Australian Government
Attorney-General's Department

# Reforming Australia's anti-money laundering and counter-terrorism financing regime

## Paper 5: Broader reforms to simplify, clarify and modernise the regime

## May 2024

# Contents

Introduction ..... 3
Reforms in this paper ..... 4
AML/CTF programs ..... 5
Customer Due Diligence (CDD) ..... 13
Exception for assisting an investigation of a serious offence ..... 25
CDD exemption for gambling service providers ..... 27
Tipping off offence ..... 28
Moving some exemptions from the Rules to the Act ..... 31
Repealing the *Financial Transaction Reports Act 1988* ..... 32
Consultation questions ..... 33
Table 1 – Proposed model of reforms to simplify, clarify and modernise the regime ..... 34

# Introduction

Each year billions of dollars of illicit funds are generated from illegal activities such as drug trafficking, tax evasion, people smuggling, cybercrime, arms trafficking and other illegal and corrupt practices. Money laundering is not a victimless crime. It is a critical facilitator of most serious crimes and undermines the rule of law globally.

Serious and organised criminal groups are driven by illicit profit. It sits at the centre of why they conduct their illegal activities. Laundering this illicit wealth allows them to enjoy the proceeds of crime and to reinvest in further criminal activities. Illicit financing facilitates serious crimes across Australia and the world, diverting government resources which could be used for social, health or education services, increasing the burden on law enforcement, and ultimately impacting the most vulnerable in our community. Money laundering and illicit financing also erodes trust in Australia's stable financial system, our government institutions and the equitable application of the rule of law across Australian society.

Australia's anti-money laundering and counter-terrorism financing (AML/CTF) regime establishes a regulatory framework for combatting money laundering, terrorism financing and other serious financial crimes. At its core, the AML/CTF regime is a partnership between the Australian Government and industry. No legitimate business wants to unwittingly assist money laundering. Through the regulatory framework, businesses are asked to play a vital role in detecting and preventing the misuse of their sectors and products by criminals seeking to launder money and fund terrorism.

As the Attorney-General announced in April 2023, the Attorney-General's Department (the department) is consulting on reforms to the regime. The reforms aim to ensure it continues to effectively deter, detect and disrupt money laundering and terrorism financing, and meet international standards set by the Financial Action Task Force (FATF), the global financial crime watchdog.

Ensuring Australia is compliant with the international standards set by the FATF is a fundamental objective of the proposed reforms. Australia's AML/CTF regime will next be comprehensively assessed by the FATF over 2026-27, where Australia will be assessed against strengthened standards. A poor assessment risks Australia being 'grey listed' by the FATF, which could have serious consequences for Australia, including tangible economic and gross domestic product (GDP) impacts, and increased threats, risks and burdens for law enforcement.

The reforms also present an opportunity to improve the effectiveness of the regime and ease regulatory burden by simplifying and clarifying the regime to make it easier for businesses to meet their obligations, and modernising the regime to reflect changing business structures and technologies across the economy.

Ultimately, the reforms aim to significantly improve Australia's ability to target illicit financing. They will reduce the ability of criminal actors and autocratic regimes to invest their illicit funds into further criminal activities, and disrupt serious crime in the Australian community and in our region.

The proposals outlined in this paper have not been settled. The paper is designed to seek your feedback on the practical impact on you or your business to inform Australian Government decisions on the proposed reforms to the regime.

# Reforms in this paper

Key requirements relating to AML/CTF programs and Customer Due Diligence (CDD) are dispersed throughout the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (the Act) and the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007* (the Rules) making them difficult to follow and creating implementation challenges. A key objective underpinning the reforms is ensuring a reporting entity's obligations are clear, easy to understand and reflect contemporary business.

This paper provides an overview of proposed changes to address these challenges, and to simplify and clarify the AML/CTF regime. These reforms will apply to both existing and newly regulated entities. It proposes to replace the current prescriptive AML/CTF program and CDD requirements with clear, risk-based, and outcomes-focused obligations.

This paper also outlines reforms to simplify, clarify and update obligations relating to:

- exceptions for assisting an investigation of a serious offence
- updated obligations for gambling service providers
- the tipping off offence
- exemptions, and
- the repeal of the *Financial Transactions Reports Act 1988* (Cth).

Table 1 summarises the new model for proposed simplification, clarification and modernisation reforms outlined in this paper.

# AML/CTF programs

An AML/CTF program demonstrates how a business or organisation addresses the money laundering and terrorism financing risks it may reasonably face. It is a collection of documented policies, procedures, systems and controls that a business or organisation uses to identify, mitigate and manage those risks.

## Why are reforms to AML/CTF program obligations needed?

The 2016 *Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations* (the Statutory Review) noted the complexity of the AML/CTF program requirements generates uncertainty and ambiguity for reporting entities.

The department is committed to ensuring that AML/CTF program obligations remain fit-for-purpose and balanced. Clarifying the obligations under the regime would reduce the burden that businesses face interpreting complex provisions, and help regulated entities understand the outcomes they are expected to achieve. Greater levels of industry compliance following the revised, clearer obligations will also assist law enforcement to protect the Australian community, as this will result in better financial intelligence. The proposed changes seek to simplify and clarify obligations in the regime, rather than fundamentally change existing obligations that are based on international standards.

### What are the challenges with the current obligations?

Stakeholders have expressed concern that the requirement for a two-part AML/CTF program is overly complicated, fragmented across the Act and the Rules, and does not contribute to businesses effectively understanding and appropriately managing the risks they may face.

The regime currently requires that before a reporting entity can provide a designated service, it must 'have and comply with' a two-part AML/CTF program that outlines the risks and mitigations of providing this service. The purpose of Part A of the program is to identify, mitigate and manage the risks associated with the entity providing a designated service, while Part B of the program sets out the entity's applicable customer identification procedures. The requirements for Parts A and B of AML/CTF programs are spread across the Act and Rules.

Due to this complicated fragmentation, a small or medium business may enlist an external advisor to develop an AML/CTF program for them. While this may acquit their obligation to 'have and comply with' an AML/CTF program, this approach does not require the business to effectively understand and appropriately manage the risks they may reasonably face in providing a designated service.

A key objective of the proposed reforms is to ensure a reporting entity's obligations are clear and simple, reducing the administrative burden of interpreting complex provisions and reinforcing a risk-based approach to implementing an AML/CTF program.

Australia's AML/CTF regime and the international FATF Standards take a risk-based approach to regulation. This means regulated businesses (known as reporting entities) implement compliance measures that are proportionate to their assessed level of risk. This recognises that the reporting entity is best placed to assess the risks posed by its customers, delivery channels, products and services.

The risk-based approach allows entities to introduce mitigation measures commensurate to this risk. The range, frequency or intensity of mitigation measures and internal controls would necessarily be greater in higher risk scenarios. This paper highlights the risk-based principles that underpin the reform measures and the outcomes they are intended to achieve.

Changes to the regime would be supported by targeted guidance materials from Australia's AML/CTF regulator and financial intelligence unit, AUSTRAC, to assist reporting entities to implement effective AML/CTF programs.

## Overview of AML/CTF program reforms

The department proposes to streamline the separate parts of an AML/CTF program into a single obligation, and reinforce the requirement for regulated entities to take a risk-based approach to their AML/CTF program.

The revised AML/CTF programs obligations would include the following key elements:

1. **An overarching risk assessment obligation**: reporting entities will be required to assess the risk of money laundering, terrorism financing or proliferation financing that they may reasonably face in the provision of a designated service.

2. **Proportionate risk mitigation measures:** reporting entities will be required to implement risk mitigation measures in its AML/CTF program, in response to its risk assessment. The reporting entity must extend these measures to its internal policies, systems and controls to ensure a culture of compliance within its business.

3. **Simplified business group concept:** the 'designated business group' will be replaced with a simplified 'business group' concept that will extend to all related entities, including non-AML/CTF reporting entities where appropriate. This will facilitate greater information sharing between members of a business group and allow for appropriate group-wide risk management and sharing of AML/CTF obligations.

