify existing CDD obligations. The Australian Government is considering the implications of the revised standards for Australia's existing regime, particularly in relation to CDD obligations as this is an area where the Australian regime has been identified as not meeting the standards. Other countries around the world, including the United States and Canada, have also taken into account the revised standards in shaping CDD obligations under their AML/CTF regimes.

This consultation paper outlines the latest international standard on CDD and explains the purpose of the standard. It considers whether Australia's AML/CTF regime could benefit from adopting the standard and seeks views on some possible ways to closer align Australia with the standard. The paper explores early options with a view to obtaining a preliminary understanding of the costs and benefits of reform in this area. The options discussed are not intended to limit consideration of this issue, but rather to facilitate the consultation process, and so stakeholders are also encouraged to provide options or ideas.

We formally invite industry and other stakeholders to provide their experiences, opinions and information on:

- current practices, including if and how the international standards are already being met
- any possible additional measures that may be required in order to meet the international standards
- any possible measures to simplify CDD obligations
- the costs associated with compliance with the standards, and
- the benefits of compliance with the standards.

The Government is especially interested in hearing industry stakeholder views on current practices and the impact of any clarifying measures that may be considered. Respondents should also feel free to raise any issues they see as relevant.

The Government recognises that any change has the potential to impact on industry, particularly small businesses. Effective CDD remains the overarching objective and any potential changes would not impose new obligations in that respect. However, these potential

changes would clarify and codify current expectations of how regulated businesses undertake CDD, which may, in practice, result in regulated businesses collecting additional information.

Information provided through this consultation process will enable the Government to consider how Australia's system can be strengthened and to more fully appreciate the costs and benefits of reform to industry and other stakeholders. It will also enable Government to consider how existing industry practice could be leveraged in the design of any reforms to minimise any regulatory burden. The Government appreciates that a 'one size fits all' approach may not be the most appropriate and strongly encourages all stakeholders to provide their views. The Government is committed to ensuring that any potential reforms strike an appropriate balance with privacy considerations, and further invites stakeholders to provide their views on privacy matters related to these possible reforms.

It is anticipated that any potential reforms could be achieved through modification of the existing AML/CTF Rules, complemented by supporting guidance. If, after consultation with stakeholders, amendments to the AML/CTF Act are required, this would be subject to a separate legislative process. Suggestions on the approach and characteristics of any potential amendments are also welcome.

Structure of the paper

Part 1 provides context and highlights relevant domestic and international factors.

Part 2 outlines possible areas for reform. Each area for possible reform includes analysis of the underlying AML/CTF concern. A summary of the identified deficiencies and potential areas for reform is provided at Table 1.

Part 3 outlines possible methods for minimising any additional costs arising from possible reforms. The Government welcomes comments on these options as well as other suggestions.

Specific questions are included throughout this consultation paper to guide discussion. These questions are not intended to limit comment.

Attachments to this discussion paper provide more detail on the relevant FATF international standards referred to throughout the paper.

Consultation process

If you would like to make a submission, please send it to:

Discussion Paper – Customer Due Diligence Reform
International Policy
Legal and Policy Branch
AUSTRAC
PO Box 5516
West Chatswood NSW 1515

Submissions may also be submitted by email to <CDD_Consultation@austrac.gov.au> or by facsimile to (02) 9950 0054.

The closing date for submissions is **30 September 2013.**

All submissions and the names of persons or organisations that make a submission will be treated as public and may be published on AUSTRAC's website, unless the author clearly indicates to the contrary. A request made under the *Freedom of Information Act 1982* for access to a submission marked confidential will be determined in accordance with that Act.

All submissions will be reviewed by the Attorney-General's Department (AGD) and AUSTRAC.

Next steps

Following receipt and review of submissions, the Government will consider the issues raised. If the Government considers that amendments to the CDD regime are desirable and can be achieved through the AUSTRAC CEO's formal rule-making powers, formal draft AML/CTF Rules will be provided to industry through AUSTRAC's normal consultation process for Rules.

There will be further consultation throughout the process to ensure stakeholders' views and the costs and benefits of reform are fully understood and taken into account. The key obligation for reporting entities remains effective CDD and any potential changes would not impose new obligations in that respect. However any changes may, in practice, result in regulated businesses collecting additional information. As such, the regulatory and privacy impact of any changes will be considered further once the approach is finalised.

Part 1

Introduction

Organised crime is big business. A recent United Nations Office of Drugs and Crime report estimates the annual income of organised crime in Asia and the Pacific at nearly 90 billion USD. Organised crime poses a sophisticated threat to Australian businesses and industry. Money laundering is an evolving threat as criminals adapt to sidestep regulatory and law enforcement measures and exploit market and technology developments. Government and industry must remain vigilant and continue to enhance Australia's AML/CTF regime if it is to remain effective.

The revised 2012 FATF Standards were a direct response to a call by the G20 to update and implement AML/CTF standards relating to customer due diligence and transparency of beneficial ownership. This call was made to take steps to address the increasing number of high profile cases involving the use of legal entities and complex legal structures to hide the true ownership and control of those entities. In Australia, Project Wickenby has provided numerous examples of the abuse of complex legal structures for tax evasion purposes.

Australia is recognised internationally as having a robust AML/CTF regime. The legislative authority and direction is provided by the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act), the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No.1)* (the AML/CTF Rules) and the *Financial Transaction Reports Act 1988* (FTR Act). The AML/CTF regime provides a comprehensive legal framework designed to ensure that Australia's financial system is hostile to money laundering and terrorism financing, and helps to protect Australia, its people and financial institutions against abuse from criminal activity.

However, FATF has identified a number of deficiencies in Australia's regulatory obligations. These deficiencies highlight shortcomings in the efficacy of Australia's current regime. The possible reforms outlined in Part 2 of this paper are aimed at potentially addressing the identified shortcomings, particularly in relation to CDD measures that must be undertaken by reporting entities. The potential reforms would not introduce any new concepts or obligations, but would clarify and codify existing expectations of the CDD required to be undertaken by regulated businesses to understand their risks. The potential reforms would allow reporting entities to better understand and mitigate the full range of risks associated with commencing or continuing business relations with their customers, and would foster greater consistency in the application of CDD preventative measures across the regulated population. Information provided by stakeholders on current practices will allow the Australian Government to consider whether Australia's AML/CTF regime is achieving its original objectives with respect to CDD.

Reporting entities benefit from a strong AML/CTF regime that protects their businesses from criminal abuse, and associated commercial fraud and reputational risks. For many businesses, preventative AML/CTF measures including strong CDD are an integral component of their wider risk management programs. Obtaining a sound understanding of a customer's business, ownership and control structures also provides reporting entities with added opportunity to identify and maximise potential opportunities to meet their customers' needs.

Sound CDD measures improve the quality of information that can be provided to agencies such as AUSTRAC and other law enforcement agencies. Better quality reporting allows law enforcement to identify and investigate potential money laundering, terrorism financing and

other serious crime. Improved reporting generated by strong CDD processes also enables law enforcement and regulatory agencies to provide reporting entities with better feedback as to emerging criminal trends and risks. This information may particularly benefit smaller reporting entities that may not have the resources or analytical capabilities to identify these trends independently. This will help make the small business and others sectors less vulnerable to criminal abuse and increase public confidence in the integrity of the financial, gambling and remittance sectors. Additionally, criminals seeking to operate in Australia may be hesitant to commit resources and money if they are likely to face greater scrutiny.

