MODERNISING AUSTRALIA'S AML/CTF REGIME

AMENDMENT BILL INTRODUCED INTO PARLIAMENT

Contents

Legislative reforms to modernise and expand Australia's AML/CTF regime go straight to Parliament 1

AML/CTF Programs – risk assessments and policies 2

Reforms to governance requirements 4

New approach to regulating offshore operations 6

Reforming Customer Due Diligence requirements 8

Virtual asset service providers – new terminology and scope 11

Transfers of value – new concept with broad application 14

Transfers of value – expansion of travel rule 16

International value transfer services – the new IFTIs 19

Rewrite of tipping off offence 23

Assisting an investigation of a serious offence 25

New AUSTRAC investigation and enforcement powers 26

Legislative reforms to modernise and expand Australia’s AML/CTF regime go straight to Parliament

On 11 September 2024, amendments to the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**AML/CTF Act**) were introduced into Parliament through the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2024* (Cth) (**AML/CTF Bill**). The Bill includes significant proposals to expand the application of the AML/CTF Act to additional sectors of the Australian economy, including lawyers, real estate agents, accountants and others.

The AML/CTF Bill also proposes significant reforms to the AML/CTF Act for those reporting entities that are already subject to its requirements. The reforms are wide reaching and have the potential to make the regime easier to navigate and implement. However, there are also new issues to address from an operationalisation perspective – the AML/CTF Bill includes updates that will mean that reporting entities need to adjust their systems and processes that have been embedded after close to two decades of compliance.

There are also changes that would result in a marked expansion in the investigation and enforcement powers that AUSTRAC has available to it and may signal a new approach from the regulator.

We have been closely following the Consultations that have led to the Bill and you can read our previous articles here , here and here. While there have been two Consultations on these reforms, no exposure draft legislation was released before the Bill entered Parliament. There is therefore a significant amount of detail to carefully review as it is expected that the reforms will be passed relatively swiftly.

In this article we have focussed on the impact that the AML/CTF Bill will have on existing reporting entities. This article does not seek to examine every aspect of the proposed reforms. There is also a significant amount of detail that will become clearer once proposed changes to the AML/CTF Rules are made public. We expect that a consultation on the Rules will occur before the end of this year.

AML/CTF Programs – risk assessments and policies

What is currently required and what did the Consultation propose?

Under Part 7 of the AML/CTF Act, reporting entities are required to maintain an AML/CTF Program meeting the requirements prescribed by the AML/CTF Rules. An AML/CTF Program must be made up of Part A and Part B:

- The primary purpose of Part A is to identify, manage and mitigate ML/TF risk that a reporting entity may reasonably face in relation to the provision of designated services at or through a permanent establishment in Australia.
- Part B must set out the reporting entity's applicable customer identification procedures (**ACIP**).

While an obligation to implement a risk-based approach has been successfully pursued by AUSTRAC in enforcement actions, the Consultation Papers acknowledged that the obligation to assess risk is not expressly contemplated in Australia's AML/CTF framework.

What does the Bill propose?

AUSTRAC has successfully pursued action against reporting entities on the basis that, without an appropriate risk assessment, a reporting entity does not have an AML/CTF Program for the purpose of the AML/CTF Act. Under the reforms, this concept would be embedded into the Act.

A new definition of AML/CTF Program would be introduced which comprises:

(a) the reporting entity's money laundering, terrorism financing and proliferation financing (**ML/TF**) risk assessment (**ML/TF Risk Assessment**); and

(b) the reporting entity's anti-money laundering and counter-terrorism financing (**AML/CTF**) policies, procedures, systems and controls (**AML/CTF Policies**).

Broad scope of AML/CTF Policies definition

The AML/CTF Act's definition of AML/CTF Program contemplates a written program that is divided into Part A and Part B. The AML/CTF Program is generally thought of as a document that sits in one file, has the headings and content prescribed by the AML/CTF Rules and is approved by a reporting entity's Board.

