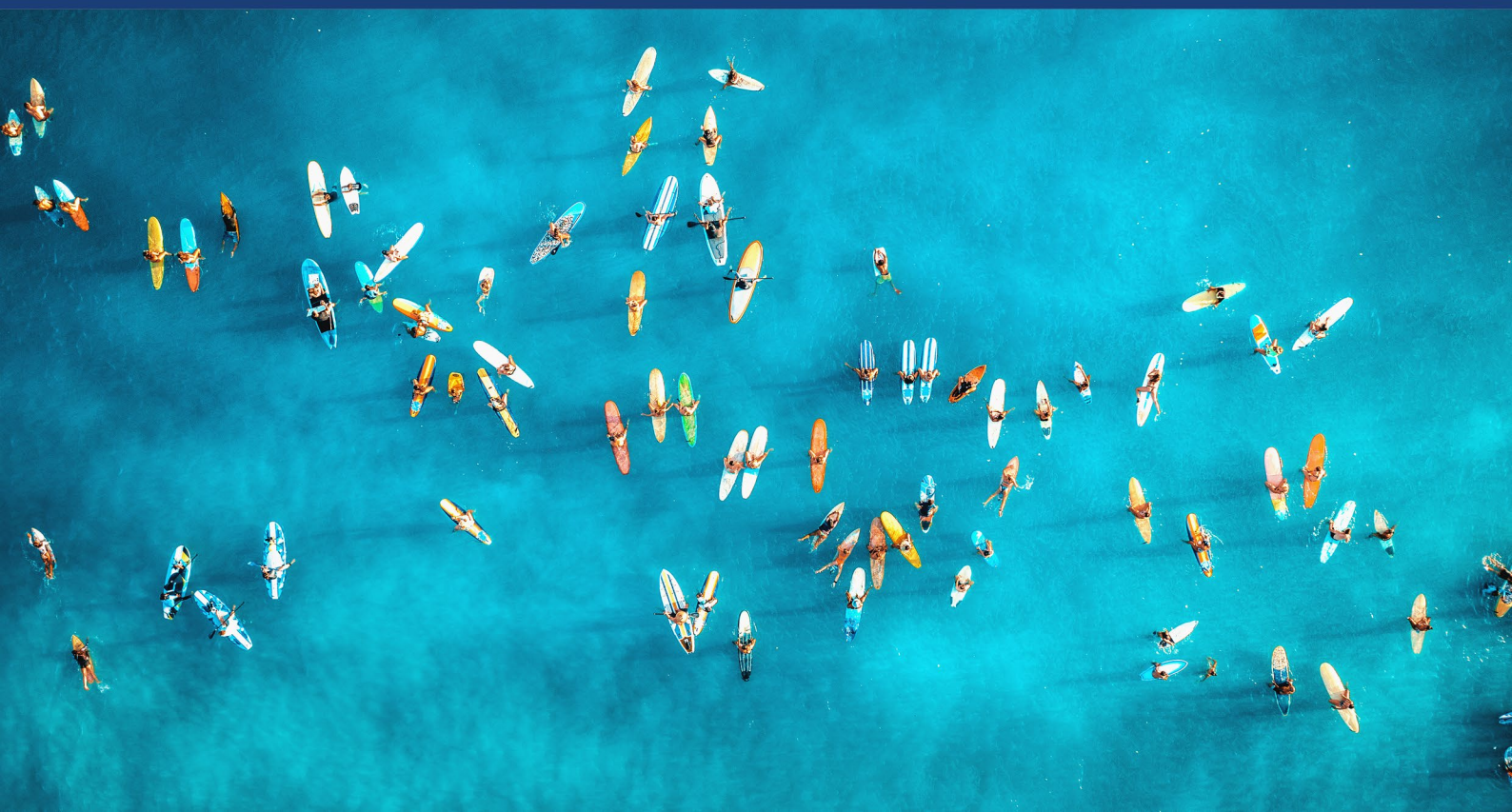
HERBERT SMITH FREEHILLS

JINGLE BILLS

UNWRAPPING THE AML/CTF REFORMS PASSED BY PARLIAMENT AND AUSTRAC'S CONSULTATION PAPER



Contents

Jingle bills: unwrapping the AML/CTF reforms passed by Parliament and AUSTRAC's consultation paper

Authors: Alice Molan, Charlotte Henry, Bryony Adams, Julia Massarin, David Curley, Daniel Hyde and Ayman Shash

The passage of the bill to amend the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**AML/CTF Act**) through the Federal Parliament during the final sitting week for 2024 marks a significant milestone on the journey to reform Australia's AML/CTF regime. The *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2024* (Cth) (**Amendment Act**) received royal assent on 10 December 2024, starting the clock for reporting entities to engage with the substance of the reforms. For existing reporting entities, the majority of the provisions in the Amendment Act commence on 31 March 2026, save for amendments to the 'tipping off' offence provisions and new investigation powers for AUSTRAC which take effect in the first quarter of 2025.

Consultation Paper and Draft Rules

AUSTRAC has moved quickly to release its consultation paper on the new AML/CTF Rules (**Consultation Paper**), as well as publishing the first exposure draft of the *Anti-Money Laundering and Counter-Terrorism Financing Rules* on 11 December 2024 (**Draft Rules**). As much of the granular detail required to comply with the AML/CTF Act is captured in the AML/CTF Rules, AUSTRAC have proposed a wholesale rewrite in the Draft Rules to align with the reforms in the Amendment Act.

The Draft Rules cover the revised requirements for comment in connection with:

- AML/CTF programs;
- reporting groups (formerly 'designated business groups');
- customer due diligence;
- travel rule;
- compliance reports;
- keep open notices (formerly 'Chapter 75 notices'); and
- correspondent banking relationships.

Making a submission and what's next

AUSTRAC is accepting submissions in response to the Consultation Paper and Draft Rules until 14 February 2025. AUSTRAC will then release a second exposure draft of the Draft Rules including updates in response to the Consultation Paper feedback, as well as covering topics not addressed in the first Consultation Paper. Areas of the existing AML/CTF Rules that cover exemptions will be published in separate standalone exemption rules.