The conduct of international business relationships depends on the assessment of the strength and effectiveness of Australia's AML/CTF regime by the international community and business counterparts. Global corporations and foreign investors, when looking to establish operations in Australia, pay close attention to Australia's approach to meeting international regulatory standards. Knowing that the AML/CTF standards in Australia meet FATF requirements provides assurance as to the integrity, stability and security of doing business with Australian institutions.

Similarly, maintaining a sound reputation as to the strength of Australia's AML/CTF regime provides advantages to Australian businesses that operate in overseas jurisdictions.

Government policy on AML/CTF

Australia is a long-term advocate in the Asia-Pacific region and globally for the effective implementation of the FATF AML/CTF standards.

The Government is committed to ensuring that Australia maintains a strong AML/CTF framework that:

(i) minimises the risk of money laundering (ML) and terrorism financing (TF) in the Australian economy

(ii) supports domestic and international efforts to combat organised crime, corruption and terrorism

(iii) does not impose an unnecessary burden on Australian business, and

(iv) is consistent with the internationally endorsed FATF AML/CTF standards in combating money laundering and terrorism financing.

The Government recognises the valuable ongoing support of reporting entities in achieving these objectives.

As Australia's AML/CTF regulator and financial intelligence unit (FIU), AUSTRAC, together with the Attorney-General's Department and other government agencies, is committed to maintaining the effectiveness of Australia's AML/CTF regime. AUSTRAC continues to work with reporting entities to ensure that the regulatory measures in place are effective and proportionate to the risks they face. The Government recognises this is particularly important in relation to smaller reporting entities to ensure that the regulatory regime is not unduly onerous.

A statutory review of the AML/CTF Act is required to commence by December 2013. However, given the significance of CDD measures to the effectiveness of Australia's AML/CTF regime and international concern regarding Australia's current approach, it is appropriate that reforms to amend existing CDD obligations be considered in advance of any wider review of the operation of the legislative framework. As noted below, examining this issue now will also assist in identifying opportunities for harmonisation with the work currently being undertaken by those reporting entities that are subject to the United States Foreign Account Tax Compliance Act (FATCA).

What is customer due diligence (CDD)?

CDD is a fundamental part of an effective AML/CTF regime. Reporting entities must know and understand their customers if they are to be sufficiently informed to determine the risk posed by each customer, whether to proceed with the business relationship or transaction, and the level of future monitoring required.

The FATF standards require reporting entities[1] to:

1. understand who is the customer
2. understand who owns and controls the customer – this includes the beneficial ownership and control structures
3. understand the purpose and intended business relationship of the customer, and
4. conduct ongoing due diligence of the business relationship – including scrutiny of transactions involving that customer (on the basis of the risk assessed in steps 1 to 3 above).

In order to achieve this understanding, the FATF standards require reporting entities to identify and verify their customers, identify the natural person(s) that have beneficial ownership or control of these customers, and use reasonable measures to verify the beneficial ownership and control information.

In Australia, the AML/CTF Act and Rules set a minimum baseline for reporting entities to know their customers and beneficial owners.

Currently reporting entities must have in place AML/CTF programs to identify, mitigate and manage risks that a designated service it provides may involve or facilitate money laundering or terrorism financing. Before providing a service, reporting entities are required to have appropriate CDD programs in place to:

- enable them to 'know their customers' (KYC)
- perform ongoing customer due diligence
- monitor transactions, and
- report suspicious matters to AUSTRAC.

Such measures are to be applied in a manner that is proportionate to the money laundering or terrorism financing risk.

The AML/CTF Act and AML/CTF Rules seek to implement a risk-based approach to AML/CTF and to CDD, in line with FATF principles. The risk-based approach requires a reporting entity to assess and determine the level of risk associated with a customer. The risk profile is developed in part based on the customer type, the potential designated service and

[1] The FATF standards apply generically to financial institutions and non-financial businesses and professions. The equivalent term in Australia is 'reporting entities'.

product being offered, the nature of the customer's business and the geographic location of the customer.

The risk-based approach allows reporting entities to effectively target their resources by assessing the money laundering and terrorism financing risks associated with their services and enabling the use of proportionate measures to mitigate those risks.

Why reform? – Potential areas of cost and benefit

Keeping up with evolving threats

By their nature, money laundering and terrorism financing are evolving crimes. Criminals continue to search for gaps in the existing AML/CTF framework, and seek alternative ways to process and disguise the funds associated with their criminal activities. Government and industry must remain vigilant and continue to enhance Australia's AML/CTF regime if it is to remain effective.

The 2011 Australian Crime Commission (ACC) Organised Crime Threat Assessment identified money laundering as one of the three critical risks facing Australia and a crucial enabler of organised crime. Organised crime is conservatively estimated to cost Australia $10–15 billion each year. The ACC considered that money laundering was a threat to Australia's national security and prosperity with the potential to undermine the integrity of the Australian financial system.[2]

Further, the *Money Laundering in Australia 2011* report provided a consolidated picture of money laundering, including key threats and vulnerabilities. The report highlighted concerns with the lack of transparency of the beneficial ownership of legal persons and arrangements.[3]

Recent Australian examples demonstrating the abuse of legal structures for illicit purposes include case studies from Project Wickenby. Project Wickenby uncovered the abuse of complex legal structures involving chains of company ownership, trusts and other corporate entities to hide the true ownership of funds for tax evasion purposes. A further example is the Firepower scandal, in which funds derived from one of Australia's largest frauds were hidden in legal structures in offshore jurisdictions. These funds were ultimately unable to be traced or recovered.

Australia's regime needs to continue to evolve to effectively address identified vulnerabilities. Without measures to increase the transparency of beneficial ownership, criminals and terrorists will be able to continue to abuse legal structures to aid money laundering or terrorism financing.

Increased levels of money laundering and terrorism financing abuse have the potential to distort markets creating illegitimate competitive advantage. This can be particularly damaging for smaller businesses trying to compete in these markets. Increased money

---

[2] *Organised Crime in Australia 2011*, report of the Australian Crime Commission, available at: <www.crimecommission.gov.au>

[3] *Money Laundering in Australia 2011*, AUSTRAC, 2011, available at: <www.austrac.gov.au/money_laundering_in_australia_2011.html>

laundering and terrorism financing abuse also damages Australia's international reputation and increases the cost of business.

Customer due diligence and reporting by businesses, including small businesses, is critical to enabling the detection, investigation and prosecution of offences and protecting the Australian financial system, revenue base and national security interests. Regulated businesses are best placed to assess their money laundering risks. To properly assess these risks, businesses need a full understanding of their customers.

Keeping Australian businesses competitive on the global economic stage

FATF criticisms and implications for business

The FATF is the global standard setter for AML/CTF regulation. The FATF plays an important role in coordinating an international approach that ensures that criminals cannot exploit vulnerabilities arising from differences between the laws of different jurisdictions. Over 180 countries around the world have undertaken to implement the FATF standards. The FATF standards include a requirement for countries to consider the level of risk posed by other jurisdictions. Regulated entities are to apply a higher level of due diligence when dealing with businesses from countries which have been identified by the FATF as having deficiencies in their AML/CTF regimes.