AUSTRAC's more recent enforcement action has highlighted that AUSTRAC's view of AML/CTF Programs is that these must be more granular, with responsibility for risk and risk management set out in the Program and supported by policies, processes, systems and controls.[1] This language has been reflected in the AML/CTF Bill's definition of AML/CTF Policies.

Civil penalties associated with the ML/TF Risk Assessment and AML/CTF Policies

The proposed updates will have the effect that a reporting entity will breach a civil penalty provision each time a designated service is provided:

- without an ML/TF Risk Assessment that is kept up to date in accordance with the Act; and/or
- without the required AML/CTF Policies in place.

The reforms also maintain the obligation on reporting entities to comply with their AML/CTF Policies. The obligation to comply with the entity's AML/CTF Policies is a civil penalty provision.

This means that the potentially incalculable fines that can accumulate in getting the risk assessment or the policies wrong, will continue with these reforms and, as described below, will go further than under the current Act.

[1] See for example Particulars included in paragraphs 215, 218 and 282 of AUSTRAC's filing in *AUSTRAC v The Star Ltd*.

Key considerations in implementing changes to the AML/CTF Program – risk assessments and policies

<table>
<tr><th>Implementation consideration</th><th>Insights</th></tr>
<tr><td>Meeting the prescribed ML/TF risk assessment</td><td>While a money laundering and terrorism financing risk assessment is clearly the expectation under the current AML/CTF Act, the Bill will introduce prescribed requirements in connection with the ML/TF Risk Assessment.

This includes:
subject to certain exceptions, incorporating an assessment of proliferation financing risk into that assessment – this would involve considering the risk that designated services are being used to facilitate the proliferation of weapons of mass destruction; and
ensuring that a review of ML/TF risk is undertaken in accordance with the Act. This would require event driven changes as well as a periodic review at least every 3 years.
Reporting entities will need to review their current ML/TF risk assessment framework to ensure that this is established in a manner that is consistent with the prescribed requirements to be introduced.</td></tr>
<tr><td>Non-compliance with AML/CTF Policies</td><td>Under the current AML/CTF Act, non-compliance with Part A of an AML/CTF Program is a civil penalty provision. Under the proposed reforms, failure to comply with the AML/CTF Policies of the reporting entity is a civil penalty provision. The amendments:
do not distinguish between customer due diligence procedures (as the distinction between Part A and Part B is removed); and
do not differentiate between content of policies and procedures that are included for compliance with the legislation and those that are not.
On the face of the Bill, this means that non-compliance with anything that is put into a reporting entity's AML/CTF Policies, which is itself defined broadly, would be a breach of a civil penalty provision.</td></tr>
</table>

Reforms to governance requirements

What is currently required and what did the Consultation propose?

The AML/CTF Rules currently require that Part A of a reporting entity's AML/CTF Program is approved by the reporting entity's board and senior management. There is otherwise very little prescription around the oversight that must be exercised.

In addition, the AML/CTF Rules require that reporting entities must designate an AML/CTF Compliance Officer at management level but, again, there is little other prescription in connection with the role.

Consistent with the focus of AUSTRAC's enforcement action, the Consultations included emphasis on ensuring a culture of compliance within reporting entities. The Consultations proposed that the Board or equivalent senior management would be required to maintain oversight of the AML/CTF Program with recognition that the change in structure of AML/CTF Programs would affect the governance of that document.

What does the Bill propose?

Board responsibility

The Bill proposes new provisions specifically detailing the responsibilities of governing bodies in connection with AML/CTF compliance. In particular, the board would be required to:

- exercise appropriate ongoing oversight of the ML/TF Risk Assessment and the compliance with the AML/CTF Policies and relevant laws; and
- take reasonable steps to ensure that the reporting entity is appropriately identifying relevant ML/TF risks and complying with the AML/CTF Policies and relevant laws.

New concept of "senior manager"

Rather than requiring the AML/CTF Program to be approved by the board of a reporting entity, the reforms would require the ML/TF Risk Assessment and AML/CTF Policies, including any updates to these, to be approved by a "senior manager" of the reporting entity.