4. **Specific internal controls:** the legislation will clarify the roles and responsibilities of a reporting entity's board or equivalent senior management and its AML/CTF Compliance Officer, in relation to the implementation of internal controls. The role of the AML/CTF Compliance Officer will be clarified to be that of an individual in management who oversees the operational implementation of the AML/CTF program.

5. **Simplified obligations for foreign branches and subsidiaries:** the Act will simplify and clarify requirements for reporting entities with foreign branches and subsidiaries. This will reduce complexity when Australian AML/CTF obligations interact with local laws in the host country.

## Establishing a clearer requirement to conduct a risk assessment

The department proposes to establish a clear, rather than implied, requirement that a reporting entity must conduct a risk assessment. This would involve the reporting entity taking steps to identify and assess the risks it may reasonably expect to face in providing designated services. The risk assessment would then be used to inform the policies, systems and controls that form their AML/CTF program to mitigate and manage those risks.

The department proposes that the Act would clearly state the reporting entity must consider the nature, size and complexity of its business in determining risk level, incorporate relevant risks identified and communicated by AUSTRAC, and document its risk assessment methodology as part of its AML/CTF program. As a baseline, reporting entities would be required to consider risks related to customer types, types of designated services provided, methods of delivery and the jurisdictions they deal with. Additional factors may be specified in the Rules, if required.

The Act would also clarify that a reporting entity is required to review and keep its risk assessment up to date. Triggers for reviewing a risk assessment could include changes to a business's risk profile or the adoption of new technologies to manage certain AML/CTF obligations. At a minimum, risk assessments would need to be reviewed every four years.

A reporting entity's board or equivalent senior management would be required to approve the entity's risk assessment and be informed of updates to that assessment.

In addition, to align with FATF Standards, reporting entities must consider the risk that their business may facilitate proliferation financing when conducting a risk assessment.[1] The department notes that exposure to proliferation financing risk will vary significantly between sectors and businesses. The AML/CTF regime would be sufficiently flexible to recognise that many businesses do not have material proliferation financing exposure.

Businesses that reasonably assess their proliferation financing exposure could be mitigated by existing measures, or that the risk is immaterial, would not be required to implement additional policies, systems and controls.

[1] The FATF defines proliferation financing risk as the potential breach, non-implementation or evasion of targeted financial sanctions obligations related to preventing the financing and proliferation of weapons of mass destruction. The department will consider how to define proliferation financing in the Australian legal context.

## Ensuring reporting entities implement proportionate risk mitigation measures

Once a reporting entity has completed a risk assessment as part of its AML/CTF program, and considered any relevant risks communicated by AUSTRAC, it must implement proportionate risk mitigation measures. The Act would include a specific obligation that reporting entities develop, implement and maintain enterprise-wide policies, systems and controls proportionate to the nature, size and complexity of its business.

In ensuring an outcomes-focused approach, the Act would not specify the detail of mitigation measures. Feedback from the first round of consultation noted that many entities already have certain risk mitigation measures in place due to other regulatory regimes or as part of standard business practice. The reformed AML/CTF program requirement would allow reporting entities to leverage these existing mitigation measures for their AML/CTF program obligations.

### What would this look like?

For example, many legal practitioners have existing systems in place to comply with the Australian Registrars' National Electronic Conveyancing Council (ARNECC) framework to verify their clients' identities. Legal practitioners who become reporting entities under the AML/CTF regime may determine that the ARNECC Verification of Identity Standards are sufficient to meet some AML/CTF customer identification requirements for certain customer types. These reporting entities would be able to identify and include that practice in their AML/CTF program.

This obligation would be supported by specific types of risk mitigation measures that an AML/CTF program must include. These could include:

- enterprise-wide risk management practices, to ensure that risk is considered across the reporting entity's day-to-day operations
- clear documentation of how the policies, systems and controls mitigate and manage the risks identified in the risk assessment
- details about customer due diligence (initial, ongoing, enhanced and simplified)
- review of risk mitigation measures in response to updates to its risk assessment, including when adopting new technologies, and
- identification and reporting of suspicious matters.

Additional detail about these types of measures may be included in the Rules, where required.

## Ensuring reporting entities maintain internal controls

The department proposes an express obligation in the Act that requires a reporting entity to establish internal practices that ensure the business, its managers, employees and agents comply with AML/CTF obligations. These are necessary to support risk mitigation measures and ensure a culture of compliance.

Board or equivalent senior management oversight of the AML/CTF program is a key internal control for a reporting entity. The department proposes that the Act would ensure this oversight is appropriate to the individual entity or business group and focused on strategic decisions related to risk management. This means the board or equivalent senior management would need to ensure that it is reasonably satisfied that the AML/CTF program is effectively identifying, mitigating and managing the entity's risk. For reporting entities that have limited resourcing, including smaller businesses, the owner of the business may be best placed to acquit the AML/CTF program oversight.

The board or equivalent senior management would not be required to approve the implementation of day-to-day, operational measures to ensure they are not overburdened. Entities would be required to have an AML/CTF Compliance Officer, who will manage the implementation of operational measures.

A reporting entity's AML/CTF Compliance Officer would be responsible for oversight and coordination of the AML/CTF program and ensure that any changes made to the AML/CTF program are approved by an individual in senior management such as the Chief Risk Officer. This would ensure operational decisions can be made with greater flexibility.

**What would this look like?**

For example, as a reporting entity under the proposed reforms, Savings and Loans Bank is required to implement and maintain an AML/CTF program. Its AML/CTF program sets out how the reporting entity conducts risk awareness training. The specifics around this training, for example its frequency and who is required to participate, would not need to be approved by the board and could be approved by the Chief Risk Officer on advice from the AML/CTF Compliance Officer. The board will just be required to determine whether it is satisfied that the AML/CTF program, including its risk awareness training requirements, is operating effectively.

The AML/CTF Compliance Officer also oversees the development and implementation of other operational measures including Savings and Loans Bank's customer due diligence procedures, rules for identifying unusual transactions and rules for conducting employee due diligence.

Further, the department proposes to move the requirement for reporting entities to have a suitable AML/CTF Compliance Officer from the Rules to the Act, to reduce complexity and co-locate relevant AML/CTF program requirements. The Act would:

- clarify that the AML/CTF Compliance Officer is an employee at the management level responsible for overseeing and coordinating the day-to-day operation and effectiveness of a reporting entity's AML/CTF program, and the reporting entity's compliance with the Act, Rules and Regulations
- require that the AML/CTF Compliance Officer has sufficient authority, independence and resourcing to fulfil their function (proportionate to the scale of the business)

- require reporting entities to certify to AUSTRAC that their AML/CTF Compliance Officer is a fit and proper person, and
- empower the AUSTRAC CEO to make rules in relation to the requirements of the AML/CTF Compliance Officer position.

It would be the responsibility of the reporting entity's senior management to ensure the functions of the AML/CTF Compliance Officer are designated to an appropriate member of management. The specific level of the AML/CTF Compliance Officer would vary depending upon the type and scale of the business.

**What would this look like?**

For example, senior management of Rodgers & Gavelstein – a law firm employing 34 people – decide to designate the functions of their AML/CTF Compliance Officer to a Principal Lawyer in their firm. This person has sufficient knowledge of the corporate workings of Rodgers & Gavelstein, and the appropriate seniority and resourcing to fulfil the AML/CTF Compliance Officer role.

For reporting entities that have limited resourcing, including smaller businesses, the owner of the business may be best placed to fulfil the AML/CTF Compliance Officer role requirements. This would meet the requirement for the AML/CTF Compliance Officer to exercise independence as the owner would not be subject to direction in the exercise of their judgment about AML/CTF matters.

**What would this look like?**

For example, Bill runs a small accountancy firm. Eddie is his only employee, and is responsible for answering phone calls and emails, and managing Bill's diary. He does not make any decisions about the running of the business. As the business owner, Bill decides that given their respective roles, Bill has the appropriate authority to fulfil the role of AML/CTF Compliance Officer for the business.