About this article

In this article we have focussed on the impact that the Amendment Act and Draft Rules will have on existing reporting entities. This article does not seek to examine every aspect of the reforms – you can read more background on these reforms in our previous articles available here and here. We would be pleased to discuss any aspect of the reforms that may impact on your business.

AML/CTF Programs get a makeover

A quick recap on reforms affecting AML/CTF Programs

Overview of the Amendment Act's impact on AML/CTF Programs

The Amendment Act will implement a wholesale re-write of the provisions relating to AML/CTF Programs through the introduction of new Part 1A into the AML/CTF Act. As explained in our previous articles, some key features of the Amendment Act in connection with AML/CTF Programs include:

- removing the distinction between Part A and Part B of an AML/CTF Program;
- making a reporting entity's money laundering, terrorism financing and proliferation financing (**ML/TF**) risk assessment (**ML/TF Risk Assessment**) a component of the AML/CTF Program;
- including a reporting entity's anti-money laundering and counter-terrorism financing (**AML/CTF**) policies, procedures, systems and controls (**AML/CTF Policies**) as part of the AML/CTF Program; and
- providing that a breach of the AML/CTF Policies is a civil penalty provision.

Risk Management and Internal Compliance Management Policies

While the Amendment Act removed the concept of Part A and Part B, it introduced new language in the framing of AML/CTF Policies. In particular, the Amendment Act provides that AML/CTF Policies must be developed and maintained to:

- appropriately manage and mitigate the risks of ML/TF that the reporting entity may reasonably face in providing its designated services (**ML/TF Risk Management Policies**); and
- ensure that the reporting entity complies with the obligations imposed by the AML/CTF Act, regulations and AML/TF Rules that apply to the reporting entity (**Compliance Management Policies**).

The specific areas that the AML/CTF Policies need to cover, as outlined on in both the Amendment Act and the Draft Rules, link to one of these categories – being either ML/TF Risk Management Policies or Compliance Management Policies.

What is proposed in the Draft Rules?

While the Amendment Act includes detailed expectations in connection with the content of AML/CTF Policies, additional requirements are proposed to be included in the AML/CTF Rules.

Compliance Management Policies

Under the Draft Rules, AML/CTF Policies must cover the following matters under its Compliance Management Policies:

- the establishment of safeguards to prevent tipping off provisions of the AML/CTF Act being contravened;
- the provision of information to the governing body of the reporting entity to enable that governing body to fulfil its responsibilities under the Act;
- reporting from the AML/CTF Compliance Officer. This includes that the AML/CTF Policies must provide for the reporting to occur regularly, with a frequency of at least once every 12 months;
- matters that the reporting entity must assess in undertaking due diligence in connection with its personnel as well as in providing initial and ongoing training to staff;
- matters that must be covered as part of an independent evaluation, including the production of a written report and the delivery of that report to the governing board and any senior manager responsible for approvals of the AML/CTF Program. It also requires the Policies to deal with reviewing and updating those Policies following an independent review if required;
- ensuring information reported to AUSTRAC is complete, accurate and free from unauthorised change when lodging suspicious matter reports (**SMR**), as well as reporting threshold transactions, international value transfer reports and connected reports; and

- enabling the timely review of material that is relevant to SMRs and ensuring determination as soon as reasonably practicable of whether the entity suspects grounds for making a report as prescribed by the Act.

ML/TF Risk Management Policies

In connection with ML/TF Risk Management Policies, the Draft Rules provide that AML/CTF Policies must cover the following:

- ensuring that the approval of a senior manager is obtained:
  - in connection with certain politically exposed persons (**PEPs**) in prescribed circumstances;
  - before entering into an ongoing reliance agreement under section 37A of the AML/CTF Act (described further below); and
  - before providing a designated service as part of a "nested services relationship";
- ensuring that a senior manager of the reporting entity is informed before making a payment under a life policy or sinking fund policy if the ML/TF risk if the customer is high;
- where the reporting entity acts as an ordering institution in relation to the transfer of a virtual asset, certain matters in connection with conducting due diligence on the wallet (including whether it is custodial or self-hosted), the regulated status of the wallet controller and other matters connected to the management and mitigation of ML/TF risk;
- where the reporting entity acts as beneficiary institution in relation to a transfer of value, certain matters in connection with the monitoring of information received, determining whether to make transferred value available and whether to request further information from another institution in the value transfer chain. Additional matters must be included if the designated service is provided in relation to the transfer of a virtual asset; and
- where the reporting entity acts as the intermediary institution in relation to a transfer of value, certain matters must be included in connection with monitoring information received, passing on transfer messages and determining whether to request further information from another institution in the value transfer chain.

Approving and keeping AML/CTF Program up to date

The Amendment Act requires that the AML/CTF Program must be documented within any period specified in the Rules. The Draft Rules propose that:

- the ML/TF Risk Assessment must be undertaken and the AML/CTF Policies developed before the reporting entity first commences providing a designated services; and
- if the ML/TF Risk Assessment or the AML/CTF Policies are updated, the AML/CTF Program must be updated within a prescribed period. This prescribed period is left "*to be drafted*" in the Draft Rules. The Consultation Paper is asking for feedback on what would be a reasonable period to document the updates.