"Senior manager" would be defined as an individual who:

> *"makes or participates in making, decisions that affect the whole, or a substantial part, of the business of the reporting entity".*

Updates to the ML/TF Risk Assessment must be notified in writing to the governing body as soon as practicable following the update.

Additional prescription for AML Compliance Officers

The role of the AML/CTF Compliance Officer will be subject to more specific obligations in respect of their competency and their responsibility. The AML/CTF Compliance Officer must meet prescribed requirements in connection with their authority and position in the business and they must be located in Australia if the reporting entity is providing the services through a permanent establishment in Australia. We have described some of the changes proposed by the Amendment Bill in connection with offshore operations in the section below.

Introduction of “lead entity” – new obligations for entities not providing designated services

A new concept of “lead entity” is proposed to be added to the Act. The definition of “lead entity” will be defined in the AML/CTF Rules so the exact scope and impact of this new concept is currently unclear.

Under the proposed updates a “lead entity” will be treated as a reporting entity, whether or not they provide designated services. This means that the lead entity will breach the AML/CTF Act if the reporting entities in the group provide designated services without the required ML/TF Risk Assessment or AML/CTF Program being in place.

The draft Explanatory Memorandum states that:

> *“Lead entities’ governing bodies will be required to exercise appropriate ongoing oversight across the reporting group and take reasonable steps to ensure that reporting entities in the reporting group are appropriately identifying, assessing, managing and mitigating their ML/TF risks and otherwise complying with AML/CTF obligations”.*

Key considerations in implementing changes to governance arrangements

Implementation consideration	Insights
Location of AML/CTF Compliance Officer	Currently a reporting entity that operates on a cross jurisdictional basis may leverage international expertise within its business, including the appointment of an AML/CTF Compliance Officer located outside of Australia. Under the reforms this would not be acceptable where the reporting entity is providing the designated services through a permanent establishment in Australia – the AML/CTF Compliance Officer would need to be resident in Australia.
Senior manager of the reporting entity	Where a reporting entity appoints a senior manager with authority to approve the ML/TF Risk Assessment and AML/CTF Policies (and any updates to these), the reporting entity should consider its obligations under the Financial Accountability Regime including how this responsibility sits within the responsibilities of accountable persons.
Impact on lead entities	The expansion of statutory obligations under the AML/CTF Act to entities within a corporate group that are not providing any designated service is a significant change to the liability framework under the Act. Any reporting entity that is operating within a group that includes entities that do not provide designated services should keep this reform under close review, in particular the definition of “lead entity” to be introduced under the Rules. This may have significant ramifications for the liability and obligations of the governing boards of those entities.

New approach to regulating offshore operations

What is currently required and what did the Consultation propose?

The AML/CTF Act has wide territorial reach. It applies to:

a) services provided at or through a permanent establishment of a person in Australia; (Onshore Activities)

b) activities undertaken by Australian residents at or through permanent establishments in foreign countries (Resident Offshore Activities); and

c) subsidiaries of Australian resident companies providing services at or through permanent establishments in foreign countries (Subsidiary Offshore Activities).

While the application of the Act is clearly broad, the impact on Resident Offshore Activities and Subsidiary Offshore Activities (together termed in this paper (Offshore Activities) is less clear. The Consultations contemplated reform of the application of the Act to Offshore Activities.

What does the Bill propose?

The broad jurisdictional reach of the AML/CTF Act would be maintained under the Bill. However, amendments are proposed to be made in connection with the application of ongoing obligations to Offshore Activities. We have highlighted some key differences between the application of obligations to reporting entities undertaking Onshore Activities compared to those undertaking Offshore Activities.

Designated service provided through Offshore Activities	Additional requirements if designated service through Onshore Activities
Must undertake the ML/TF Risk Assessment and keep it updated	Must undertake the ML/TF Risk Assessment having regard to matters prescribed by the AML/CTF Act.
Must develop and maintain AML/CTF Policies	Must develop and maintain AML/CTF Policies which deal with matters prescribed by the AML/CTF Act.
Must not provide a designated service to a customer without first establishing certain CDD information about the customer.	In undertaking the prescribed CDD, must have regard to additional considerations including the entity's ML/TF Risk Assessment.