The Rules would also include specific requirements regarding the AML/CTF Compliance Officer function, including for:

- the AML/CTF Compliance Officer to report at least annually to the entity's board or equivalent senior management on the day-to-day operation and effectiveness of the AML/CTF program, and
- the reporting entity to notify AUSTRAC of the details of the AML/CTF Compliance Officer upon enrolment of the reporting entity and within 14 days of any change (as per current requirements).

To complement risk mitigation obligations, the Act would specify categories of internal controls that must be included in an AML/CTF program, with additional details in the Rules. These are broadly in line with existing obligations and could include:

- compliance management arrangements for the AML/CTF Compliance Officer and the board or equivalent senior management, including ensuring that the reporting entity is meeting its reporting obligations
- initial and ongoing employee due diligence and screening appropriate to the organisation and to the position held by the employee
- ongoing employee AML/CTF training, and
- a requirement for independent audit with a frequency determined by the entity's risk profile (with a potential minimum frequency of every four years) and detail around the minimum standards for auditors.

## Establishing a new 'business group' concept and ensuring group-wide risk management

Under the current regime, reporting entities within a group of related entities can choose to manage their common risks, information sharing and compliance obligations by establishing a designated business group (DBG).

The department proposes replacing the concept of a DBG with a simplified 'business group' concept, which would automatically include all related entities in a corporate group or other structure. A business group head would be responsible for assessing risk across the group and its members and developing a group AML/CTF program. The business group head must ensure that its AML/CTF program applies to all business group members that provide designated services in Australia—obligations for overseas branches and subsidiaries are detailed later in the paper.

The simplified business group concept would capture traditional corporate group arrangements as found in the financial services sector, as well as other non-corporate structures and, where appropriate, franchise arrangements. The group-wide program would require a risk assessment that identifies and assesses risk at both the group and individual member level.

Non-reporting entities within the ownership or control structure would be included in the concept of a business group. This would reflect how modern businesses are structured in practice and facilitate information sharing between group members for the purposes of customer due diligence and risk management. The concept would also allow other members (including non-reporting entities) within business groups to fulfil AML/CTF obligations on behalf of reporting entities. A non-reporting entity member of a business group will not, however, be subject to direct AML/CTF regulation for functions delegated to them.[2] Liability for any failings in carrying out AML/CTF obligations would remain with the reporting entity on whose behalf the obligation is carried out.

[2] This relates to non-reporting entity subsidiaries. A non-reporting entity is the business group head will be regulated for group-level risk assessment and compliance responsibilities under the Act.

**What would this look like?**

For example, Big Bank has a number of subsidiary businesses, including ID Services which performs identity verification for Big Bank's retail banking services. ID Services does not provide any designated services under the Act and is therefore not a regulated entity. The proposed model would allow Big Bank and its subsidiaries to be considered a business group, which would allow for information collected by ID Services to be shared with Big Bank and other members of the Big Bank group in order to assist with fulfilling customer due diligence and broader risk management requirements.

Business group heads would be required to provide for the following in the group-wide AML/CTF program:

- sharing of customer due diligence information and related record-keeping requirements for customer due diligence reliance within the group
- arrangements for a business group member to fulfil AML/CTF obligations on behalf of another reporting entity in the business group
- sharing of information about customers for risk management and mitigation as well as to support group-level compliance, audit and AML/CTF functions, and
- safeguarding the confidentiality of shared information, including to manage the risk of tipping off.

The proposed group-wide risk management framework would apply to all reporting entities in the group, regardless of the types of designated services they provide, and would assist in reducing regulatory cost.

**What would this look like?**

For example, 'Home Sweet Home' is a real estate brand made up of 30 Australian franchisees, led by HSH Group as the franchisor. HSH Group and its franchisees agree to amend their franchise agreement to make HSH Group responsible for overseeing the development and implementation of a group-wide AML/CTF program on behalf of the franchisees, who are all individual reporting entities. The franchisor and franchisees now meet the criteria of a business group and abide by the relevant business group obligations. As business group head, HSH Group must develop, implement and maintain a group-wide AML/CTF program and ensure that all reporting entity members comply with their obligations. Individual Home Sweet Home franchisees would remain responsible for fulfilling their own obligations within the group-wide AML/CTF program for the services they provide.

The department proposes that the Act could also include a provision enabling the AUSTRAC CEO to make particular rules with respect to group AML/CTF policies, systems and controls, and foreign branches and subsidiaries.

## Simplified obligations for foreign branches and subsidiaries

The department also proposes to consolidate and simplify the different parts of the Act and Rules relating to the obligations of a reporting entity that has foreign branches and subsidiaries. Current obligations for foreign branches and subsidiaries are not clearly articulated and are inconsistent with FATF requirements. Challenges for Australian businesses include:

- regulatory uncertainty about which obligations apply to designated services provided at or through overseas permanent establishments, and
- difficulties providing domestic services to customers who have been subject to customer due diligence at overseas branches (also known as 'passporting').

The Act will allow flexibility in how a business group head meets the general obligations under Australia's AML/CTF regime, to the extent permitted by local laws in the host country. This would align Australia's AML/CTF regime more closely with FATF Recommendation 18.[3]

### Consultation questions

a. Under the outlined proposal, a business group head would ensure that the AML/CTF program applies to all branches and subsidiaries. Responsibility for some obligations (such as certain customer due diligence requirements) could also be delegated to an entity within the group where appropriate. For example, a franchisor could take responsibility for overseeing the implementation of transaction monitoring in line with a group-wide risk assessment. Would this proposal assist in alleviating some of the initial costs for smaller entities?
b. The streamlined AML/CTF program requirement outlined provides that the board or equivalent senior management of a reporting entity should ensure the entity's AML/CTF program is effectively identifying and mitigating risk. To what extent would this streamlined approach to oversight allow for a more flexible approach to changes in circumstance?
c. Many modern business groups use structures that differ from the traditional parent-subsidiary company arrangement. What forms and structures of groups should be captured by the group-wide AML/CTF program framework?

# Customer Due Diligence

## Why are reforms to CDD needed?

In line with the Statutory Review, the department proposes to reform the Act to more clearly set out the globally recognised core AML/CTF measures and reinforce the risk-based approach to regulation. The first round of consultation noted that Australia's AML/CTF regime focuses on procedure, rather than outcome, and outlined significant challenges that reporting entities face when trying to fulfil their CDD obligations.

[3] Recommendation 18 requires foreign branches and subsidiaries of Australian companies to apply home country AML/CTF requirements, where the requirements of the host country are less strict than the home country, to the extent permitted by local laws.

**What are the challenges with the current obligations?**

Currently, CDD obligations are overly detailed, complex and are substantively contained in the Rules despite being a core pillar of the AML/CTF regime. In some instances, the obligations are implied, which the department has heard makes it difficult for reporting entities to understand and comply with their obligations, and for AUSTRAC to issue clear but legally accurate guidance.

Additionally, the regime is comprised of distinct but interrelated concepts that are difficult to follow, understand and comply with. Finally, the regime currently has a procedural focus on *how* a reporting entity should fulfil its CDD obligations rather than describing the outcome to be achieved. For example, reporting entities are required to carry out the *applicable customer identification procedure* in respect of a customer, rather than being required to actually *know* their customer. There is also no express requirement for businesses to understand the risks presented by particular customers.

The department is committed to ensuring that CDD obligations are fit-for-purpose and balanced. Clarifying obligations under the regime will reduce the burden on businesses of interpreting complex provisions, and help regulated entities understand the outcomes they are expected to achieve.

The proposed reforms seek to focus on outcomes, and reporting entities would be empowered to mitigate, manage and respond to their risks in ways that best reflect their unique risks and that of their customers. The proposed reforms are also consistent with requirements outlined in FATF Recommendation 10.

## Overview of CDD reforms

CDD measures are at the foundation of reporting entities' obligations to identify, mitigate and manage the money laundering and terrorism financing risks that they may be exposed to through their customers. CDD helps reporting entities to verify the identity of their customers as well as to identify unusual transactions and behaviour, manage and mitigate risks arising from providing designated services and, when required, report suspicious matters to AUSTRAC.