Key considerations in implementing AML/CTF Program updates

Implementation consideration	Insights
Tipping off safeguards	Section 10 of the Draft Rules requires that AML/CTF policies must deal with "establishing safeguards *to prevent any* contravention of subsection 123(1) by the reporting entity, or an officer, employee or agent…including *by ensuring* the confidentiality and appropriate use of [the] information" (emphasis added). The Draft Rules therefore, seemingly set a very high bar for reporting entities in how to manage disclosures that might breach the tipping off restriction, and one that is much more onerous than suggested by the wording in the substantive tipping off prohibition itself (of the disclosure prejudicing or being reasonably expected to prejudice, an investigation). The strictness of this requirement may cause a chilling effect on reporting entities who avoid availing themselves of the full benefit of the revised tipping off regime for fear of any inadvertent and unintended disclosure exposing them to a civil penalty. It also suggests that this section of AML/CTF Policies may need to be comprehensive and cater for a wide range of potential disclosures that may conceivably arise in a reporting entity's business.
Provision of information to, and reporting to, the governing body	The exercise of appropriate and ongoing oversight by governing bodies has been a focus of AUSTRAC for a number of years. AUSTRAC has stated that its regulatory priorities during 2024 include board and executive accountability for maintaining a culture of AML/CTF compliance and risk management. This expectation of ongoing oversight is embedded into new Division 4 of Part 1A of the AML/CTF Act. The Draft Rules propose that the AML/CTF Policies must deal with: • the provision of information to the governing body to enable the governing body to fulfil its responsibilities; and • ensuring that the governing body receives reporting from the AML/CTF Compliance Officer on specified matters. Given AUSTRAC's interest in this area we expect that reporting entities will have been focussed on these governance and information flows over recent years. How this is documented should be reviewed to ensure that this is consistent with the updated regime. In addition, while the Draft Rules propose that the AML/CTF Policy should provide for the AML/CTF Compliance Officer to report at least every 12 months, this should not be taken to be a signal to reduce reporting that is already in place where this has been determined appropriate for the proper oversight and engagement of the governing body.
Assessing potentially suspicious matters	Section 18 of the Draft Rules will require reporting entities to ensure their AML/CTF Policies provide for both: • the "timely review" of unusual activity that may lead to a relevant suspicion for the purposes of section 41 of the AML/CTF Act; and • "*ensuring…as soon as practicable*" the determination with respect to any such suspicion. To the extent that reporting entities do not already do so, this will require mechanisms for these steps to occur, **as well as** quality control measures that actively monitor the timeliness of these steps. While the Draft Rules are not prescriptive as to the timeframes in which these steps must occur (which will no doubt be a relief to many reporting entities dealing with large volumes of unusual activity escalations and suspicion determinations), reporting entities should be

Implementation consideration	Insights
	prepared to defend where necessary how their review timeframes are appropriate in the circumstances. This will also likely require the ability to draw quickly upon additional resourcing when needed so potential non-compliance can be avoided.
Approval of PEPs	In addition to imposing additional customer due diligence (**CDD**) and ongoing customer due diligence (**OCDD**) requirements with respect to PEPs (see below), Draft Rule 19 requires that a reporting entity's AML/CTF Policies ensure a newly defined "senior manager" of the reporting entity approves certain PEP relationships *prior* to the provision of designated services. That requirement applies to all foreign PEPs, and high risk domestic and international organisation PEPs (and the definitions of these include, among others, certain family members of PEPs). The concept of obtaining approval to provide designated services to these types of PEPs is not new (see existing Rule 4.13.3). However, the Draft Rules do raise some new practical considerations. **The role and responsibility of the senior manager** The "senior manager" concept has been introduced and defined in the Amendment Act. This is a person "*who makes, or participates in making, decisions that affect the whole or a substantial part, of the business*". Consultation Paper 2 contemplated that the role would be fulfilled by an individual such as a Chief Risk Officer. The term, as defined, is similar to the concept of "officer" under the *Corporations Act 2001* (Cth). Under the Amendment Act, one or more senior managers must be designated with responsibility for approving the AML/CTF Policies and ML/TF Risk Assessment of the reporting entity. It is apparent that the senior manager has a particularly senior role in an organisation. While the AML/CTF Rules currently require all foreign PEPs and high risk domestic and international organisation PEPs to be subject to "senior management" approval, this may be approval from persons that may not now meet the new definition of a "senior manager" – they may not be involved in decisions affecting the whole or a substantial part of the business. **Timing of approval – senior manager engagement** Obtaining the prior approval of a person that meets the definition of "senior manager" may raise practical difficulties in obtaining this approval within a commercially feasible timeframe. Business interruptions and delays may arise at onboarding in circumstances where that approval cannot be obtained promptly. This will also require that the designated senior manager(s) have the appropriate capacity, as well as the training and understanding of the potential AML/CTF risks and corresponding controls to ensure those approvals are sufficiently informed. For some, this may be a step-change from focusing the detailed knowledge of AML/CTF risks and controls within specialised departments. **Timing of approval – interaction with Draft Rule 32** As part of the Consultation process, there has been significant noise in the market around the need for a "day 2" process on PEP and sanctions screening. This has been addressed in Draft Rule 32 which would allow PEP and sanctions screening to be delayed where prescribed conditions are met.

Implementation consideration	Insights
	However, this delay does not sit comfortably with Draft Rule 19 which requires that Policies "ensure" approval is obtained "before" the designated service is provided. This may be an area for submission to ensure consistency within the Rules so that Rule 19 does not undermine the flexibility offered by Rule 32.
Independent evaluation	The current AML/CTF Rules require Part A of an AML/CTF Program to be subject to regular independent review. While the independent review must assess the effectiveness of Part A, there is no prescribed requirement in connection with a review of Part B and associated implementation of customer due diligence measures. The Amendment Act, together with the Draft Rules, requires a more holistic review to be undertaken of a reporting entity's AML/CTF Policies. The Draft Rules 15 and 16 propose that the AML/CTF Policies must require a number of measures to be undertaken as part of "independent evaluations", including prescribing that the AML/CTF policies must cover the production of a report, the delivery of the report to the board and senior manager and steps required to be taken following an independent evaluation where adverse findings are made. Any reporting entity that has previously focussed only on Part A in its independent reviews will need to ensure that a most holistic approach is undertaken going forward, and that this is reflected in its AML/CTF Policies.

Customer due diligence [CDD]

A quick recap on customer due diligence reforms

The Amendment Act has largely replaced the CDD provisions contained in Part 2 of the current AML/CTF Act. As part of these changes, the concept of 'applicable customer due diligence' has been removed and 'initial customer due diligence' has been introduced.