Key considerations in implementing changes to application to Offshore Activities

Implementation consideration	Insights
Customer due diligence requirements and approach to AML/CTF Act compliance more generally	The AML/CTF Act currently provides that Part 2 (in connection with CDD) does not apply to reporting entities providing designated services through Offshore Activities. The reforms in the Bill make it clear that CDD requirements will apply to any reporting entity, although with some more prescriptive requirements for reporting entities providing services in Australia ie through Onshore Activities. Any reporting entity that is operating outside of Australia will need to consider how it has approached compliance to Australia's AML/CTF Act as the compliance framework will be materially rewritten.
Record keeping in English	Reporting entities that are providing services through Offshore Activities will have obligations under the AML/CTF Act, although they will be less prescriptive. This includes having an AML/CTF Program although with less prescriptive requirements. The Bill proposes that all reporting entities must maintain records of compliance with its obligations in connection with the AML/CTF Program provisions and that these must be in English or in a form that is readily accessible and readily convertible into writing in English. Given that the entity may be operating outside of Australian and in another language, this may require the entity to consider its documentary approach to complying with the Australian AML/CTF Act record keeping requirements.

Reforming Customer Due Diligence requirements

What is currently required and what did the Consultation propose?

The existing AML/CTF regime requires all reporting entities to include ACIP within Part B of their AML/CTF Program. ACIP must meet the prescriptive requirements for different customer types (individuals, companies, trusts etc.) set out in Chapter 4 of the AML/CTF Rules. As well as Part B of the Program meeting these specified requirements, Part A must include enhanced CDD procedures and a transaction monitoring program.

While the legislative requirements are prescriptive in nature, the separation of these requirements between Part A and Part B means they can be difficult for entities to navigate.

The response of the financial services industry to Consultation Paper 1 was overwhelmingly supportive of updates to the CDD framework and a move away from the prescriptive requirements in Chapter 4 of the AML/CTF Rules.

Consultation Paper 2 proposed a significant re-write of the CDD framework and reframing of the provisions. Importantly, it included a proposal to introduce an obligation on reporting entities to individually risk rate each customer prior to providing a designated service. Entities would implement a risk rating scale against which customers would be assessed as high, medium, or low risk. The rating would then dictate the initial CDD a customer would be subject to (simplified, standard, or enhanced).

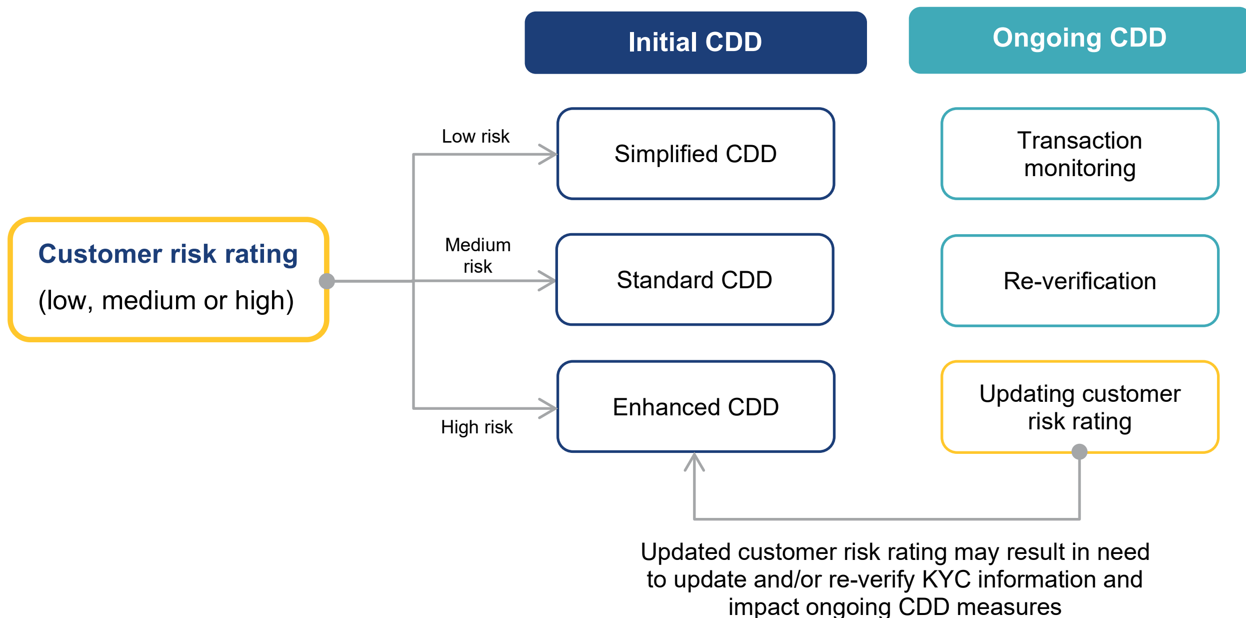
What does the Bill propose?