The department proposes to replace the existing CDD framework and clearly outline the following core obligations of CDD:

- **Customer risk rating**
    - Reporting entities must assign each customer a risk rating that reflects the risks presented by the provision of a designated service to that customer.
- **Initial CDD**
    - Reporting entities must collect and verify information about the identity of a customer and understand potential risks involved in providing designated services to that customer before providing a service.
- **Ongoing CDD**

- Reporting entities must apply ongoing CDD measures to each customer proportionate to risk, including transaction monitoring and re-verifying Know Your Customer (KYC) information when appropriate.

The customer risk rating will determine what type of initial CDD and ongoing CDD is required:

- **Enhanced CDD**
  - Reporting entities must apply additional CDD measures to customers rated as *higher risk*, and to some specified relationships.
- **Simplified CDD**
  - Reporting entities may apply simplified CDD measures to customers rated *as low risk*.

In circumstances outside of enhanced CDD and simplified CDD, reporting entities may conduct **standard CDD** in line with requirements set out in the Rules.

Comprehensive guidance would be developed by AUSTRAC to provide details on how a reporting entity might implement the obligations and support reporting entities as they transition to the new AML/CTF regime. The reforms would also clarify that reporting entities are required to keep records obtained through any of the core CDD obligations outlined above. Reporting entities will also be required to assign a risk rating to existing pre-commencement customers, and there will be new triggers for undertaking initial CDD when there is a material change in the customer relationship that results in a rating of medium or high risk.

### Ensuring the AML/CTF regime remains technology neutral

The department is committed to ensuring that the Act and Rules remain technology neutral. Feedback from stakeholders indicated that some reporting entities may be unaware that the AML/CTF regime currently allows the use of electronic data for customer identification and verification purposes, providing the data is reliable and independent. Additionally, the reforms will provide flexibility to reporting entities about how they fulfil their CDD obligations commensurate to customer risk. This will support the use of new and developing technologies so long as a reporting entity can demonstrate how such technologies are sufficient to meet their AML/CTF obligations.

The department is also working with the Department of Finance in considering how changes to Australia's Digital Identity Framework might be leveraged by reporting entities to comply with certain CDD obligations under the AML/CTF regime, whilst also ensuring compliance with relevant FATF Recommendations.

The figure on the following page provides a visual representation of how the core obligations of CDD would interact. The figure does not set out specific processes, and reporting entities will have the flexibility to develop CDD processes suitable for their business in their AML/CTF programs.

## Customer Risk Rating

Reporting entities must assign a risk rating to each customer ***before*** providing a designated service, and must ***update*** this rating as part of

*Initial CDD and initial risk rating occur in parallel and inform each other*

## Initial CDD

To inform the customer risk rating, reporting entities must **collect** 'Know Your Customer' (KYC) information related to the customer's identity and relevant related parties. Reporting entities must then **verify** the KYC information proportionate to risk ***before*** providing a designated service.

### Simplified (low risk)

*E.g. inferring (rather than collecting) KYC information based on the nature of the service, verifying less KYC information*

### Standard

*E.g. collecting and verifying KYC in line with the reporting entity's risk assessment, which must at least meet minimum requirements in the Rules*

### Enhanced (high risk)

*E.g. verifying more KYC information and/or applying additional controls such as senior manager approval to provide services*

*Through initial CDD, a reporting entity must believe on reasonable grounds that it knows the identify of its customer. The Rules will establish minimum KYC information collection and verification requirements for customer types, such as individuals, bodies corporate and trusts. Reporting entities will retain flexibility in how to meet initial CDD obligations in practice.*

## Ongoing CDD

Reporting entities must monitor and apply ongoing CDD measures proportionate to risk for the duration of the relationship with the customer, and to identify potentially suspicious occasional transactions.

### Simplified (low risk)

*E.g. less frequent review and re-verification (where required) of KYC information*

### Standard

*E.g. collecting and verifying KYC in line with the reporting entity's risk assessment, which must at least meet minimum requirements in the Rules*

### Enhanced (high risk)

*E.g. collecting additional KYC information, re-verifying KYC information more frequently*

*Ongoing CDD must include transaction monitoring and, for customers in ongoing business relationships, keeping KYC information up to date and verified and, when required, updating the customer risk rating. Updating a customer risk rating to a different level may then also require re-verifying KYC information or trigger the collection and verification of additional information.*

## Clarifying that reporting entities must assign a risk rating to each customer

A risk-based approach to CDD requires that a reporting entity not only understand its entity or group-wide risks, but also the risks presented by the provision of a designated service to a particular customer. As such, the department proposes to establish an explicit, outcomes-focussed obligation for reporting entities to understand customer risk.

A reporting entity must assign a risk rating to each customer before commencing the provision of a designated service to that customer, and must update this rating as part of ongoing due diligence where appropriate. In assigning a risk rating, the reporting entity must consider:

- the reporting entity or group-wide risk assessment
- the nature and purpose of the business relationship or occasional transaction
- information collected about the customer, and
- any other risk factors present, including the customer type, jurisdiction risk, the type of designated service being provided and the method of delivery.

The department proposes that reporting entities would need to decide where each customer falls on their customer risk rating scale. A reporting entity would be able to determine the format of a risk rating scale and could be a matrix, a numerical scale or another means that best reflects a reporting entity's needs and risk tolerance. However, it must be clear from the scale where customers are high, medium or low risk. These risk ratings could be applied at the individual customer level or, where customers can be grouped by similar characteristics, applied across a cohort or grouping of similar customers. Customer risk ratings would need to be reassessed periodically and updated if necessary in response to any changes in the risks posed by a customer. Changes to the customer risk could be triggered by a customer seeking to use a designated service to engage with a new high-risk jurisdiction, or identifying that the customer's beneficial ownership structure has changed.

The department also proposes that the AUSTRAC CEO be empowered to make rules providing for specific risk factors to be considered as part of the customer risk rating, to allow flexibility and responsiveness to emerging risks and to provide clarity to reporting entities where required. This could include mandating a high-risk rating for certain customers in specified circumstances, for example, where a certain customer is connected with a country subject to sanctions.

### Clarifying 'initial customer due diligence'

The department proposes to replace the existing 'applicable customer identification procedures' (ACIP) with the term 'initial CDD'. The term 'initial CDD' more accurately reflects the purpose of this obligation and its operation under the CDD framework. It would shift the focus from prescriptive procedures to the outcome of knowing your customer and understanding the associated risk.

A reporting entity would typically undertake initial CDD prior to providing a designated service to a customer (subject to only limited exceptions set out below).

Initial CDD would require a reporting entity to collect and verify information about the identity of a customer, and to understand the potential risks involved in providing designated services to that customer.

The department proposes that reporting entities must verify their customer's identity (and other relevant information) using reliable and independent source documents, data or information. Collectively, this information would still be referred to as 'Know Your Customer information'. Before providing a designated service, a reporting entity must be reasonably satisfied that it knows:

- the identity of its customer
- the nature and purpose of the business relationship or occasional transaction
- the identity of the beneficial owners of its customer or the individuals on whose behalf the customer receives the designated service
- the ownership and control structure of its customer
- the identity of any person acting on behalf of the customer and their authority to act, and
- whether the customer or beneficial owner is a politically exposed person (PEP) or designated for targeted financial sanctions under an Australian sanction law. [4]

The Act would provide that the principle of 'being reasonably satisfied' involves two elements:

1. collecting information about, and verifying, a customer's identity, and
2. in the case of customers who are individuals, having reasonable grounds to believe that customer is who they claim to be (e.g. that the verified identity relates to the person receiving the service and has not been stolen).

The Rules would:

- establish the minimum information collection and verification requirements for a reporting entity to be reasonably satisfied that it knows the identity of its customer, and
- support rating the risk of providing designated services to the customer.

[4] Politically exposed persons (PEPs) are individuals who hold a prominent public position or role in a government body or international organisation, either in Australia or overseas. Immediate family members and close associates of these individuals are also considered PEPs.