The updated provisions under the Amendment Act are intended to make the CDD process more focused on outcomes, rather than the procedures, allowing greater flexibility for reporting entities to determine the steps that they should take to know their customers.

What is proposed in the Draft Rules?

The Draft Rules on CDD are significant and wide ranging. They represent a wholesale rewrite to the prescriptive requirements under the existing AML/CTF Rules and will require reporting entities to carefully engage with their current approaches in onboarding and monitoring customers.

While the Draft Rules prescribe detail in connection with CDD that supplements the Amendment Act, the requirements in the Draft Rules are far less granular than the approach taken under the current AML/CTF Rules. For example, the prescribed minimum collection and verification steps for prescribed customer types has been removed.

The Draft Rules propose measures additional to the Amendment Act in connection with CDD in the following areas:

CDD	Draft Rules overview
Initial CDD	The Draft Rules contain additional detail in respect of the conduct of initial CDD, distinguishing between individual customers and customers where the designated service is proposed to relate to the customer's conduct of a business (ie an individual obtaining a service for a business purpose)
Exemptions	The Draft Rules provide for certain exemptions from initial CDD, including delaying elements of initial CDD in prescribed circumstances. This includes in connection with PEPs as described earlier in this article.
Deemed compliance	In certain circumstances a reporting entity will be deemed to have complied with the initial or ongoing CDD requirements of the Amendment Act. The Draft Rules provides for deemed compliance including under transitional provisions, compliance with laws of foreign countries (described further in this article) as well as embedding expectations in providing services to customers that do not have traditional evidence of identity (an area that AUSTRAC has provided guidance on in the past). The Draft Rules also provide for deemed compliance with ongoing monitoring obligations where unusual transactions and behaviours are monitored for in connection with prescribed offences. This is a broader list than ML/TF offences and reflects the value of broader serious crime intelligence to AUSTRAC in fulfilling its functions.
Simplified and enhanced CDD	The Draft Rules contain some further expectations in connection with simplified and enhanced CDD, although with minimal prescription in these areas, particularly in respect of simplified CDD.
PEPs	The Draft Rules include specific expectations in connection with PEPs, aspects of which we have considered above.

CDD	Draft Rules overview
Nested services relationships	Additional expectations are provided in connection with initial and ongoing CDD for nested services relationships. The Draft Rules prescribe an extensive list of additional matters that must be addressed as part of the initial and ongoing CDD requirements for nested service relationships.
Other CDD areas	We have separately considered the updates to the Draft Rules in connection with reliance arrangements and keep open notices in this article.

Key considerations in implementing CDD reforms

Implementation consideration	Insights
Mapping of current approach to collection and verification against the Draft Rules	Although there is a grandfathering of CDD conducted by reporting entities before 31 March 2026, reporting entities will need to undertake a gap analysis of their current processes, procedures and policies to ensure that they comply with the new principles-based requirements proposed in the Draft Rules that flow from the changes to CDD in the Amendment Act. Detailing how CDD is carried out in accordance with Part 2 of the Amendment Act (which include the accompanying Rules) is a matter that must be covered in a reporting entity's ML/TF Management Policies. It is likely that current Part B of AML/CTF Programs will need to be revisited, at least to some extent, to meet the requirements of the updated regime.
Collection and Verification of place of birth	In implementing the outcomes focused approach to CDD, the Amendment Act requires a reporting entity to establish certain matters on '*reasonable grounds*' before providing designated services.[1] There is generally very little prescription in how this is satisfied and, subject to certain exceptions, the Draft Rules continue this principles-based approach. However, for designated services that are subject to travel rule obligations, Draft Rule 25 requires a reporting entity to collect and verify at least the following KYC information about the customer: • date of birth; and • place of birth. Place of birth is not KYC information that is contemplated as minimum KYC information in the existing AML/CTF Rules. The Consultation Paper contemplates that AUSTRAC will issue guidance on how reporting entities can comply with this obligation. However, given the limited documents that would contain a person's place of birth, it would appear that reporting entity's will be restricted in how they comply with this obligation.
Trustees – section 28(2) establishing the identities of beneficiaries	The Amendment Act has introduced a requirement for a reporting entity to establish the identity of any person on whose behalf a customer is receiving the designated service. The supporting explanatory materials to the Amendment Act contemplate that, if the customer is a trustee, the beneficiaries of the trust are the persons on whose behalf the customer (trustee) is receiving the designated service. Accordingly, the identity of beneficiaries of a trust must be established on reasonable grounds.

[1] The matters that must be established on reasonable grounds include the identity of the customer and any person on whose behalf they are receiving the designated service, the identity of agents, beneficial owners, whether the customer (or a beneficial owner) is a PEP or subject to sanctions and the nature and purpose of the business relationship or occasional transaction.

Implementation consideration	Insights
	When providing services to a trustee, the current AML/CTF Rules contemplate that CDD obligations in connection with beneficiaries of the trust may be satisfied by collecting the name of each beneficiary or a description of each class of beneficiary. The Draft Rules require reporting entities to go further than collecting just the class of beneficiaries. The Draft Rules provide that, where, because of the nature of the trust it is not possible to identify each beneficiary of a trust, the reporting entity would be required to: • establish on reasonable grounds a description of each class of beneficiary; and • collect sufficient information for the reporting entity to be satisfied that it will be able to establish the identity of beneficiaries when there is a distribution from the trust or when a beneficiary intends to exercise vested rights. While this requirement is made under the initial CDD provisions of the Amendment Act, arguably Draft Rule 28 suggests that reporting entities must then actually take steps to obtain this information in the relevant circumstances. Whether or not that is the intention of the Draft Rule is not clear. If this is AUSTRAC's expectation it would mark a significant shift in the practices of undertaking ongoing CDD in connection with trustee customers.
Simplified CDD	The Draft Rules add very little prescription in connection with simplified customer due diligence (CDD that can be undertaken in certain low risk circumstances). However, the Draft Rules do provide that for a reporting entity to apply simplified CDD, the AML/CTF policies of the reporting entity must deal with the application of those measures. It is therefore necessary for any entity that wishes to apply simplified CDD measures, to have this approach documented as part of the ML/TF Risk Management Policies of the reporting entity.
Assessment of reliable and independent data	The Amendment Act requires that reporting entities verify KYC information, as is appropriate for the ML/TF risk, using reliable and independent data. Unlike the existing AML/CTF Rules, the Draft Rules do not prescribe matters that must be taken into account and documented in determining whether documentation or electronic data is reliable and independent. As part of moving to a principles-based approach, the Draft Rules also do not include safe harbours that are currently available under the AML/CTF Rules where no separate assessment of reliability and independence is required. Reporting entities that have focussed on using the documentation or electronic data safe harbours under the existing AML/CTF Rules, will need to consider: • their processes to ensure that these are designed in a manner that is appropriate to the ML/TF risk of the customer; and • documenting the process that was followed in order to reach this conclusion. This should form part of the ML/TF Risk Management Policies of the reporting entity.