The FATF evaluated Australia's implementation of the international AML/CTF standards (the FATF standards) in 2005. That evaluation found that Australia's AML/CTF regime contained key deficiencies in respect of our CDD obligations. Certain core measures have not been explicitly (or fully) addressed in our legislative framework. In some instances, reporting entities are provided with too much discretion in addressing these mandatory obligations; for example, the need to gain an appropriate understanding of the beneficial ownership, control and nature of business of their customers.

Australia is not alone in reconsidering its approach to CDD obligations in light of the FATF Recommendations. As the internationally accepted AML/CTF standards, many of our major trading partners, including the United States and Canada, have taken measures, or are in the process of implementing measures, to ensure that their businesses understand who owns and controls their customers.

If the deficiencies are not rectified, Australia's reputation for having a strong and effective AML/CTF regime will be adversely affected. Such judgments can have adverse commercial and reputational implications, including the potential to:

- undermine the soundness and stability of financial institutions
- discourage legitimate foreign investment
- distort capital flows
- increase the cost of doing business, and
- increase Australia's vulnerability to serious and organised crime, corruption and terrorism.

A practical example of the adverse impact on business that could flow from ongoing non-compliance with the FATF standards is the potential for Australia to be removed from the European Union (EU) Equivalence List. This list enables EU regulated entities to apply simplified due diligence measures when dealing with industry in listed countries. Australia is currently one of twelve countries on the list. The EU considers countries' compliance with the FATF standards in maintaining the list Removal from this list would mean that Australian businesses operating in the EU would be subject to more stringent due diligence measures and therefore increased transaction costs. Removal from the EU Equivalence List has impacted on countries' international reputation and economic competitiveness. These impacts are not limited to businesses directly participating in international markets as costs may be passed downstream to small businesses and other customers in the course of transactions.

The views of other international bodies including the G20 and the United Nations

The international community, including the G20 and the United Nations, are increasingly focused on improving the transparency of legal entities in order to combat crime and corruption. Cases involving the international transfer of assets by corrupt political leaders have highlighted vulnerabilities in the financial system where legal entities have been used to obscure beneficial ownership. These cases have led to reputational damage and regulatory sanctions for the reporting entities involved.

It is widely recognised that strong and effective CDD measures are an integral element to addressing beneficial ownership vulnerabilities. Australia will assume the G20 Presidency in 2014 and these potential amendments are important to meeting our obligations under the G20 Anti-Corruption Action Plan. The G20 and the FATF are closely linked. The 2009 Pittsburgh G20 Leaders' Statement called on the FATF to prioritise work to revise standards on CDD, beneficial ownership and transparency. In response to the G20's call, the FATF revised its standards in February 2012, including the requirements in relation to customer due diligence on beneficial ownership. The revision of the FATF Standards was welcomed by the 2012 Los Cabos G20 Leaders' Statement. When considering addressing Australia's FATF-identified deficiencies, it is important to incorporate the revised FATF standards, which clarify CDD obligations, ensuring that all countries are implementing the expected requirements.

The United States' FATCA and implications for business

The United States (US) Foreign Account Tax Compliance Act (FATCA) will require Australian financial institutions to report certain information to the US Internal Revenue Service (IRS) about customer accounts held by US taxpayers. The Australian Government is currently negotiating an intergovernmental agreement (IGA) with the US Government to facilitate Australian financial institutions' compliance with FATCA in a manner consistent with Australian law. The proposed IGA will allow Australian institutions' FATCA obligations to be met by reporting the required information to the Australian Taxation Office (ATO), which will pass on the information to the IRS under existing tax information sharing arrangements. To fulfil FATCA obligations, Australian institutions will need to identify their US customers, including beneficial owners. In the absence of an Australian-US IGA, failure to comply with FATCA's requirements would expose Australian financial institutions to a 30% withholding tax on their US source income.

Enhancements to Australia's CDD regime would enable financial institutions to establish more robust beneficial ownership identification and verification practices. It is expected that

financial institutions would be able to leverage these practices to assist in complying with their FATCA obligations under the proposed Australia-US IGA.[4]

Industry practice – toward an enhanced understanding of risks

Australia's current regulatory CDD obligations in some instances do not require, and in others are not sufficiently explicit in obliging, reporting entities to undertake certain core CDD measures. For example, it is left to the discretion of reporting entities whether to undertake further checks in order to understand the beneficial ownership of a non-corporate customer, whereas the FATF standards require that a reporting entity **must** undertake checks to be fully informed of the risks associated with their customers.

This discretion has, in part, led to variable practice across the regulated sector. Such inconsistency has the potential to create cost and competitive distortions between reporting entities that provide similar designated services.

The Government is aware that examples exist of the potential reforms outlined in Part 2 of this paper already being undertaken by a range of reporting entities to meet other business, regulatory and overall risk management imperatives. For example, a reporting entity which is a subsidiary or affiliate of an international group may be required by its parent company to have in place a more stringent CDD program to meet the requirements of its parent company's global AML/CTF program. Such entities should be well placed to readily implement the potential reforms.

Government also recognises that many reporting entities are not undertaking CDD measures beyond the minimum threshold mandated by the AML/CTF regime. Although technically compliant in meeting their existing regulatory obligations, such reporting entities may be limited in their ability to understand the full spectrum of the risks presented by their customers. This leaves their business more vulnerable to exploitation and abuse by criminal elements.

The Government recognises the possible impact of reform on small business. Certain reporting entities, such as those in the gambling and alternative remittance sectors, are not expected to be significantly affected by the possible reforms outlined in this paper. Designated services provided by these sectors cater primarily to individual clients and should not, as a matter of course, give rise to additional regulatory impact. However, to the extent that these sectors have corporate clients, these reforms could entail a regulatory impact. A focus of the consultation process will be on measures that could be taken to mitigate the regulatory impact on these smaller entities. The Government is also willing to consider measures that will assist small business in dealing with regulatory change.

[4] The institution must, as part of the processes of confirming whether the customer is a US taxpayer, rely on its AML procedures to identify and verify the beneficial ownership and, in certain cases, the control structures of its US customers.

Part 2

Summary of potential reforms

This section of the paper discusses in detail technical concepts and obligations that clarify existing expectations. It also offers suggestions on a mechanism to enhance CDD obligations required to be undertaken by regulated businesses to understand their risks.

Table 1 – Summary of Australia's deficiencies and associated potential reforms

Ownership and control		
	The deficiency	**The potential reform to address the deficiency**
1	***Requirements for beneficial ownership and control***	
	The obligation on reporting entities to determine the beneficial ownership and control structures of customers is inadequate and inconsistent with the FATF standards because: ▪ there is no provision for a reporting entity to understand the 'control structures' of a customer ▪ there is no requirement for a reporting entity to collect information on the powers that bind the legal person (e.g. company) or legal arrangement (e.g. trust).	It is possible to extend the definition in the AML/CTF Rules of beneficial ownership of all customers to explicitly introduce a concept of 'control'.
2	***Requirements for beneficial ownership and control***	
	There is no explicit requirement for a reporting entity to identify and take reasonable measures to verify the beneficial ownership and control of its customers.	It is possible to amend the AML/CTF Rules to explicitly require reporting entities to: ▪ identify and take reasonable steps to verify the identity of beneficial owners for all categories of customer that are legal persons or legal arrangements, and ▪ clarify that the term 'beneficial owner' means the natural person(s) (individual(s)) who ultimately owns or controls a customer.
3	***Situations where a customer is acting on behalf of a person***	
	The AML/CTF regime does not require a reporting entity to determine whether a customer, who is a natural person, is acting on behalf of another person and, if so, to take reasonable steps and apply adequate measures to verify the identity of that other person.	It is possible to amend the AML/CTF Rules to explicitly require a reporting entity to take appropriate steps to: ▪ determine whether the customer is conducting a transaction on behalf of another person or third party, and accordingly ▪ identify the beneficiaries and the destination of the transaction.