PEPs hold positions of power and influence, including over government spending, procurement, development approvals and grants. As such, they can be targeted for corruption and bribery attempts, and ultimately for money laundering and terrorism financing activities. For this reason, it is important that reporting entities can identify, mitigate and manage any such potential risks. However, identifying an individual as a PEP does not automatically mean they are involved in criminal activities.

This includes specifying requirements in relation to identifying and verifying distinct customer types, such as individuals, bodies corporate and trusts. Reporting entities would retain flexibility in determining how to meet initial CDD obligations in practice.

**What would this look like?**

Initial CDD may include leveraging existing 'Know Your Customer' or CDD processes established to fulfil regulatory obligations outside of the AML/CTF regime. For example, as flagged above, pre-existing e-conveyancing processes that verify client identities such as the ARNECC Verification of Identity Standards may contribute to a business meeting its AML/CTF obligations. These frameworks or processes would not be explicitly outlined in the legislation. When they are utilised, reporting entities must be able to demonstrate that these processes meet the requirements of the AML/CTF regime or are appropriately supplemented to do so.

### Timing for initial CDD

The department proposes that in certain specified circumstances, the verification of 'Know Your Customer information' can be completed as soon as reasonably practicable after commencing the provision of a designated service, rather than always mandating a hard deadline as is currently the case. This would continue to apply only to circumstances identified in the Rules where additional risk associated with delayed verification is low and where it is essential to avoid interrupting the ordinary course of business. The current circumstances set out in the Rules, for example those relating to opening bank accounts, will be retained with more flexibility about timing of verification.

## Refining the requirements for ongoing CDD

Ongoing CDD obligations require reporting entities to monitor and understand their customers on an ongoing basis. Reporting entities must be able to detect any suspicious activities, unusual transactions, and material changes in their customer's behaviour. A reporting entity must apply ongoing CDD measures proportionate to risk throughout the course of a business relationship, as well as in relation to the provision of designated services provided as occasional transactions. Ongoing CDD must enable a reporting entity to:

- monitor transactions and behaviours that are unusual or to identify those that may give rise to SMR obligations under section 41 of the Act
- update and, where appropriate, re-verify 'Know Your Customer information', including to determine whether there have been changes in 'Know Your Customer information', or where the reporting entity has doubts about the adequacy or veracity of previously collected 'Know Your Customer information', and
- update the customer risk rating in accordance with information obtained through transaction and behaviour monitoring and re-verifying 'Know Your Customer information', or when the reporting entity determines the level of risk has changed.

The department proposes the Act would be amended to define 'unusual transactions or behaviour' as those that have no apparent economic or lawful purpose, or are inconsistent with what the reporting entity knows about:

- the customer
- the nature and purpose of the business relationship
- the customer risk or business profile, and
- where relevant, the source of funds.

This would extend the ongoing CDD requirement to monitor for unusual behaviour.

Reporting entities have indicated that the current regime leads to significant regulatory burden by requiring transactions to be monitored for 'all crimes.' To reduce this burden, the department proposes to streamline and focus the transaction monitoring requirement in line with FATF requirements related to designated categories of offences. Under the revised approach, reporting entities would be required to undertake risk-based, tailored transaction monitoring for:

- terrorism financing
- money laundering
- proliferation financing (where relevant)
- serious money laundering predicate crimes, and
- other serious crimes identified and assessed as material risks in their risk assessments.

Reporting entities would be able to design their monitoring processes around the frequency of transactions occurring within their business and on a risk basis. The Rules would outline the categories of serious money laundering predicate crimes and, as such, require consideration by reporting entities as part of their transaction monitoring program.

**What would this look like?**

For example, transaction monitoring would be expected to identify if a domestic business customer starts making frequent, large overseas transactions that are not typical of their usual transaction behaviour and which have no apparent lawful economic purpose. A large business may require software tools to assist in monitoring large volumes of transactions as opposed to smaller businesses with less frequent customer transactions, where an employee may be able to regularly monitor transactions using manual processes.

### Clarifying the application of ongoing CDD for a business relationship vs occasional transaction

To support the practical operation of ongoing CDD requirements, the department proposes to clarify how the requirements apply in relation to a business relationship and an occasional transaction. If a reporting entity provides a designated service as an occasional transaction, not all ongoing CDD measures need to be applied. For occasional transactions, ongoing CDD would

involve monitoring transactions and behaviours for suspicious or unusual activities over the course of the provision of service. It would not involve periodically re-verifying 'Know Your Customer information' or updating the customer risk rating as the need for these would be considered discretely for each occasional transaction.

If the customer is being provided with services as part of a business relationship, all ongoing CDD measures must be conducted throughout the relationship. To support the operation of these requirements, the department is considering defining the terms 'business relationship' and 'occasional transaction' in the regime. The proposed definitions can be found at page 25.

## Confirming when enhanced CDD must apply

Enhanced CDD captures those additional measures, both proactive and reactive, that reporting entities must apply to higher risk business relationships and occasional transactions, and to some specified relationships regardless of assessed risk. Enhanced measures must be applied to both initial CDD and ongoing CDD.

A reporting entity must apply enhanced due diligence measures proportionate to the risk where:

- it has rated the risk associated with providing the designated service to the customer as high
- there is a suspicion of money laundering, terrorism financing or identity fraud and the reporting entity proposes to continue the business relationship
- the customer or its beneficial owner is a foreign PEP, or
- the customer or its beneficial owner is physically present in, or is a legal entity formed in, a high-risk jurisdiction for which the FATF has called for enhanced due diligence to be applied.

The department's intention is that enhanced CDD measures must enable the reporting entity to continue to believe on reasonable grounds that it knows the identity of the customer, and to obtain additional information relevant to mitigating the identified higher risk.

The enhanced CDD framework will continue existing requirements related to senior management approval to establish or continue a business relationship with a foreign PEP, or a high-risk domestic or international organisation PEP. Reporting entities will also be required to take reasonable measures to establish the source of wealth and source of funds for such PEPs.

The department proposes the AUSTRAC CEO be empowered to make rules setting out specific circumstances or types of business relationships that AUSTRAC assesses should trigger enhanced CDD. These are not intended to be prescriptive but to allow flexibility and certainty in responding to current and emerging risks. The AUSTRAC CEO would also be given a power to prescribe certain types of business relationships as high-risk which would trigger enhanced CDD, as well as optional or mandatory enhanced CDD measures to be applied to high-risk customers.

**What would this look like?**

For example, Henry, a potential customer of Lucra Ltd, is identified as a foreign PEP during the customer risk rating and initial CDD processes. Lucra Ltd is now required to undertake enhanced initial CDD measures, in accordance with their policies, systems and controls, prior to the commencement of the designated service with Henry. This includes seeking and documenting approval from a senior manager to establish the business relationship and asking Henry to provide evidence of the source of the funds relevant to the transaction. Throughout the course of the business relationship, Lucra Ltd is required to apply enhanced ongoing CDD measures in accordance with its AML/CTF program.

## Streamlining the application of simplified CDD

The department proposes to allow simplified due diligence measures to be used for customers who pose low risk, removing the prescriptive approach in the existing framework. Increased flexibility in the use of simplified due diligence, where justified, may provide regulatory savings to reporting entities and reduce the need for frequent changes to the Rules.[5]

The department proposes that the Act be amended to clarify that a reporting entity may apply simplified CDD measures proportionate to risk where:

- it has rated the risk associated with the business relationship or occasional transaction as low, and
- none of the triggers for enhanced CDD apply.

Reporting entities would be provided with discretion to determine when simplified due diligence measures should be used and the extent to which their CDD measures should be simplified. This could include:

- reduced evidence requirements for verification
- not seeking information on the nature and purpose of the business relationship where this can be inferred from the designated service
- relying on the customer's advice about beneficial owners, and
- less frequently re-verifying 'Know Your Customer information' or different thresholds for transaction monitoring alerts.