Offshore operations

A quick recap on reforms affecting offshore operations

As described in our previous article, the Amendment Act does not affect the wide territorial reach of the AML/CTF Act. However, how the AML/CTF Act applies to services provided through permanent establishments in foreign countries was substantially re-written in the Amendment Act. These changes were made under the modernisation and simplification ambit of the reforms, as well as being responsive to FATF expectations.

What is proposed in the Draft Rules?

The Draft Rules continue the focus on the AML/CTF Act's interaction with foreign operations, seeking to reduce the burden of engaging with customers where the AML/CTF regimes of different jurisdictions may apply. In particular, the Draft Rules provide modifications to the CDD requirements where services are provided in connection with a foreign country.

Draft Rule 33 provides an exemption from initial CDD (effectively allowing delayed verification) while Draft Rule 37 deems compliance with initial CDD in certain circumstances:

- **Exemption from initial CDD (delayed verification):** The Draft Rules provide an exemption from the obligation to undertake initial CDD before providing a designated service where the service is to be provided by the reporting entity in a permanent establishment in a foreign country. This is subject to certain requirements being satisfied, including:
  - the laws of the foreign country must give effect to the FATF Recommendations and allow the identity of the customer as well as other matters set out in section 28(2) of the AML/CTF Act to be established after providing the service;
  - the reporting entity must take reasonable steps to establish that the customer is the person that they claim to be;
  - the reporting entity must identify the ML/TF risk of the customer based on KYC information reasonably available to them before commencing to provide the designated service; and
  - the reporting entity must collect KYC information about the customer that is appropriate to the ML/TF risk.
- **Deemed compliance with initial CDD:** The Draft Rules deem a reporting entity to have complied with the initial CDD requirements under section 28(2) of the AML/CTF Act where CDD has been undertaken in accordance with the laws of a foreign country. This is subject to certain requirements being satisfied, including:
  - the laws of the foreign country must give effect to the FATF Recommendations relating to customer due diligence and record-keeping;
  - those laws of the foreign country must have been complied with;
  - the customer must have been provided with a service by the reporting entity or by a member of the reporting group at or through a permanent establishment in a foreign country; and
  - the reporting entity must either hold the KYC information and verification data or otherwise have arrangements in place permitting immediate access to that information.

  The concept of deemed compliance within corporate groups is currently provided for to some extent under section 38 of the AML/CTF Act and associated Rule 7.3.5. The Draft Rules would rework these provisions into the CDD provisions of the AML/CTF Act and associated Rules.

Key considerations in implementing reforms connected to foreign standards

Implementation consideration	Insights
Processes when providing services outside of Australia	Reporting entities that are providing services from a permanent establishment outside of Australia have previously had to engage with the Australian AML/CTF Act only to a limited extent in connection with CDD. This is because the AML/CTF Act provides that the CDD provisions of the Act (set out in Part 2 of the Act) do not apply to designated services provided at or through a permanent establishment of an entity in a foreign country. While the CDD provisions introduced in the Amendment Act mean that many requirements will have general application, any entity that is providing designated services through a permanent establishment in a foreign country should revisit its approach to CDD, including how this is documented, and consider the application of the proposed exemption in the Draft Rules.
Process when providing services within Australia to a customer onboarded outside of Australia	Passporting of customers within an entity or intragroup has been the subject of varied approaches within organisations operating across jurisdictions. This includes leveraging existing the reliance provisions of the AML/CTF Act or applying global policies uplifted to the specifics of Australia's requirements. Any organisation that engages with customers on a cross border basis should revisit its approach and consider if the deemed compliance under the Draft Rules may be of assistance. As described below, the reliance provisions should also be reviewed to the extent that these are currently being applied.

Reforms to reliance arrangements

A quick recap on the use of reliance arrangements under the AML/CTF Act

Under the current AML/CTF Act there are two avenues for reliance on another reporting entity to carry out CDD:

- as part of an ongoing arrangement; or
- on a case by case basis.

Ongoing arrangements

Under section 37A of the current AML/CTF Act, a reporting entity can rely on the CDD of another reporting entity on an ongoing basis where:

- it has entered into a written agreement with the other reporting entity; and
- it has reasonable grounds to believe that each of the requirements prescribed under Part 7.2 of the current AML/CTF Rules is met (which includes periodic reviews of the agreement for compliance with the requirements).

Case by case arrangements

Section 38 of the AML/CTF Act permits a reporting entity to rely on the CDD carried out by another reporting entity on a case-by-case basis, without putting in place an ongoing CDD agreement with that party. Typically, this arrangement is used where the relying party is comfortable to rely on the other person's CDD (as the relying party is liable for any breaches of the CDD requirements), taking into account the ML/TF risks the relying party faces and the other matters set out in Part 7.3 of the current AML/CTF Rules.

What is proposed in the Draft Rules?

The majority of the requirements pertaining to both section 37A and sections 38 under the current AML/CTF Rules have been carried across into the Draft Rules 44 and 45, and have been simplified. Therefore, we do not expect that significant changes will need to be made to existing reliance arrangements.