4	***Settlor of a trust***	
	Where a reporting entity is dealing with a customer that falls under the category of a legal arrangement (e.g. trust), there is no explicit requirement under the AML/CTF regime to identify and verify the settlor of a trust.	It is possible to amend the AML/CTF Rules to explicitly require a reporting entity to identify and verify the settlor of a trust.
5	***Enhanced customer due diligence and politically exposed persons (PEPs)***	
	The AML/CTF regime does not provide sufficient clarity on the application of enhanced customer due diligence measures where a reporting entity has a high-risk situation. The AML/CTF regime does not contain an obligation for a reporting entity to apply enhanced customer due diligence measures where a customer is classified as a politically exposed person (PEP).	It is possible to amend the AML/CTF Rules to: ▪ define the meaning of politically exposed person ▪ require reporting entities to introduce appropriate risk-based controls to identify whether their customer (and beneficial owners) may be a foreign, domestic or international organisation PEP ▪ include provision for the conduct of explicit enhanced CDD measures where the customer is a PEP, and ▪ prescribe specific measures to be taken to perform a range of enhanced CDD measures for high-risk situations.
6	***Purpose of business relationship***	
	There is no explicit requirement for a reporting entity to consider and understand the purpose and nature of the business relationship with the customer.	It is possible to amend the AML/CTF Rules to include an explicit requirement that Part A of a reporting entity's AML/CTF program must include appropriate risk-based systems and controls to ensure that the reporting entity has a reasonable understanding of the nature of the customer's business or occupation.
7	***CDD records***	
	The AML/CTF Act does not place a general obligation on reporting entities to keep CDD information up to date, regardless of the ML/TF risk assessed for a customer.	It is possible to introduce a general obligation for reporting entities to keep CDD information up to date and relevant, and that risk-based systems be used to determine what CDD information should updated or verified and at what intervals. The scope of CDD information to also reflect additional requirements of the potential reforms outlined in this paper.

Potential reforms to strengthen CDD requirements

Ownership and control

The two components to this deficiency are detailed at items 1 and 2 below.

Deficiency 1: There is no requirement to take reasonable measures to understand the control structure of a customer that is a legal person or arrangement.

The obligation on reporting entities to determine the ownership and control structure of such customers is inadequate and inconsistent with the FATF standards. There is no mandatory requirement for a reporting entity to:

- understand the 'control structure' of a customer. For example, whether the customer is a subsidiary of another entity and the organisation and management structure of the customer, and
- collect information on the powers that bind the legal person (e.g. company) or legal arrangement (e.g. trust). For example, for a company this would be the memorandum and articles of association.

The AML/CTF Rules set out the customer identification requirements for companies (domestic and foreign) and varying forms of legal arrangement. The AML/CTF Rules specify what minimum information must be collected and verified in relation to the existence and control structure of legal persons or arrangements.

Table 2 below sets out the minimum information to be collected for various non-individual customer types:

Table 2 – Summary information required currently under the AML/CTF Rules to be collected for entities

Type of entity	Required information
Companies	• existence of company • name of each director
Trust	• existence of trust • name of each trustee and beneficiary, or a description of each class of beneficiary
Partnership	• existence of partnership • name of each of the partners

Association (incorporated or unincorporated)	• existence of association • names of any members of the governing committee (however described)
Registered cooperative	• existence of registered cooperative • names of the chairman, secretary and/or equivalent officer
Government body	• existence of government body • for foreign government bodies – beneficial ownership (KYC information about the ownership or control) if sought by the reporting entity

Under the AML/CTF Rules reporting entities **may** obtain additional information if they consider that such information is warranted by their risk assessment of the customer. However, to fully understand the risks presented by a customer, a reporting entity needs to also understand the control structure of a customer (legal person or arrangement). The FATF standards consider access to such information to be an essential part of the CDD and risk assessment processes. While customer ownership and control is more likely to be an issue for businesses that routinely engage in complex corporate transactions, small businesses are not immune from such risks, which may in some circumstances, under existing legislation, trigger suspicious matter reporting obligations. It is important that all businesses are able to form an accurate assessment of the risks associated with a customer's ownership or control.

Potential reforms

An option is that the AML/CTF Rules be amended to require a reporting entity, regardless of the level of perceived risk, to collect the following information from customers:

- the powers that regulate and bind the customer which would include, but not be limited to:
    - the memorandum and articles of association for a company
    - in the case of a partnership, a copy of the partnership agreement
    - in the case of a trust, the trust deed, and
    - the constitution of an incorporated association, and/or
- the management and organisation structure of the customer including the names and the positions held.

Furthermore, the requirement could extend to all categories of legal persons and legal arrangements.

Questions

1. To what extent are reporting entities already assessing the concept of 'control' as part of the beneficial ownership procedures and what information is being sourced from customers?

2. To what extent are reporting entities obtaining and verifying information on the powers that bind a customer?

Deficiency 2: There is no comprehensive requirement to identify and verify beneficial owners of a customer that is a legal person or arrangement.

The obligation on reporting entities to understand the identity of their customers' beneficial ownership and control is inadequate and inconsistent with best practice and the FATF standards. In particular:

- reporting entities are not required to identify the beneficial owner for customers that are legal persons or legal arrangements, other than for certain types of companies[5]
- reporting entities are not required to take reasonable measures to verify beneficial ownership information
- the requirement to identify beneficial ownership in respect of companies does not include the concept of 'control'
- it is unclear whether there is a requirement to look beyond the first layer of beneficial ownership (this has resulted in an inconsistent approach across the regulated sector), and
- there is confusion regarding the terms 'ultimate beneficial ownership' and 'beneficial ownership'.[6]

[5] The AML/CTF Rules require reporting entities to collect (identify) the name and address of beneficial owners of proprietary or private companies (except where proprietary companies are licensed and subject to regulatory oversight of a Commonwealth, state or territory statutory regulator in relation to its company activities). Verification is discretionary, based on assessment of the ML/TF risk relevant to the provision of the designated service.

[6] The definition of 'ultimate beneficial ownership', while including the concept of control, only applies to enhanced customer due diligence requirements in Chapter 15 of the AML/CTF Rules, not to other identification rules (e.g. Chapter 1 – Introduction and Key Terms and Concepts).

Under the AML/CTF Rules a reporting entity is only required to confirm the existence of the customer and undertake the collection and verification of certain prescribed information on the customer. This information varies depending on whether the customer is a legal person or a legal arrangement.[7] However, apart from certain categories of company, there is no requirement that a reporting entity **must** identify and take reasonable steps to verify the beneficial ownership of their customers, as part of their normal CDD of a customer, regardless of the perceived risk. Furthermore, for companies, a reporting entity has the discretion to determine whether and to what extent verification of the beneficial ownership is required.[8]

Under the AML/CTF Rules, a reporting entity has the discretion to decide if additional KYC information, including information relevant to understanding beneficial ownership, should be obtained. In most cases, a reporting entity would be expected to do so in cases of high risk. However, the FATF standards require that reporting entities **must** be required to undertake CDD measures, including identifying, and taking reasonable measures to verify the identity of the beneficial owner, regardless of the level of perceived risk and category of customer. The FATF standards also require reporting entities to identify and verify the individuals who are able to exercise effective control over the decision making of the customer, for example, senior management of the customer.