Replacement of 'Applicable Customer Identification Procedure'

The widely criticised current definition of 'applicable customer identification procedure' has been struck out in the new Bill. Instead, a new and more streamlined section on 'undertaking initial customer due diligence' requires entities to establish certain matters, including the 'identity' of individual customers, 'beneficial owners' of customers that are not individuals, whether any such persons are PEPs or targeted for financial sanctions and any other matters specified in the AML/CTF Rules. The granularity of these 'other matters' is unclear pending release of the draft AML/CTF Rules.

Conducting a Customer Risk Assessment

As contemplated in Consultation Paper 2, the Bill introduces an obligation to undertake a customer risk rating which will have flow on consequences for the CDD to be applied.



Importantly, and as anticipated, the new provisions require that as part of initial due diligence, an entity '*identify the ML/TF risk of the customer*'. This is defined as the:

> *'risks of money laundering, financing of terrorism and proliferation financing that a reporting entity may reasonably face in providing its designated service, or designated services, to the customer.'*

When assessing a customer's risk rating, the entity will be required to consider:

- the KYC information collected;
- the entity's own ML/TF Risk Assessment;
- the kind of customer to whom the designated service is provided;
- the kinds of service being provided;
- the delivery channels that the reporting entity is or will be providing eth services to the customer through; and
- the countries with which the reporting entity details, or will deal, in providing designated services to the customer.

The Bill provides for simplified due diligence measures to be applied to low risk customers. However, the detail of these measures has been left to the Rules and so it remains to be seen what these will entail and how prescriptive they will be.

Similarly, the Bill provides for enhanced due diligence measures for customers who are considered high risk or who meet other specified criteria, including those who are PEPs, existing customers for whom suspicious matter reporting obligations have previously arisen (but to whom the entity proposes to continue to provide a service) or a customer present in a jurisdiction for which FATF has called or enhanced due diligence to be applied. As anticipated from Consultation Paper 2, these enhanced measures are required to be '*appropriate to the ML/TF risk of the customer*.' It is unclear whether any further prescriptive requirements or guidance on what may be 'appropriate' will be issued.

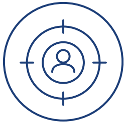
Providing a Designated Service before CDD

The Bill also puts forward modified provisions that would apply where an entity proposes to commence provision of a designated service before conducting initial due diligence. Whilst prescription of some circumstances have again been left to the Rules, the Bill requires that such services only be provided prior to CDD where it is '*essential to avoid interrupting the ordinary course of business*'.

Key considerations in implementing changes to Customer Due Diligence

With detail on several key areas being left to the AML/CTF Rules, it remains to be seen whether the new regime will continue to follow the existing, more prescriptive approach to customer identification.