**What would this look like?**

For example, Jimmy is an eight-year-old Australian child who opens a savings account with Savings and Loans Bank and deposits his $5 a week of pocket money. Given the value of the transactions, the limited use of the account and Jimmy's risk profile, Savings and Loans Bank assesses the risk of the business relationship with Jimmy as low. Jimmy also does not meet any of the triggers for enhanced CDD. Accordingly, in line with its AML/CTF Program, Savings and

[5] Recommendation 5.5 of the Statutory Review states that AUSTRAC should consider expanding the availability of simplified due diligence to low-risk designated services and customers.

Loans Bank verifies Jimmy's identity based on a birth certificate alone, combined with verifying the identity of a parent or guardian, and requires less frequent 'Know Your Customer' refreshes.

The Act would include a rule-making power to allow the AUSTRAC CEO to make rules mandating certain factors to be considered before applying simplified due diligence and to prohibit simplified due diligence in certain inappropriate circumstances. For example, factors for consideration could include particular types and location of customers and services. Introducing this rule-making power would ensure the regime remains flexible to emerging risks and particular areas of concern can be targeted in appropriate circumstances.

## Additional measures

### Record keeping for CDD

In compliance with FATF Recommendation 11, the department proposes to clarify that reporting entities are required to keep records obtained through any of the core CDD obligations outlined above (customer risk rating, initial CDD, ongoing CDD, enhanced CDD and simplified CDD). This includes records relating to any analysis or decisions that have been taken, such as a decision not to apply enhanced CDD, or to apply simplified CDD. All reporting entities regulated under the AML/CTF regime are required to comply with the *Privacy Act 1988* (Cth).

The department is committed to working with stakeholders to explore options to reduce the requirements for sensitive data retention, while maintaining the integrity of the AML/CTF regime. The department is also currently leading targeted engagement to implement the Government response to the Privacy Act Review, including in relation to the small business exemption.

### Existing customers

For reporting entities that came under the AML/CTF regime in 2007, pre-commencement customers are those that a reporting entity began to provide a designated service to before the commencement of the Act. Currently, these customers are treated differently for customer identification and verification purposes compared to post-commencement customers. This has resulted in a significant cohort of long-standing customers that have never had their identity verified for AML/CTF purposes, which exposes reporting entities and the broader financial system to significant risk.

To respond to this risk, the department proposes to transition pre-commencement customers for new and existing regulated entities into the AML/CTF regime over a specified period of time. This would ensure the risks associated with this currently unverified cohort of customers can be effectively identified and mitigated. In particular, the department proposes to:

- add a trigger for CDD for pre-commencement customers where there is a material change in the nature and purpose of the business relationship that results in medium or high risk, and

- extend the requirement for a customer risk rating to all pre-commencement customers to inform a risk-based transition into the regime. The Act would then require a reporting entity to collect and verify 'Know Your Customer information' about any pre-commencement customer who is rated as medium or high risk. 'Know Your Customer information' that has previously been collected and verified by a reporting entity could be used for this purpose, where appropriate.

Once a pre-commencement customer has been subject to CDD they would transition to being an ordinary customer for AML/CTF purposes.

The department seeks stakeholder feedback on what timeframes might be suitable for all pre-commencement customers to undergo a risk rating and transition medium and high-risk customers to regular customers under the AML/CTF regime.

### Defining a 'business relationship' and 'occasional transaction'

The department is considering defining the terms 'business relationship' and 'occasional transaction' in the regime. The term 'business relationship' is currently undefined, and the regime does not explicitly distinguish between circumstances where a reporting entity is providing a sustained designated service or set of designated services to a customer, and a one-off or occasional transaction. This raises questions about when a customer should be subject to ongoing CDD requirements, as well as when a reporting entity's ongoing CDD obligations end in relation to that customer.

To create a clear distinction between what ongoing CDD measures should be undertaken and when, the department proposes to define a business relationship as a relationship between a reporting entity and a customer involving the provision of a designated service that has, or is expected to have, an element of duration. An occasional transaction would be defined as the provision of a designated service to a customer outside a business relationship.

For example, a business relationship would include:

- a bank opening an account for a customer and allowing transactions in relation to that account over time (multiple point in time designated services), or
- a safe deposit box provider holding items in a safe deposit box over time (a single designated service with an element of duration).

An occasional transaction could include a currency exchange business exchanging foreign currency over the counter where the customer does not have an account and there are no other indications of an enduring relationship.

This measure is also relevant to the proposed approach to identifying pre-commencement customers for new reporting entities (real estate professionals, lawyers, accountants, trust and company service providers and dealers in precious metals and stones). For details on this proposal, please refer to the additional consultation papers.

**Consultation questions**

d. To what extent do the proposed core obligations clarify the AML/CTF CDD framework?
e. What circumstances should support consideration of simplified due diligence measures?
f. What guidance should AUSTRAC produce to assist reporting entities to meet the expectations of an outcomes-focused approach to CDD?
g. When do you think should be considered the conclusion of a 'business relationship'?
h. What timeframe would be suitable for reporting entities to give a risk rating to all pre--commencement customers?

# Exception for assisting an investigation of a serious offence

## Why are reforms needed?

Chapter 75 of the Rules allows the AUSTRAC CEO to exempt reporting entities from particular sections of the Act where providing a designated service to a customer would assist the investigation of a serious offence.

There is increasing demand for these exemptions and the department considers the current case-by-case application process initiated by investigative agencies and processed by AUSTRAC is administratively burdensome and inefficient. AUSTRAC operates as the intermediary between investigative agencies and reporting entities, performing largely an administrative role in this process and adding unnecessary time to the process. The scope of the exemption is also unnecessarily broad and inconsistent with international standards and best practice.

## Detailed proposal

The department proposes changing the process for issuing Chapter 75 exemptions by specifying in the Act that eligible law enforcement agencies can issue a 'keep open notice' directly to a reporting entity. An eligible law enforcement agency could issue a 'keep open notice' without requiring approval from AUSTRAC in circumstances where a senior delegate within the agency reasonably believes that maintaining the provision of a designated service to the customer would assist the investigation of a serious offence.

The Act would specify that a reporting entity is permitted to not perform certain CDD measures when they receive a 'keep open notice' from an eligible agency and the entity reasonably believes that performing those CDD measures would alert the customer to law enforcement interest. Under the proposed model, entities must still undertake CDD measures that can be carried out without alerting the customer, such as transaction monitoring.

A notice would not compel the reporting entity to continue to provide designated services to the customer. Rather, the reporting entity would be exempt from liability under the AML/CTF Act for keeping a customer's account open if it chooses to act in accordance with the notice. For

example, if the reporting entity is made aware by law enforcement that an account is held in a false name, the reporting entity would not be liable for an offence of providing a designated service to the customer using a false name if they continue to provide a service to that customer during the period of the notice.

Further, reporting entities would not be required to file an SMR where they receive a 'keep open notice' from an eligible agency, unless they independently develop grounds for suspicion.

The department also proposes to clarify that a reporting entity is permitted to not undertake specific CDD measures where they have independently developed a suspicion of money laundering or terrorism financing, and they reasonably believe that undertaking those measures would tip off the customer. This would eliminate any perceived inconsistency between CDD obligations and the tipping off prohibition. In these circumstances, the reporting entity would be required to file a SMR in accordance with existing obligations under section 41 of the Act.

### Safeguards for reporting entities

The department proposes to include safeguards to ensure that the quality of the process is upheld and to minimise regulatory impact on industry.

The form of the 'keep open notice' would be prescribed in the Rules, ensuring consistency and giving reporting entities certainty about the validity of a notice. While eligible agencies would be able to issue notices directly to reporting entities, notices must be copied to AUSTRAC when they are sent to reporting entities to allow AUSTRAC to maintain oversight of notices. AUSTRAC would have the ability to revoke notices that are considered invalid or do not meet the requirements of the Act and Rules.

Notices would be valid for six months unless terminated by the issuing agency. Eligible agencies would be required to advise AUSTRAC and the reporting entity if the investigation concludes prior to the expiry of the notice. Notices would be able to be extended by the issuing agency twice, for up to a total period of 18 months. Any further extension would require approval from the AUSTRAC CEO.