The FATF standards provide further clarity as to what constitutes 'reasonable measures'. In short,

For legal persons:

(i.i) The identity of the natural persons (if any – as ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control of the legal person or arrangement through ownership) who ultimately have a controlling ownership interest in a legal person; and

(i.ii) To the extent that there is doubt under (i.i) as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural persons (if any) exercising control of the legal person or arrangement through other means.

(i.iii) Where no natural person is identified under (i.i) or (i.ii) above, financial institutions should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of senior managing official.

For legal arrangements:

(ii.i) Trusts – the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership);

(ii.ii) Other types of legal arrangements – the identity of persons in equivalent or similar positions.

These measures are not alternative options, but cascading measures, with each to be used where the previous measure has been applied and has not identified a beneficial owner.

---

[7] Refer to the Glossary of terms on page 3. An example of a legal person is a company, an incorporated association, an incorporated partnership, and an example of a legal arrangement is a trust or an unincorporated partnership.

[8] Chapter 4.3.10 to 4.3.15 of the AML/CTF Rules outline the different levels of discretion allowed for different categories of company.

For reporting entities whose customers are mostly or all natural persons, it is not anticipated that these possible reforms would entail a significant regulatory impact. In particular, some small businesses, such as those in the gambling and alternative remittance sectors, are more likely to have a high percentage of individuals as customers.

Potential reforms

It is possible that the AML/CTF Rules be amended to clarify that the term 'beneficial owner' means the natural person(s) (individuals) who ultimately owns or controls a customer, and explicitly require reporting entities to identify and take reasonable steps to verify the identity of beneficial owners for all categories of customer that are legal persons or legal arrangements.

Questions

1. To what extent are reporting entities already assessing the beneficial ownership of customers that are legal persons or arrangements?
2. Is the element of control taken into account?
3. In seeking to understand the beneficial ownership of a customer, do you go beyond the first layer of ownership?
4. Do you consider the cascading measures outlined by the FATF standards provide a reasonable approach to identifying beneficial ownership that balances the risks and practicalities? If not, do you have an alternative approach to suggest?

Customer acting on behalf of another person

Deficiency 3: There is no requirement for reporting entities to determine whether the customer is acting on behalf of another person and, if so, to take reasonable steps to verify the identity of that other person.

Currently a reporting entity must identify a customer before providing them with a designated service. Where a reporting entity is aware that an *agent* is acting on behalf of a customer, a reporting entity is required to identify both the agent and the customer.

However, there is no mandatory obligation for reporting entities to proactively determine whether a customer who is a natural person is acting on behalf of another person, and if so, to take reasonable steps to verify the identity of that other person.[9] The AML/CTF Rules do not cover situations where someone may be:

- attempting to disguise or conceal ownership or control of an account or a transaction
- less formally acting on behalf of someone else.

Expectations are that in most cases individuals will be acting on their own behalf.

Potential reforms

It is possible to amend the AML/CTF Rules to require a reporting entity to take appropriate steps to:

- determine whether the person is conducting a transaction on behalf of another person or third party and, accordingly
- identify and verify that third party in accordance with the current customer identification processes outlined in the Rules.

Question

1. Are reporting entities already considering whether a person in acting on behalf of the customer is attempting to conceal or disguise the true 'owner' of the transaction? If so, to what is extent is this being considered and how is this achieved?

[9] This information is currently optional under the KYC requirements in Chapter 1.2 of the AML/CTF Rules

Settlor of a trust

Deficiency 4: There is no specific requirement for reporting entities to identify and verify the settlor of a trust.

The settlor of a trust is the person (natural or legal entity) who sets up the trust and signs the trust deed to 'create' the trust. The settlor gives the trustee a 'settlement' sum of money or property to be held on trust for the beneficiaries of the trust and should have no further involvement in the affairs of the trust.

There is no specific obligation in the AML/CTF Rules for a reporting entity to identify or verify the identity of the settlor of a trust, although it is noted that information on the settlor of a trust may be collected under its risk-based systems.

The FATF standards require that the settlor of a trust be identified and reasonable measures be taken to verify the identity of such persons because this person may be able to, under certain circumstances, exercise informal control over the assets of the trust by appointing a close associate or family member as a trustee. The identification and verification of the settlor of a trust will increase the transparency of this legal arrangement and enable the identification of the source of funds or assets.

The information concerning the settlor of a trust is almost always contained in the trust deed. The identification of the settlor of a trust should therefore not impose a significant additional burden on reporting entities.

Potential reforms

It is possible to amend the AML/CTF Rules to explicitly require a reporting entity to identify and verify the settlor of a trust.

Question

1. To what extent are reporting entities already identifying and verifying the settlor of a trust?

Enhanced customer due diligence and politically exposed persons

Deficiency 5:

There is no specific requirement to apply a range of measures in high-risk situations and some enhanced due diligence measures are not clearly distinguishable from normal CDD measures.

Reporting entities are not required to take specific additional measures for customers (or their beneficial owners) who are politically exposed persons (PEPs).

Chapter 15 of the AML/CTF Rules sets out the enhanced CDD requirements a reporting entity is expected to undertake in high-risk situations.

Australia's deficiencies with the FATF standards associated with enhanced CDD measures are two-fold:

1. Chapter 15 of the AML/CTF Rules only requires reporting entities to apply at least one of the listed measures where enhanced CDD is required in 'high-risk' situations. Furthermore, some of these measures are not clearly distinguishable from normal customer due diligence measures. However, the FATF requires reporting entities, in high-risk situations, to use a **range** of measures, and

2. There is no explicit requirement to undertake the specific enhanced measures prescribed by the FATF standards in relation to customers (or their beneficial owners) who are PEPs.

Based on the FATF standards, some of the measures listed in Chapter 15 of the AML/CTF Rules apply under normal (rather than enhanced) CDD. Specifically, measures to:

- clarify the nature of the customer's ongoing business with the reporting entity, and
- verify KYC information.

Specific measures concerning PEPs

The FATF standards define three categories of PEPs:

- Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country. For example, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations and important political party officials.
- International organisation PEPs are individuals who are or have been entrusted with a prominent function by an international organisation.
- Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions. For example Heads of State or of government, senior

government, judicial or military officials, senior executives of state-owned corporations and important political party officials.

Currently the AML/CTF Rules require a reporting entity to consider its customer types, including any PEPs, in identifying its money laundering and terrorism financing risk. However, the AML/CTF Rules do not set out any specific, enhanced due diligence measures in relation to identified PEPs.

The FATF standards require reporting entities to perform a range of additional due diligence measures in relation to both customers and beneficial owners who are PEPs or who are a family member or close associate of a PEP. In addition to performing normal CDD a reporting entity must:

- have appropriate risk-management systems to determine whether the customer or beneficial owner is a foreign PEP, and
- take reasonable measures to determine whether a customer or beneficial owner is a domestic or international organisation PEP.