Implementation consideration	Insights
How will the requirement to undertake customer risk ratings prior to the provision of designated services be operationalised?	Entities will need to establish a customer risk rating for each customer before providing them with a designated service. The definition of 'ML/TF risk of the customer' in the Bill is broad - the '*risks of money laundering, financing of terrorism and proliferation financing that a reporting entity may reasonably face in providing its designated service, or designated services, to the customer*.' Entities are expected to collect and use KYC information to establish this risk, as well as considering 'the kind of customer' to whom the designated services will be provided and the 'kinds of designated services' that will be provided. Entities will need to conduct careful review of their customers, services, channels, and operating locations, as well as any other factors the new AML/CTF Rules may provide for, to help develop their sliding scale of customer risk and categorise customers as high, medium, or low risk.
How will a business draw clear lines on what is or is not '*essential to avoid interrupting the ordinary course of business*'?	Where an entity provides designated services before conducting initial due diligence, it will be required to demonstrate that, among other things, doing so was '*essential to avoid interrupting the ordinary course of business*'. This language is consistent with the terminology currently contained in Rule 79 in connection with account opening. Entities will need to implement clear boundaries in relying on this provision to ensure any provision of designated services before conduct of due diligence does not occur habitually.



Virtual asset service providers – new terminology and scope

What is currently required and what did the Consultation propose?

The AML/CTF Act currently includes digital currency exchanges within the remit of the AML regime. These are entities which exchange fiat for digital currency or vice versa, but not those that only exchange one type of digital currency for another type (that is not fiat).

The definition of 'digital currency' is broad capturing most types of cryptocurrency but not all types of digital assets. In particular, digital currency must be '*generally available to members of the public without any restriction on its use as consideration*'.

The AML/CTF Act prescribes that the act of exchanging fiat to digital currency or vice versa is a designated service bringing digital currency exchanges within scope of the AML regime.

For some time, FATF has required countries to regulate a broader set of digital asset providers and to regulate them in additional ways.

Consultation Paper 2 proposed to bring Australia's AML regime in line with FATF requirements and, indeed, made proposals that went beyond those set out by FATF.

What does the Bill propose?

The Bill largely adopts the position as consulted on in Consultation Paper 2.

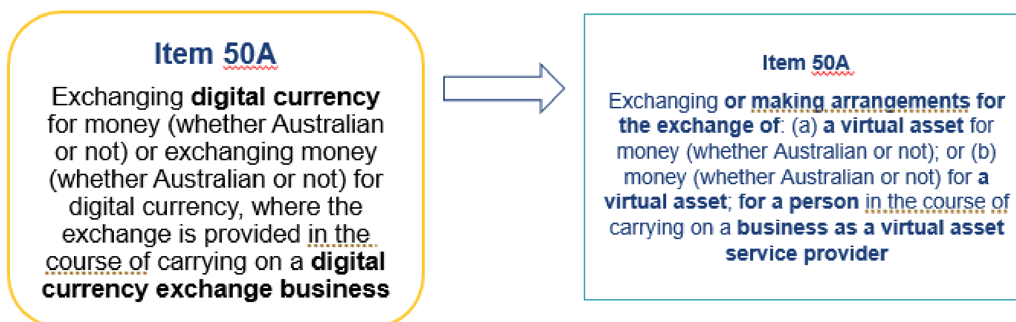
New definition of 'virtual asset'

In a change from Consultation Paper 2, the Bill proposes to adopt the language used by FATF so 'digital currency' will be replaced with 'virtual asset'. This will make Australia consistent with other international regimes.

The definition of 'virtual asset' proposed in the Bill is broader than the current definition of digital currency and, importantly, no longer requires that the virtual asset is generally available to members of the public. This means that a wider range of digital representations of value will be captured. However, some new exclusions have been proposed.

Change to current designated service

The current designated service in item 50A will be replaced with:



Of particular importance is the inclusion of 'making arrangements' which goes beyond what FATF requires. This concept was included in Consultation Paper 2 and submissions asked for clarity on what this means, which the Bill does not do. The concept of "making arrangements" or arranging is a known concept for the purposes of the AFSL regime under the Corporations Act, and the designated service of item 54 includes 'making arrangements' but in the capacity of being an AFSL holder meaning it is linked to how that term is used in the Corporations Acts. This will need further clarity.