#### What would this look like?

A senior member of the Australian Federal Police (AFP) reasonably believes that John may be using his bank account with Big Bank to launder the proceeds of a drug dealing operation. In order to retain visibility while the offending is investigated, this senior AFP member issues a 'keep open notice' to Big Bank in relation to John's account. The 'keep open notice' is issued in the form specified by the Rules and a copy provided to AUSTRAC for visibility.

Big Bank had recently developed its own suspicions regarding John's transaction behaviour. Big Bank's AML/CTF program means it would normally apply enhanced CDD measures and potentially exit John as a customer if it determines that he exceeds the bank's risk appetite. However, due to the existence of the notice, the bank does not exit John as a customer and

opts not to re-verify John's identity in accordance with its enhanced CDD program as it holds a reasonable belief that it would alert John to the law enforcement interest. Big Bank does perform enhanced CDD measures that do not involve engagement with John, including conducting third party searches to try and identify information about John's source of wealth.

Big Bank is protected from any liability under the Act for maintaining the account while acting in accordance with the notice, including for not exiting John as a customer in accordance with its AML/CTF program. The investigation concludes four months later following John's arrest. The AFP notifies AUSTRAC and Big Bank that the notice is no longer in effect. Big Bank then manages John's account in line with normal processes.

# CDD exemption for gambling service providers

## Why does the CDD threshold need to be updated?

Chapter 10 of the Rules currently provides gambling service providers with an exemption from undertaking CDD obligations. This exemption applies for relevant gambling transactions, where the transaction is below the designated $10,000 threshold.

The gambling sector is often exploited by criminals seeking to launder the proceeds of their crimes, as it is an efficient way to launder cash that does not necessarily require significant skill. Exploitation occurs across multiple types of gambling operations, by a range of criminal entities. Therefore, the mechanisms in Australia's AML/CTF regime for regulation need to be consistently reviewed to ensure they remain effective and fit-for-purpose to address these risks.

FATF Recommendation 22 requires casinos to conduct CDD when customers engage in a financial transaction equivalent to or above a designated threshold. The FATF determines this threshold to be either USD3,000 or EUR3,000.

The exemption currently in Chapter 10 of the Rules has been in place since the introduction of the Rules in 2007. Therefore, the current threshold used in Australia has been well above the FATF threshold since the introduction of the AML/CTF regime. This drew criticism from FATF during Australia's 2015 Mutual Evaluation.

## Detailed proposal

The department proposes to lower the threshold exempting reporting entities from conducting CDD measures when providing certain gambling services to customers involving transactions from less than $10,000 to less than $5,000. The exemption is currently in the Rules, however, as part of the reforms the department proposes to shift this threshold into the Act.

This would strike the appropriate balance between aligning with the threshold set by the FATF, addressing the risks of the sector and minimising regulatory burden. The proposed $5,000 threshold would generally align the sector's CDD requirements to FATF Recommendation 22 (subject to exchange rate fluctuations). Further, a $5,000 threshold would align with current

electronic gaming machine requirements for payouts outlined in New South Wales and Queensland state legislation. Aligning with pre-existing legislation where possible would minimise the regulatory impact for gambling service providers, as requirements for businesses in these states would not change significantly.

The department is also seeking to ensure consistency across exemptions for different gambling services. The exemption for conducting CDD below a proposed $5,000 would be clarified to ensure that newer technology is explicitly captured in the exemption. This would not have any impact on how the exemption functions.

### What would you have to do?

The current exemption in Chapter 10 of the Rules covers casinos, oncourse bookmakers and TABs, and gaming machine venues. To ensure consistency in approach across all gambling service providers, the change to the designated threshold would apply to these three business types.

If the threshold is amended, gambling service providers would only be required to conduct CDD when providing any of the services outlined in the exemption when this transaction is equal to or greater than $5,000, unless they determined that enhanced CDD should be applied. Conducting CDD on these customers does not necessarily mean that their transaction needs to be reported to AUSTRAC through a suspicious matter report (SMR) or threshold transaction report (TTR). Requirements for this SMR or TTR reporting would remain unchanged.

Casinos would also continue to be exempt from conducting CDD when providing specified designated services involving amounts greater than $5,000 where the service involves the customer giving or receiving only gaming chips or tokens.

## Tipping off offence

If reporting entities submit, or are required to submit, a suspicious matter report (SMR), they must not disclose any information about the report, except in limited circumstances. The reporting entity must also not disclose any information or documents related to notices issued by an authorised agency under section 49 of the Act. [6] This is known as 'tipping off', and is prohibited under section 123 of the Act. A breach of the tipping off offence is a criminal offence.

The tipping off offence aims to:

- protect the reputation of the customer who is the subject of an SMR, who in some circumstances may be the victim of criminal activity

[6] Under section 49 of the Act, AUSTRAC or its partner agencies, may by written notice require a reporting entity to produce further information or documents in relation to a threshold transaction report, an IFTI report or a SMR. For example, if a bank has submitted a SMR due to a customer depositing a significant amount of cash, the bank may be required under a section 49 notice to produce information about other significant cash deposits the customer may have made.

- protect the privacy of individuals and entities involved in submitting the SMR, and
- mitigate the risk of criminals hiding their illegal activities if they become aware that their behaviour has raised suspicion.

## Why are reforms needed?

The tipping off offence and its exceptions aim to balance the need to disclose information to mitigate money laundering and terrorism financing risks without compromising law enforcement investigations. Feedback from the first round of consultation indicates that the current framework does not strike the correct balance.

The tipping off offence framework needs to be updated because it is complex and difficult to understand. The current structure of the tipping off offence has not kept up to date with modern business practices. The broad scope of the offence captures a large range of information sharing for legitimate business purposes, including sharing that would allow reporting entities to effectively identify, mitigate and manage their risks. Efforts to protect investigations should not also inhibit appropriate information sharing to prevent criminal activity in the first place.

The proposed reforms would simplify and modernise the tipping off offence to better support industry to comply with their AML/CTF obligations while balancing the need to protect the integrity of law enforcement investigations.

## Detailed proposal

The department proposes to reframe the tipping off offence away from a prescriptive prohibition on disclosing that a reporting entity has given or is required to give an SMR or information related to a section 49 notice, or information from which this could be inferred.

Instead, the new offence will focus on preventing the disclosure of SMR information or section 49 related information where it is likely to prejudice an investigation or potential investigation. The proposed change to the tipping off offence framework would better target the underlying harms the offence is intended to prevent while being more flexible for reporting entities.

By amending the offence in this way, the new framework would clarify that reporting entities can disclose information for legitimate purposes. This includes sharing information within business groups to manage and mitigate risks in accordance with the controls and business processes that will be outlined in the group's AML/CTF program. The department is also considering framing the offence in a way that could help facilitate private-to-private information sharing in future subject to appropriate protections being in place.

### What would this look like?

If reporting entities submit, or are required to submit, a SMR, they must not disclose any information about the report, where such disclosures would prejudice an investigation or potential investigation.

For example, disclosing SMR information directly to the person of interest or an associate would constitute tipping off, whereas disclosure to another entity within a business group or to an Australian Government regulator would not.

Intentional disclosure would be an offence, as would reckless or negligent disclosures, for example, where a disclosure occurs as a result of a reporting entity's failure to develop, implement or maintain adequate measures to prevent tipping off.

The new offence would apply to a person who is or has been:

- a reporting entity
- an officer, employee or agent of a reporting entity, or
- required to give information or produce documents in response to a section 49 notice.

Restructuring the tipping off offence framework would mean a broader cohort of persons could receive SMR and section 49 notice information. Reporting entities would be required to implement controls and protections around SMR and section 49 notice related disclosures as part of their internal AML/CTF controls and business processes. For example:

- reporting entities could be required to be reasonably satisfied that the proposed recipients have appropriate policies, systems and controls in place such as employee screening and AML/CTF training
- reporting entities could be required to specify in their AML/CTF programs the circumstances under which they would disclose SMR and section 49 notice information and how they would manage and mitigate the risks of tipping off, and
- reporting entities could be required to specify in their AML/CTF programs the controls related to sharing SMR and section 49 notice information with offshore employees, including physical controls, systems and training.