For all foreign PEPs and for domestic or international organisation PEPs with whom the reporting entity has a higher risk business relationship, reporting entities must also:

a) obtain senior management approval for establishing or continuing business relationships

b) take reasonable measures to establish the source of wealth and source of funds, and

c) conduct enhanced ongoing monitoring of the business relationship.

Potential reforms

It is possible to amend the AML/CTF Rules to:

- prescribe specific measures to be taken to perform a range of enhanced CDD measures for high-risk situations, and
  - define the meaning of politically exposed person
  - require reporting entities to:
    - introduce appropriate risk-management systems to determine whether customers and beneficial owners are foreign PEPs,
      - e.g. taking proactive steps such as assessing customers on the basis of risk criteria, risk profiles, the business model, and the institution's own research
    - take reasonable measures to determine whether a customer or beneficial owner is an international organisation or domestic PEPs,
      - e.g. reviewing, on a risk based approach, the customer due diligence data which was collected, and
- provide for the conduct of enhanced CDD measures where the customer is a foreign PEP, or is domestic or international organisation PEP assessed as being high risk.

Questions

1. To what extent do reporting entities already undertake a range of measures under enhanced CDD in ‘high-risk’ situations? (that is, more than one measure)?

2. What measures are reporting entities commonly applying in high-risk situations?

3. To what extent do reporting entities already apply enhanced measures for a) foreign PEPs, b) domestic PEPs, and c) international organisation PEPs?

4. What measures are reporting entities commonly applying in relation to PEPs?

Purpose of business relationship

Deficiency 6: There is no requirement to collect information on the purpose and intended nature of the business relationship.

There is no explicit obligation requiring a reporting entity to obtain information on the 'purpose' and intended nature of the business relationship.

The AML/CTF Rules outline what minimum information must be collected and what information must be verified. This information mostly relates to **identification** of the customer (including confirmation of its existence in the case of a legal person or arrangement), and is usually limited to details such as name, address/location, date of birth (for individuals), registration or identification numbers (for companies) and location (for entities).

Under a reporting entity's risk-based systems and controls, additional KYC information **may** be collected as set out in **Table 3:**

Table 3 – Additional KYC information that may be collected relevant to the business relationship

Subparagraph of Part 1.2.1 of the AML/CTF Rules	Customer	Type of information
1(g)	Individual	The customer's occupation or business activity
1(h)	Individual	The nature of the customer's business with the reporting entity including: (i) the purpose of specific transactions; or (ii) the expected nature and level of transaction behaviour
2(j)	Company	The nature of the business activities conducted by the company
4(g)	Partnership	The business of the partnership
5(g)	Incorporated association	The objects of the association
6(e)	Unincorporated association	The objects of the association
7(i)	Registered cooperative	The objects of the cooperative

The FATF standards require a reporting entity to take CDD measures in order to '*understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship*.' The underlying principle is to ensure that the reporting entity better understands the nature of the business of the customer. This knowledge of the 'purpose' of the business relationship is considered to be an essential element for a reporting entity to fully understand the risks associated with a customer.

Potential reforms

It is possible to amend the AML/CTF Rules to include an explicit requirement that Part A of a reporting entity's AML/CTF program **must** include appropriate risk-based systems and controls to ensure that the reporting entity has a reasonable understanding of the nature of the customer's business or occupation.

Question

1. To what extent do reporting entities already include processes and procedures to understand the 'purpose' of the business relationship, for example, as part of commercial and other risk-management requirements?

Updating customer due diligence records

Deficiency 7: The obligations on reporting entities concerning record-keeping requirements regarding documents collected as part of the processes of identification, verification and updating of customers are inadequate.

Under AML/CTF Rules reporting entities must have in place appropriate risk-based systems and controls to determine whether, and in what circumstances, KYC information should be updated or verified in respect of its customers for ongoing CDD purposes. As the decision to update or verify such information can be made on a risk basis, there is a possibility that reporting entities may only be choosing to update or verify KYC information in situations where the risks are high. Even then, the discretion currently provided under Chapter 15 of the Rules allows a reporting entity to undertake enhanced measures other than updating KYC information.

The FATF standards require reporting entities to keep documents, data or information collected under the CDD process up to date and relevant by undertaking reviews of existing records. Although there is added emphasis on high-risk customers, the standards impose a general obligation for all CDD documentation to be reviewed and updated.

The potential reforms in Part 2 of this consultation paper would require the collection of additional CDD information, including:

- purpose of business
- control structures of legal persons and arrangements, and
- beneficial ownership.

If accepted, the scope of this reform will also need to encompass other CDD information requirements outlined in this paper. It is noted that reporting entities already have existing obligations to take reasonable steps to keep customer information up to date under privacy legislation, such as National Privacy Principle (NPP) 3 of the *Privacy Act 1988* (Cth).

Potential reforms

It is possible to enhance the AML/CTF regime to include a general obligation for reporting entities to keep all collected CDD information up to date and relevant, regardless of assessed risk, and that risk-based systems be used to determine what CDD information should be updated or verified and at what intervals.

Question

1. On what basis are reporting entities already updating the records arising from the obligations to obtain and collect documents as part of the processes to identify and verify customers?

Part 3

Options to minimise regulatory burden associated with the potential reforms

Australia's reporting population is far from homogenous, with reporting entities ranging from local family-owned businesses to major banks with an international presence. Experience and familiarity with Australia's AML/CTF regulations varies, as does the sophistication of AML/CTF programs and their supporting infrastructure.

Similarly, not all sectors of the reporting population face the same level of money laundering and terrorism financing risk. Certain products and services are known to be more attractive to criminals and terrorists, just as the presence of certain 'red flags' mean that it is more likely that a transaction is being undertaken for illegitimate purposes.

In reforming CDD requirements, the Government considers there may be various approaches available to reduce the regulatory burden on business, depending on their size and types of customers and transactions they deal with. These are outlined below. These approaches are not intended to be considered in isolation of each other, and do not exclude the possibility of other means of alleviating the potential burden on industry. Stakeholders are encouraged to provide options and approaches for consideration.

Stakeholder views are welcome in relation to the options outlined, their applicability, potential benefits and limitations, and whether there are other options that should be considered. Additional questions to help guide your considerations are included at the end of Part 3.

Exemptions for low-risk situations

It may be possible to provide regulatory exemptions for specific, well-defined situations involving a low level of money laundering/terrorism financing risk. Examples could include:

- particular sectors of the reporting population
- the provision of particular products or services, or
- particular customer types (e.g. public companies listed on a stock exchange).

Such exemptions would need to be supported by current, comprehensive risk assessments and mitigating measures to ensure such exemptions do not create new vulnerabilities in the regime. They would also need to be subject to regular review provisions to ensure that they do not become out-dated and ineffective.

In the event that broader exemptions are unable to be supported by the available evidence, another alternative for individual businesses would be to use the existing exemption granting mechanism available to the AUSTRAC CEO under the AML/CTF Act. This option would be significantly more resource-intensive for businesses, which would bear the onus and cost for justifying exemptions, and for AUSTRAC as the assessing body.

Customer self-attestation

Many of the potential reforms may be able to be instituted by allowing reporting entities to rely on information provided by the customer to fulfil the *identification* element. A realignment of the customer-generated Disclosure Certificate facility provided under Chapter 30 of the AML/CTF Rules could be considered.