The table below details a comparison of the key requirements of each of the reliance regimes under the Draft Rules (noting this is not an exhaustive list):

Key Requirement	Rule 44 (Ongoing reliance)	Rule 45 (Case by case reliance)
Written agreement	An agreement must document responsibilities of each party, including responsibilities for record keeping.	There must be a written record that documents the reasons for the relying entity concluding that the requirements for reliance are met.
Parties	The other party must be a reporting entity or person regulated by foreign laws that give effect to FATF Recommendations relating to CDD.	The other party must be a reporting entity or person regulated by foreign laws that give effect to FATF Recommendations relating to CDD.

Key Requirement	Rule 44 (Ongoing reliance)	Rule 45 (Case by case reliance)
Access to KYC information	The relying entity has obtained, from the other party, information about the identity of the customer.[2] The agreement must enable the relying entity to obtain all the KYC Information collected by the other person before it commences to provide a designated service or at a later time if section 29 applies.[3]	The relying entity has obtained, from the other party, information about the identity of the customer.[4] The relying party has reasonable grounds to believe that it can obtain all the KYC Information collected by the other person before it commences to provide a designated service or at a later time if section 29 applies.[5]
Access to verification information/data	The agreement must enable the relying entity to obtain copies of the data used by the other person to verify KYC information, immediately or as soon as practicable following a request from the relying entity.	The relying entity has reasonable grounds to believe that it can obtain copies of the data used by the other person to verify KYC information, immediately or as soon as practicable following a request from the relying entity.
Consideration of ML/TF risk	The arrangement must be appropriate to the risks of ML/TF that the relying entity may face in providing the designated services, taking into account a range of factors including nature of the other party's business, and the services, customers, delivery channel and jurisdiction risk of the other party.	Reliance on the other party's CDD must be appropriate to the risks of ML/TF that the relying entity may face in providing the designated services, taking into account a range of factors including nature of the other party's business, and the services, customers, delivery channel and jurisdiction risk of the other party.
Regular assessment of arrangement	The Draft Rules are silent on regular assessments of the agreement for reliance, despite the Amendment Act still having a requirement to do so under section 37B.	N/A.

Key considerations in implementing changes to reliance arrangements

Implementation consideration	Insights
Ongoing reliance: Regular assessments	Currently, there is a requirement for the relying entity to carry out regular assessments of the reliance arrangement to ensure the other party is continuing to meet the reliance requirements.[6] If the result of the assessment is that the other party is not in compliance, the reliance agreement must be suspended (and the relying party can no longer rely on the other party's CDD) until the reliance requirements are once again being met.[7]

2 This remains a requirement under section 37A(2)(d) of the AML/CTF Act

3 Section 29 of the Amendment Act permits delayed CDD in specific circumstances.

4 This remains a requirement under section 38(c) of the AML/CTF Act.

5 Section 29 of the Amendment Act permits delayed CDD in specific circumstances.

6 Section 37B of the AML/CTF Act and Rule 7.2.3-7.2.4 of the current AML/CTF Rules.

7 Section 37A(3) and (4) of the AML/CTF Act.

Implementation consideration	Insights
	It is not clear whether AUSTRAC intends to retain this assessment requirement. This is because the Amendment Act retains the requirement in section 37B to carry out the assessment in accordance with the AML/CTF Rules, but the Draft Rules appear to be silent on the requirements for such assessments and the frequency (whereas the current AML/CTF Rules cover this in Rule 7.2.3-7.2.4).
Ongoing reliance: Approval by Board or senior manager of relying entity	In the current AML/CTF Rules, the ongoing reliance arrangement under section 37A must be approved by the governing board or a member of senior management of the first entity.[8] This is now proposed to be addressed through Draft Rule 19 which would require the AML/CTF Policies of the reporting entity to ensure that the approval of a senior manager is obtained before entering into such an agreement. This approach of moving approval from the Board to a senior manager would maintain consistency with the reforms in the Amendment Act to the governance framework where the Board is no longer responsible for approval of the AML/CTF Program, and instead this is the responsibility of a nominated "senior manager" of the reporting entity.
Case-by-case reliance: Deemed compliance – reliance within a corporate group or designated business group (DBG)	The concept of deemed reliance within a group has been removed from the reliance provisions of the Rules. However, this does not mean that corporate groups are no longer able to leverage the CDD undertaken within the group where appropriate. Intragroup reliance – or deemed compliance in the context of compliance in a foreign country – is proposed to be dealt with under new Rule 37. We have described this in more detail in connection with offshore operations above. Rule 37 brings together concepts of reporting groups, offshore operations and CDD, all of which are being significantly rewritten as part of the Amendment Act and Draft Rules.

[8] Rule 7.2.2(d) of the current AML/CTF Rules.

Reporting groups and lead entities

A quick recap on reforms affecting business groups

The passage of the Amendment Act means that “designated business groups” are out, “reporting groups” are in. In introducing the concept of a reporting group, the Amendment Act contemplates business groups, reporting groups and a lead entity as part of that reporting group. Under the Amendment Act:

- in order for there to be a "lead entity" there must be a "reporting group";
- in order for there to be a "reporting group" there must be a "business group" where at least one member of the group provides a designated service; and
- in order for there to be a "business group", the requisite control, as defined, must exist.

Along with the new concepts, a new liability regime has been introduced for the lead entity of the reporting group.

The reforms appear to have a twofold purpose:

- address the unnecessarily cumbersome aspects of the designated business group framework. For example, removing the requirement that all members of a designated business group need to be reporting entities; and
- embed a concept of group compliance arrangements for the purpose of addressing FATF Recommendation 18.

What is proposed in the Draft Rules?

While the definition of “lead entity” is left to the Rules, the Draft Rules do not include fully completed concepts. The Consultation Paper is calling for submissions in connection with what is proposed. However, the Consultation Paper is clear that:

- The selection of the lead entity will not be left to the choice of the reporting group – it will be determined by the parameters set in the Rules.
- Every reporting group must have a lead entity. This means that wherever there is an entity providing a designated service in a business group, there will also be a lead entity regulated under the AML/CTF Act.
- The lead entity is the entity that controls all other members of the group that provide a designated service. This should be the entity with the “*most direct control of all other members of the group that provide a designated service*”.