In addition, the existing designated services relating to money transfers (items 29 and 30) (which will now relate to transfers of value) are extended to also include a transfer of virtual assets.

New designated services

In addition to the amended item 50A, a number of other new designated services are proposed for virtual asset service providers.

Item 46A

Providing a virtual asset safekeeping service, where the service is provided in the course of carrying on a business as a virtual asset service provider.

Item 50B

Exchanging or making arrangements for the exchange of a virtual asset for another virtual asset (whether or not of the same or a different kind) in the course of carrying on a business as a virtual asset service provider

Item 50C

Providing a designated service mentioned in another item of this table in connection with the offer or sale of a virtual asset, where the service is provided in the course of carrying on a business participating in the offer or sale.

Consultation Paper 2 proposed that there would be some key exclusions to the new designated services above including:

- From item 46A – businesses providing ancillary infrastructure (e.g. cloud data storage providers); and
- From item 50C – banks processing payments by customers to purchase virtual assets.

We will wait to see if these exclusions are included in the rewritten AML/CTF Rules.

Registration requirements

Each of designated service items 46A, 50A, 50B or 50C (shown above) and items 29 and 30 (where there are transfers of virtual assets) will trigger the need for the entity to be registered and included on the virtual asset service provider register.

New requirements

As money remittance and bank electronic funds transfers are proposed to be replaced by the concept of a transfer of value, virtual assets are included in this broader concept of value. Therefore, virtual asset service providers will be included in a number of other aspects that relate to the transfer of value including the travel rule requirements and the replacement IFTI reporting regime. In addition, where the transfer is to or from an unverified self-hosted virtual asset wallet, the entity must report this to AUSTRAC.

Key considerations in connection with virtual assets

Implementation consideration	Highlight
Registration	The widened definition of 'virtual asset' will now mean that a much larger set of entities could be subject to the AML regime triggering registration.
Application of AML/CTF Program	With the increased number of designated services, more activities conducted by virtual asset service providers will need to be subject to the entity's AML/CTF Program.
Reporting	Virtual asset service providers will need to prepare to be able to: • provide the replacement IFTI reports; • provide the reporting needed if there are virtual asset transfers to an unverified self-hosted wallet; and • provide the information needed to comply with travel rule requirements.

Transfers of value – new concept with broad application

What is currently required and what did the Consultation propose?

The current framework for the regulation of transfers of value across borders distinguishes between:

- electronic funds transfer instructions (or **EFTIs**) (designated services 29 and 30), which are undertaken by financial institutions; and
- remittances by remittance services providers (designated services 31 and 32) which, in the right circumstances, require the providers of registrable designated remittance services to be registered with AUSTRAC, reflecting the heighted ML/TF vulnerability associated with remittance services.

The Consultations proposed removing the definitions of 'EFTI' and 'designated remittance arrangement' in sections 8, 9 and 10 of the AML/CTF Act in favour of the streamlined concept of 'value transfer service' which would apply to remittance providers, digital asset service providers and financial institutions.

There were two important qualifications proposed by the reforms. First, the updated concept of a 'value transfer chain', comprising the ordering institution, intermediary institution and beneficiary institution, would not apply to non-financial institutions such as car fleet service providers where value is passed on behalf of a customer incidentally to another service. Secondly, in framing the definition of 'intermediary institutions', in respect of which the Consultations proposed to introduce a limited designated service related to their role in passing on messages in a value transfer chain, businesses would be excluded if their role is solely to provide the messaging infrastructure through which transfer messages are transmitted.

What does the Bill propose?

New 'transfers of value' to replace EFTIs and remittances

As foreshadowed by the Consultations, the Bill repeals the four designated services in table 1, section 6 of the AML/CTF Act relating to EFTIs and designated remittance arrangements and replaces them with three new designated services that relate to the 'transfer of value' in the 'value transfer chain'. New item 29 in table 1 relates to an ordering institution accepting an instruction for the transfer of value on behalf of a payer, and new item 30 relates to a beneficiary institution making the transferred value available to a payee.