That is, customers could be asked to provide information in relation to their beneficial ownership to be retained (collected) by the reporting entity in order to provide the product or service. Customers would certify that the information they have provided is true and correct, and face significant penalties for the provision of false information.

It is important to understand that self-attestation by the customer would not remove the existing obligation of the reporting entity to conduct adequate due diligence. Reporting entities would have to justify their use of such an approach and be able to demonstrate why other reliable and independent avenues to collect such information were not possible. It must be supported by robust procedures to *verify* the accuracy of the information provided and strict supervision by the regulator (AUSTRAC). Further, penalties for the provision of false information must be supported by the ability of regulators and law enforcement to detect breaches in order to be an effective deterrent.

Reliance on third-party due diligence

Another approach could be to enable reporting entities to rely on CDD undertaken by third parties, such as other reporting entities (particularly financial institutions), where information is accessible, credible, relevant and up to date.

Reliance enables a reporting entity to 'rely' on the applicable CDD procedures carried out by another reporting entity under certain circumstances and/or conditions, either in the same or in another anti-money laundering jurisdiction. This approach has the potential to deliver major savings to reporting entities, with particular benefit to those entities which are limited by their size and level of resourcing.

Section 38 of the AML/CTF Act and the AML/CTF Rules already provide an avenue of relief for reporting entities. A reporting entity may 'rely', subject to certain conditions, on a third party to apply any or all of the CDD measures relating to verification of identity of the customer or beneficial owner and the nature and purpose of the intended business relationship.

The revised FATF standards provide additional encouragement for countries to consider the scope of reliance that could be made available to their regulated entities. A number of potential obstacles exist in relation to this approach:

(i) To be truly effective, reliance models would likely require some form of central infrastructure

(ii) There would be privacy considerations regarding the information to be shared. Legislative amendment may be required to enable effective sharing of information

(iii) Some reporting entities (such as financial institutions) may end up shouldering a greater proportion of the costs of undertaking the initial due diligence, and

(iv) There could be an issue of legal liability if a relying entity fails to detect a money laundering or terrorism financing case due to inaccuracies in the information relied upon.

However, there could be a number of advantages to such an approach provided these issues are resolved, and provided supporting infrastructure exists to enable its efficient and effective implementation.

Supporting infrastructure

Any compliance burden on reporting entities could be alleviated by enabling access to supporting infrastructure that facilitates the checking and sharing of CDD information relating to beneficial ownership. Such infrastructure could be maintained by Government or as an industry partnership.

While this approach would probably be of most benefit in the long term in achieving an appropriate balance between business efficiency and regulatory effectiveness, its initial implementation would require a number of legal, resourcing and technical/IT issues to be overcome.

Simplified due diligence (SDD)

Under a risk-based approach, reporting entities could have greater ability to use SDD measures in low-risk situations. For example, SDD may apply in circumstances where a reporting entity is dealing with a customer that is a regulated credit or financial institution.

Examples of possible SDD measures are:

- verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold)
- reducing the frequency of customer identification updates
- reducing the degree of ongoing monitoring and scrutinising of transactions, based on a reasonable monetary threshold, or
- not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

For example, some reporting entities, such as certain gambling providers, are currently permitted to delay customer identification processes in low-risk situations, until the customer's account balance reaches a certain threshold. It may be reasonable to infer in such circumstances the purpose and intended nature of the business relationship from the nature of the account (for example, in the case of a gambling provider, it may be self-evident that the account is to be used to place bets).

Transitional arrangements

If reforms are implemented, it would be expected that at least some reporting entities will need to make changes to their current processes and systems. Although it is likely that some of the potential reforms would simply reflect the current practice of some reporting entities, this would not be the case for all.

Similarly, those reporting entities that are subject to the US' FATCA provisions will already be considering how to harmonise, where possible, the CDD requirements of FATCA and Australia's AML/CTF regime.

Consideration of transitional arrangements may be appropriate.

Questions

1. What circumstances would be appropriate for up-front exemptions?
2. What benefits and problems may arise from a self-attestation model for the purposes of *identification* of beneficial owners and control structures?
3. In what circumstances would the provision of a greater flexibility in the current AML/CTF Rules provisions for reliance assist reporting entities to undertake CDD measures in a cost effective way?
4. To what extent do reporting entities currently use simplified due diligence measures? What options may be considered to extend the use of simplified due diligence measures?
5. What independent and reliable sources of information are used by reporting entities to verify beneficial ownership and control? What are the issues and concerns of reporting entities in meeting this obligation and what alternatives may be considered?
6. If the AML/CTF regime was extended to address the deficiencies outlined at Part 2 of this paper, what is a sufficient lead time for reporting entities between the changes to the regime and the commencement of the obligations?
7. What other options may be considered to minimise or reduce potential regulatory burden on reporting entities in meeting their obligations for beneficial ownership and control, if the AML/CTF regime was extended to address the deficiencies outlined at Part 2 of this paper?

Attachment 1: FATF Recommendation 10 – Customer Due Diligence

CUSTOMER DUE DILIGENCE AND RECORD KEEPING

10. Customer due diligence

Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names.

Financial institutions should be required to undertake customer due diligence (CDD) measures when:

(i) establishing business relations;

(ii) carrying out occasional transactions: (i) above the applicable designated threshold (USD/EUR 15,000); or (ii) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;

(iii) there is a suspicion of money laundering or terrorist financing; or

(iv) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The principle that financial institutions should conduct CDD should be set out in law. Each country may determine how it imposes specific CDD obligations, either through law or enforceable means.

The CDD measures to be taken are as follows:

(a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

(b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer.

(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

(d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should be required to apply each of the CDD measures under (a) to (d) above, but should determine the extent of such measures using a risk-based approach (RBA) in accordance with the Interpretive Notes to this Recommendation and to Recommendation 1.

Financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering and terrorist financing risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with the applicable requirements under paragraphs (a) to (d) above (subject to appropriate modification of the extent of the measures on a risk-based approach), it should be required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, although financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

INTERPRETIVE NOTE TO RECOMMENDATION 10 (CUSTOMER DUE DILIGENCE)

A. CUSTOMER DUE DILIGENCE AND TIPPING OFF

1. If, during the establishment or course of the customer relationship, or when conducting occasional transactions, a financial institution suspects that transactions relate to money laundering or terrorist financing, then the institution should:

   (a) normally seek to identify and verify the identity26 of the customer and the beneficial owner, whether permanent or occasional, and irrespective of any exemption or any designated threshold that might otherwise apply; and

   (b) make a suspicious transaction report (STR) to the financial intelligence unit (FIU), in accordance with Recommendation 20.

2. Recommendation 21 prohibits financial institutions, their directors, officers and employees from disclosing the fact that an STR or related information is being reported to the FIU. A risk exists that customers could be unintentionally tipped off when the financial institution is seeking to perform its customer due diligence (CDD) obligations in these circumstances. The customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected money laundering or terrorist financing operation.

3. Therefore, if financial institutions form a suspicion that transactions relate to money laundering or terrorist financing, they should take into account the risk of tipping-off when performing the CDD process. If the institution reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file a STR. Institutions should ensure that their employees are aware of, and sensitive to, these issues when conducting CDD.