Key considerations in implementing reporting groups and lead entities

Implementation consideration	Insights
Determining control	Draft Rule 8 provides that the lead entity is the entity that "controls" all other members of the group who provide designated services, provided that they are providing a designated service, resident in Australia or registered under the Corporations Act. • If there is more than one entity that meets the definition, the lead entity will be the entity with "the most direct control" of all other reporting entities. • If no person otherwise falls within the criteria set out in the Rule, what will happen has not yet been drafted. All reporting entities will need to review their corporate structure to determine which entity will fall within the definition of "lead entity".

Implementation consideration	Insights
Compliance framework of the lead entity	Once the lead entity has been identified, steps will need to be taken to ensure that a compliance framework that meets the requirements of the Amendment Act are implemented by the lead entity. This may be an entirely new compliance framework for some entities, including the introduction of direct liability under a regime that the entity may not have previously needed to engage with. We expect that reporting groups will need to consider the experience and understanding of the governing bBoards of any entity that will be a lead entity. These governing bBoards will need to understand ML/TF risk in their group and be comfortable with the compliance framework that they have in place to address these risks.
Updating existing designated business group compliance arrangements	Reporting entities that have adopted Joint AML/CTF Programs, or that otherwise leverage group arrangements as part of their AML/CTF compliance framework, should consider whether their controls reflect the requirements under the updated AML/CTF framework. Members of the reporting group that are not reporting entities, but have a role in fulfilling the obligations of reporting entities, must be subject to controls. These are new obligations that have not otherwise applied under the existing t AML/CTF Act. In particular, Draft Rule 68 provides that in order for another member of a reporting group that is not a reporting entity (**discharging member**) to discharge the obligations of reporting entities in the reporting group, the discharging member: • must have undertaken due diligence in connection with persons performing the relevant functions in a manner equivalent to the reporting entity's AML/CTF policies; and • must have provided training to those persons that is equivalent to the training required under the AML/CTF policies of the reporting entity.

Transfers of value and the travel rule

A quick recap on the regulation of transfers of value

The current framework relating to transfers of value is based on an outdated distinction between the transfers of value undertaken by financial institutions and those undertaken by remittance service providers. In addition, current regulations have not adequately kept pace with transferring value in non-fiat products, eg with digital assets.

Overview of the Amendment Act's impact on transfers of value

The Amendment Act simplifies the regulation of payments by:

- streamlining the services provided by financial institutions, remittance service providers and digital asset service providers into three designated services connected to the transfer of value (see new designated services in items 29, 30 and 31). These designated service are connected to whether the providing entity is an:
  - ordering institution
  - beneficiary institution; or
  - intermediary institution.

  After feedback on the AML/CTF Amendment Bill, including the review of the Senate Committee, the Amendment Act was passed largely leaving the definitions of ordering institution and beneficiary institution to be set out in the Rules;
- removing the definitions of 'electronic funds transfer instruction' and 'designated remittance arrangement' in sections 8, 9 and 10 of the AML/CTF Act; and
- replacing international funds transfer instruction (**IFTIs**) with a new concept of international value transfer services (**IVTS**). This links to the updated designated services in items 29 and 30. This means that the scope of reporting obligations on international transfers of value will be expanded from what currently applies under the IFTI regime to include remittance services and digital asset transfers.

Further detail on the Amendment Act (as proposed in the Amendment Bill) is set out in our client alert available here.

A quick recap on the travel rule

Under the current AML/CTF Act, only financial institutions are subject to the travel rule. However, Recommendations 15 and 16 of the FATF Standards require the travel rule to be applied to financial institutions, remittance providers and digital asset service providers. Under the Amendment Act, the streamlined value transfer services (discussed above) would trigger the travel rule for all three entities for both domestic and cross-border transfers.

The current regime also only requires information about the payer. However, Recommendations 15 and 16 require information about both the payer and payee. In addition, Recommendation 15 requires the payer information to be verified by the ordering institution.

Overview of the Amendment Act's impact on the travel rule

As detailed in our previous client alert (available here) travel rule obligations proposed for each institution in the value transfer chain are set out in the following table:

Role of entity	Designated service	Travel rule
Ordering institution	Item 29	Collect, verify (if required) and pass on the travel rule information to the next institution in the value transfer chain
Beneficiary institution	Item 30	Take reasonable steps to monitor whether it has received the travel rule information and whether the information received about the payee is accurate If it detects that it has not received all or part of the travel rule information, or that some or all of the information about the payee is inaccurate, either: • refuse to make the transferred value available to the payee; or • take such other action as it determines
Intermediary institution	Item 31	Take reasonable steps to monitor whether it has received the travel rule information If it detects that it has not received all or part of the travel rule information, either: • refuse to pass on the transfer message; or • take such other action as it determines If it passes on a transfer message, include the travel rule information *or* information obtained in accordance with its AML/CTF Program relevant to the transfer

As transfers of value are proposed to encompass remittances and virtual asset transfers, the travel rule obligations set out above are also triggered for those types of transfer.

What is proposed in the Draft Rules?

Definitions of ordering institution and beneficiary institution

As described above, the Amendment Act was passed with the definition of ordering institution and beneficiary institution largely left to be determined by the Rules. The Draft Rules therefore propose definitions of these concepts.

The definitions proposed in the Draft Rules of both beneficiary institution and ordering institution largely follow what was proposed in the Amendment Bill that was subject to first reading in Parliament. The intention of moving these to the Draft Rules, from the Act, is to allow for greater flexibility going forward to respond to changes in technology, as well as potentially respond to updated FATF expectations.

AUSTRAC proposes that it will issue Guidance that will contain extensive example scenarios setting out different types of 'value transfer chains' and identifying the ordering institution, intermediary institutions and beneficiary institutions in each of them.