### Consultation questions

i. Are there situations where SMR or section 49 related information may need to be disclosed for legitimate purposes but would still be prevented by the proposed framing of the offence?
j. Are there any unintended consequences that could arise due to the proposed changes to the tipping off offence?

# Moving some exemptions from the Rules to the Act

## Why are changes to the exemption provisions needed?

Various provisions within the Act permit the AUSTRAC CEO to make rules exempting designated services from the Act or some of its provisions. The Rules currently contain 43 rules-based exemptions, the majority of which are made under section 39 (exemptions relating to identification procedures) or section 247 (general exemptions) of the Act.

Given the extent of proposed reform, it is likely that the Rules instrument would be repealed and remade in its entirety rather than amended, meaning that the exemptions contained within it will also need to be remade. The proposed reforms are an opportunity to embed some enduring exemptions, especially those that clarify the regulatory scope of the AML/CTF regime, into the Act.

The Senate Standing Committee for the Scrutiny of Delegated Legislation (the Committee) has concerns about delegated legislation that includes exemptions from the operation of the primary legislation, as it may limit parliamentary oversight. The Committee has previously expressed its position that an instrument which contains exemptions from primary legislation should cease to operate no more than three years after the commencement date for the instrument. However, many exemptions in the Rules have been in place for many years and are intended to be enduring. As such, the department considers these exemptions should be codified in the Act.

## Detailed proposal

The department proposes to move these enduring exemptions from the Rules to the primary legislation, either by reframing the primary obligation to avoid the need for the exemption, or incorporating an express exception in the Act. This includes exemptions related to gambling services, CDD threshold exemptions, registration exemptions, and exemptions for certain services that are not intended to be captured by the AML/CTF regime.

Legislating the exemptions would:

- ensure that exemptions which are intended to be enduring are codified in the legislation rather than remade as time-limited rules-based exemptions, providing regulatory certainty
- align with the expectations of the Committee regarding parliamentary oversight of exemptions, and
- minimise the risk of non-compliance with subsection 212(3A) of the Act (the requirement for exemptions made by the AUSTRAC CEO to be based on proven low money laundering and terrorism financing risk).

Some exemptions which are limited in scope or timeframe or are likely to require amendment to adapt to changing circumstances will be retained in the Rules to allow greater flexibility.

# Repealing the *Financial Transaction Reports Act 1988*

## Why is the FTR Act no longer needed?

The department proposes to repeal the FTR Act to streamline and simplify obligations, and establish a single source of obligations for industry. Repeal of the FTR Act was overwhelmingly supported in the first round of consultation.

The only entities which currently retain reporting obligations under the FTR Act are:

- businesses that buy and sell traveller's cheques
- online remitters which do not provide designated services at or through a permanent establishment in Australia
- motor vehicle dealers who act as insurance providers or intermediaries, and
- solicitors.

If the FTR Act is repealed, a cohort of cash dealers currently regulated under the FTR Act, other than solicitors when they provide one of the proposed new designated services, would become deregulated for AML/CTF purposes. A key priority is to focus on regulating sectors that are internationally recognised as most vulnerable to criminal exploitation. This residual cohort of cash dealers is not identified in this category, nor are they required to be regulated by the FATF. Transitioning them into the Act would therefore impose undue regulatory burden on these industries. As such, the department proposes the deregulation of these remaining cash dealers for AML/CTF purposes.

## Consultation questions

a. Under the outlined proposal, a business group head would ensure that the AML/CTF program applies to all branches and subsidiaries. Responsibility for some obligations (such as certain CDD requirements) could also be delegated to an entity within the group where appropriate. For example, a franchisor could take responsibility for overseeing the implementation of transaction monitoring in line with a group-wide risk assessment. Would this proposal assist in alleviating some of the initial costs for smaller entities?
b. The streamlined AML/CTF program requirement outlined in this paper provides that the board or equivalent senior management of a reporting entity should ensure the entity's AML/CTF program is effectively identifying and mitigating risk. To what extent would this streamlined approach to oversight allow for a more flexible approach to changes in circumstance?
c. Many modern business groups use structures that differ from the traditional parent-subsidiary company arrangement. What forms and structures of groups should be captured by the group-wide AML/CTF program framework?
d. To what extent do the proposed core obligations clarify the AML/CTF CDD framework?
e. What circumstances should support consideration of simplified due diligence measures?
f. What guidance should AUSTRAC produce to assist reporting entities to meet the expectations of an outcomes-focused approach to CDD?
g. When do you think should be considered the conclusion of a 'business relationship'?
h. What timeframe would be suitable for reporting entities to give a risk rating to all pre-commencement customers?
i. Are there situations where SMR or section 49 related information may need to be disclosed for legitimate purposes but would still be prevented by the proposed framing of the offence?
j. Are there any unintended consequences that could arise due to the proposed changes to the tipping off offence?

# Table 1 – Proposed model of reforms to simplify, clarify and modernise the regime

| | |
|---|---|
| AML/CTF programs | A reporting entity is required to detail the risk-based policies, systems and controls it implements and maintains in the provision of a designated service. This is known as an AML/CTF program.<br><br>The AML/CTF program will be informed by a clear requirement to conduct and document an assessment of the risk that the provision of a designated service may facilitate money laundering, or finance terrorism or weapons of mass destruction. The Act will:<br>• clarify that reporting entities must implement proportionate risk mitigation measures.<br>• clarify that reporting entities must maintain internal controls to ensure their business and its employees comply with their AML/CTF obligations<br>• provide clarity on the roles and responsibilities of a reporting entity's board or equivalent senior management and its AML/CTF Compliance Officer.<br>• clarify the obligations to be applied to a reporting entity's foreign branches and subsidiaries. |
| | A new 'business group' concept will be established to allow the head of a business group to manage common risks, information sharing and compliance obligations for all parts of the business. |
| Customer Due Diligence | The core CDD obligations will be:<br>• Customer risk rating: reporting entities must assign a risk rating to each customer<br>• Initial CDD: before providing a designated service, reporting entities must collect and verify information about the identity of a customer and understand potential risks of that customer.<br>• Ongoing CDD: reporting entities must apply ongoing CDD measures proportionate to customer risk.<br><br>The customer risk rating will determine what type of initial CDD and ongoing CDD reporting entities must conduct.<br>• Enhanced CDD: reporting entities must apply additional measures to higher risk customers, and to some specified relationships.<br>• Simplified CDD: reporting entities may apply simplified due diligence measures to low risk customers.<br><br>In circumstances outside of enhanced CDD and simplified CDD, reporting entities may conduct standard CDD in line with requirements set out in the Rules. |

| | |
|---|---|
| | Current pre-commencement customers will have new triggers for CDD and requirements for customer risk rating applied. |
| | The reforms will change the process for issuing Chapter 75 exemptions (continuing to provide designated services to a customer/s that is the subject of an exemption). In particular, the legislation will specify that eligible law enforcement agencies can issue 'keep open notices' directly to reporting entities, and permit entities to not perform CDD measures when they receive a notice. However, reporting entities will still be required to conduct CDD measures that can be carried out without alerting the customer. |
| | The designated threshold in the CDD exemption for gambling service providers would be lowered from transactions below $10,000 to transactions below $5,000. |
| Tipping off offence | The current tipping off offence will be updated to focus on preventing the disclosure of suspicious matter report (SMR) information or section 49 related information (information produced in response to a notice from an authorised agency on a threshold transaction report, an international funds transfer instruction report or an SMR) where it is likely to prejudice an investigation or potential investigation. |
| Administrative changes to legislation | The FTR Act would be repealed as obligations are largely captured under the AML/CTF Act and most cash dealers no longer have reporting obligations under the FTR Act. |
| | Some exemptions need to be remade in the Act rather than the Rules. None of these exemptions will be amended in substance. |