B. CDD – PERSONS ACTING ON BEHALF OF A CUSTOMER

4. When performing elements (a) and (b) of the CDD measures specified under

   Recommendation 10, financial institutions should also be required to verify that any person purporting to act on behalf of the customer is so authorised, and should identify and verify the identity of that person.

C. CDD FOR LEGAL PERSONS AND ARRANGEMENTS

5. When performing CDD measures in relation to customers that are legal persons or legal arrangements27, financial institutions should be required to identify and verify the customer, and understand the nature of its business, and its ownership and control structure. The purpose of the requirements set out in (a) and (b) below, regarding the identification and verification of the customer and the beneficial owner, is twofold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the customer to be able to properly assess the potential money laundering and terrorist financing risks associated with the business relationship; and, second, to take appropriate steps to mitigate the risks. As two aspects of one process, these requirements are likely to interact and complement each other naturally. In this context, financial institutions should be required to:

(a) Identify the customer and verify its identity. The type of information that would normally be needed to perform this function would be:

(i) Name, legal form and proof of existence – verification could be obtained, for example, through a certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust, or other documentation from a reliable independent source proving the name, form and current existence of the customer.

(ii) The powers that regulate and bind the legal person or arrangement (e.g. the memorandum and articles of association of a company), as well as the names of the relevant persons having a senior management position in the legal person or arrangement (e.g. senior managing directors in a company, trustee(s) of a trust).

(iii) The address of the registered office, and, if different, a principal place of business.

(b) Identify the beneficial owners of the customer and take reasonable measures to verify the identity of such persons, through the following information:

(i) For legal persons:

(i.i) The identity of the natural persons (if any – as ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control of the legal person or arrangement through ownership) who ultimately have a controlling ownership interest in a legal person; and

(i.ii) to the extent that there is doubt under (i.i) as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural persons (if any) exercising control of the legal person or arrangement through other means.

(i.iii) Where no natural person is identified under (i.i) or (i.ii) above, financial institutions should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of senior managing official.

(ii) For legal arrangements:

(ii.i) Trusts – the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries31, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership);

(ii.ii) Other types of legal arrangements – the identity of persons in equivalent or similar positions.

Where the customer or the owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

The relevant identification data may be obtained from a public register, from the customer or from other reliable sources.

D. CDD FOR BENEFICIARIES OF LIFE INSURANCE POLICIES

6. For life or other investment-related insurance business, financial institutions should, in addition to the CDD measures required for the customer and the beneficial owner, conduct the following CDD measures on the beneficiary(ies) of life insurance and other investment related insurance policies, as soon as the beneficiary(ies) are identified/designated:

   (a) For beneficiary(ies) that are identified as specifically named natural or legal persons or legal arrangements – taking the name of the person;

   (b) For beneficiary(ies) that are designated by characteristics or by class (e.g. spouse or children at the time that the insured event occurs) or by other means (e.g. under a will) – obtaining sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout.

The information collected under (a) and/or (b) should be recorded and maintained in accordance with the provisions of Recommendation 11.

7. For both the cases referred to in 6(a) and (b) above, the verification of the identity of the beneficiary(ies) should occur at the time of the payout.

8. The beneficiary of a life insurance policy should be included as a relevant risk factor by the financial institution in determining whether enhanced CDD measures are applicable. If the financial institution determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, then the enhanced CDD measures should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

9. Where a financial institution is unable to comply with paragraphs 6 to 8 above, it should consider making a suspicious transaction report.

E. RELIANCE ON IDENTIFICATION AND VERIFICATION ALREADY PERFORMED

10. The CDD measures set out in Recommendation 10 do not imply that financial institutions have to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. An institution is entitled to rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile.

F. TIMING OF VERIFICATION

11. Examples of the types of circumstances (in addition to those referred to above for beneficiaries of life insurance policies) where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business, include:

    - Non face-to-face business.
    - Securities transactions. In the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.

12. Financial institutions will also need to adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification.

    These procedures should include a set of measures, such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

G. EXISTING CUSTOMERS

13. Financial institutions should be required to apply CDD measures to existing customers on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

H. RISK-BASED APPROACH

14. The examples below are not mandatory elements of the FATF Standards, and are included for guidance only. The examples are not intended to be comprehensive, and although they are considered to be helpful indicators, they may not be relevant in all circumstances.

Higher risks

15. There are circumstances where the risk of money laundering or terrorist financing is higher, and enhanced CDD measures have to be taken. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher-risk situations (in addition to those set out in Recommendations 12 to 16) include the following:

    (a) Customer risk factors:

- The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer).
- Non-resident customers.
- Legal persons or arrangements that are personal asset-holding vehicles.
- Companies that have nominee shareholders or shares in bearer form.
- Business that are cash-intensive.

- The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

(b) Country or geographic risk factors:

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems.
- Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.
- Countries identified by credible sources as having significant levels of corruption or other criminal activity.
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

(c) Product, service, transaction or delivery channel risk factors:

- Private banking.
- Anonymous transactions (which may include cash).
- Non-face-to-face business relationships or transactions.
- Payment received from unknown or un-associated third parties

Lower risks

16. There are circumstances where the risk of money laundering or terrorist financing may be lower. In such circumstances, and provided there has been an adequate analysis of the risk by the country or by the financial institution, it could be reasonable for a country to allow its financial institutions to apply simplified CDD measures.

17. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially lower risk situations include the following:

(a) Customer risk factors:

- Financial institutions and DNFBPs – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements.
- Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership.
- Public administrations or enterprises.

(b) Product, service, transaction or delivery channel risk factors:

- Life insurance policies where the premium is low (e.g. an annual premium of less than USD/EUR 1,000 or a single premium of less than USD/EUR 2,500).
- Insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral.
- A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme.

- Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

(c) Country risk factors:

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems.

- Countries identified by credible sources as having a low level of corruption or other criminal activity.

In making a risk assessment, countries or financial institutions could, when appropriate, also take into account possible variations in money laundering and terrorist financing risk between different regions or areas within a country.

18. Having a lower money laundering and terrorist financing risk for identification and verification purposes does not automatically mean that the same customer is lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

Risk variables

19. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels risk, a financial institution should take into account risk variables relating to those risk categories. These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures.

Examples of such variables include:

- The purpose of an account or relationship.

- The level of assets to be deposited by a customer or the size of transactions undertaken.

- The regularity or duration of the business relationship.

Enhanced CDD measures

20. Financial institutions should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, financial institutions should be required to conduct enhanced CDD measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of enhanced CDD measures that could be applied for higher-risk business relationships include:

- Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.

- Obtaining additional information on the intended nature of the business relationship.

- Obtaining information on the source of funds or source of wealth of the customer.

- Obtaining information on the reasons for intended or performed transactions.

- Obtaining the approval of senior management to commence or continue the business relationship.

- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

Simplified CDD measures

21. Where the risks of money laundering or terrorist financing are lower, financial institutions could be allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). Examples of possible measures are:

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold).

- Reducing the frequency of customer identification updates.

- Reducing the degree of on-going monitoring and scrutinising transactions, based on a reasonable monetary threshold.

- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

- Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

Thresholds

22. The designated threshold for occasional transactions under Recommendation 10 is USD/EUR 15,000. Financial transactions above the designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

Ongoing due diligence

23. Financial institutions should be required to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of customers.