Obligations of each entity in collecting, verifying and passing on information

The Draft Rules propose obligations of ordering institutions, beneficiary institutions and intermediary institutions in fulfilling their obligations under the Amendment Act to collect, verify, pass on and monitor information. We expect that these proposals will be of particular interest to entities involved in transfers of value looking to understand their operational requirements going forward.

When value is "in" a country

The IVTS obligations under the Amendment Act are contingent on there being value transfers in Australia to a foreign country and vice versa. The Draft Rules propose guidance on determining when value is "in" a country.

Exemptions

The Draft Rules propose exemptions from the scope of a "transfer of value". This is to accommodate certain inter-financial institution transfers connected to SWIFT, cheque transfers, card-based pull payments and transfers to a self-hosted virtual asset wallet.

What is not included in the Draft Rules

The Draft Rules leave "*to be drafted*" Rules in connection with international value transfer reports. We expect this to be an area of keen interest given the significant scope of IVTS obligations and the systems and administration requirements in implementing reporting requirements.

Key considerations in navigating the transfer of value reforms

Implementation consideration	Insights
Definitions	Entities should review the revised definitions, particularly of 'ordering institution' and 'beneficiary institution' carefully against their business operations. AUSTRAC wants entities to highlight where the definitions do not provide sufficient clarity in their application to different business operations.
Intermediary Institutions	Entities who are interposed in a value transfer should consider whether the current rules provide sufficient clarity on when they are within scope of the regime or exempted and whether the requirements are sufficiently clear.
IFTIs (international value transfer reports)	Although AUSTRAC has stated that it will consult on the rules relating to IVATs separately, entities should provide any feedback on (the many) issues with the current IFTI reporting regime so that AUSTRAC can take those into account.
Travel Rule information	Entities should consider the new requirements relating to travel rule information against their business models/operations to ensure that the obligations are clear and when operationalised do not create uncertainties in their application.

Keep open notices

A quick recap on 'Keep Open' notices

“Keep Open” notices are the mechanism by which notices reporting entities are requested to continue with the supply of designated services to certain customers who are the subject of an ongoing law enforcement investigation (**Keep Open Notice**)

As we outlined in our article o of 25 September 2024, the Amendment Bill proposes to revise the current regime by which Keep Open Notices are issued by empowering agencies to issue those notices themselves, without AUSTRAC’s active involvement. These notices will be able to be issued by “senior members” of specified agencies (copied to AUSTRAC) for investigations into “serious offences” and for a period of up to a total of 18 months (but this can be longer if AUSTRAC so authorises). Although these notices do not *require* a reporting entity to continue supplying the designated service(s), they provide limited exemptions to the reporting entity from particular other AML/CTF obligations if those services are continued.

What is proposed in the Draft Rules?

The Draft Rules outline the form of the Keep Open Notice, the extension request, and the application to AUSTRAC by an agency to extend such a notice beyond the 18 month period. It also sets out the information and documents that agencies must provide to reporting entities with a Keep Open Notice. The extent of that information and accompanying documents is limited to details of the agency and “senior member” of that agency authorising the notice, the length of the notice, and details of the relevant customer(s) sufficient to enable the reporting entity to identify to whom the notice applies.

Key considerations in implementing reforms to keep open notices

Implementation consideration	Insights
Narrow scope of the exemptions and overlap with the revised ‘tipping off’ regime	The Draft Rules do not provide any further guidance to reporting entities on how they may avail themselves of the exemption under the (soon to be) section 39A(2) of the AML/CTF Act. That exemption provides that sections 28, 30 or 26G do not apply to the extent that the reporting entity “*reasonably believes that compliance with that section would or could reasonably be expected to alert the customer to the existence of a criminal investigation*” in circumstances where a Keep Open Notice has been received by the reporting entity and remains in force. The forms and scope of information outlined in the Draft Rules highlight that agencies are not required to provide any details to the reporting entity about the nature of their investigation other than the fact that it meets the definition of “serious offence” under the AML/CTF Act. Moreover, there is no guidance in the Draft Rules on whether, and if so the extent to which, a reporting entity may be able to rely on its assessment of whether the disclosure of certain information under the revised section 123 is affected by receipt of these notices, or their revocation or expiry. Revised section 123 will enable disclosure of otherwise restricted information where it cannot be said to “reasonably be expected to prejudice an investigation” into certain offences or proceeds of crime recovery operations.

Implementation consideration	Insights
Indication of the nature and extent of AUSTRAC oversight	Reporting entities may also have concerns that the removal of AUSTRAC as a gatekeeper of Keep Open Notices may result in an avalanche of requests that may not have been issued if AUSTRAC remained the sole issuer. The Draft Rules also provide no indication of the criteria by which AUSTRAC may assess whether to revoke a Keep Open Notice issued by an agency or refuse to extend one beyond the 18 month period. As such, the opacity of this process may frustrate reporting entities who, understandably, may wish for greater visibility on the extent of ML/TF risk posed to them by their customers.

Next steps

There are a number of areas in the Draft Rules that are left "*to be drafted*" and in respect of which the Consultation Paper is asking for comment on.

We expect that the time frame between the closure of submissions, due by **14 February 2024**, and the next round of industry engagement will be quick. We recommend that reporting entities, or entities that will become reporting entities, take steps now to map their compliance arrangements and consider where uplift or significant change is required to existing processes and controls.

Key contacts

Alice Molan
Partner
M +61 3 9288 1700
alice.molan@hsf.com

Charlotte Henry
Partner
M +61 2 9225 5733
charlotte.henry@hsf.com

Bryony Adams
Partner
M +61 2 9225 5288
bryony.adams@hsf.com

Kate Cahill
Partner
M +61 2 9322 4413
kate.s.cahill@hsf.com

Julia Massarin
Executive Counsel
M +61 3 9288 1117
julia.massarin@hsf.com

Daniel Hyde
Senior Associate
M +61 2 9225 5480
daniel.hyde@hsf.com

David Curley
Senior Associate
M +61 2 9225 5136
david.curley@hsf.com

Ayman Shash
Solicitor
M +61 3 9288 1741
ayman.shash@hsf.com