The Bill also proposes the introduction of a new limited designated service for intermediate institutions as item 31 in table 1. While intermediary institutions would be required to undertake ML/TF risk assessments and develop, maintain and comply with AML/CTF policies to mitigate those risks, their CDD obligations are proposed to be comparatively limited, reflecting the reality that they are not in a direct relationship with the customer in a value transfer chain.

The Bill defines the 'transfer of value' as the transfer of money, virtual assets or other property but excludes transfers of physical currency or other tangible property. This definition reflects FATF Recommendation 16 and the inclusion of virtual assets in particular reflects the increasing use of digital or virtual assets in payments. The Bill also proposes a rule-making power so that AUSTRAC can extend the scope of the definition as unanticipated scenarios arise.

Priority mechanism for designating institutions in the 'value transfer chain'

The institutions that facilitate the 'transfer of value' are defined as constituting the 'value transfer chain', i.e., the ordering institution, intermediary institution and beneficiary institution. Here, the Bill departs from the Consultations in proposing a mechanism for determining which institution in the value transfer chain is the ordering institution or the beneficiary institution. That mechanism involves a set of criteria in descending order of priority, where the 'first person to satisfy' the higher-ranking criterion is designated as the relevant institution.

The Explanatory Memorandum notes that this mechanism is designed to "*reflect the reality that transfers of value are done by different businesses in different ways*". For example, recognising that some payment businesses do not hold the funds they transfer on behalf of customers, but rather hold authorisation to draw from a linked bank account, criterion (b) in proposed section 63A(2) provides for such businesses to be

designated as the ordering institution: "*the person is authorised under an arrangement with the payer to transfer the value from another source*".

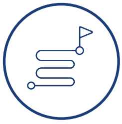
Exclusions from definitions

As foreshadowed by the Consultations, the Bill proposes to exclude from the definition of intermediary institution:

- A non-financial institution that transfers value incidentally as part of the provision of another service from the definitions of the institutions comprising the value transfer chain; and
- An entity that solely provides the infrastructure that permits a person to send transfer messages for a transfer of value to another person in the value transfer chain.

Key considerations in connection with transfers of value

Issue	Insights
The scope of the limited designated service for intermediary institutions	Intermediary institutions whose role is limited to passing on messages in a funds transfer chain may not be enrolled with AUSTRAC as this is not a designated service. The introduction of a new limited designated service for intermediary institutions would impose new regulatory burdens on those institutions and, while exemptions from CDD obligations are proposed, entities will need to carefully consider how to ensure their compliance with AML/CTF requirements.
Complexity in the priority mechanism	As indicated in the Explanatory Memorandum, transfers of value occur in many different ways and can often involve multiple parties. We expect that there may be challenges for institutions to identify their role in complex transfers of value, particularly where there are multiple institutions providing services which require the priority of those services to be assessed.



Transfers of value – expansion of travel rule

What is currently required and what did the Consultation propose?

Part 5 of the AML/CTF Act contains obligations to pass on information about the origin of the funds to be transferred that are generally referred to as the 'travel rule'. Currently, those obligations are limited to financial institutions and only require information about the payer to be passed on with transfer instructions.

The reforms proposed in the Consultations focussed on bringing the AML/CTF regime into line with FATF Standards by increasing the end-to-end transparency of transactions.

Subject to some practical exceptions, they proposed to expand the scope of the travel rule obligations in two key ways. First, as the new concept of 'value transfer services' would apply to remittance service providers, digital asset service providers and financial institutions alike, the travel rule would also be triggered for remittances and digital asset transfers and so apply to the providers of those services, for both domestic and cross-border transfers. Secondly, they proposed to require information about the payee to be included in value transfer instructions while currently that requirement is limited to information about the origin of the transferred funds.

Consultation Paper 2 suggested that the full travel rule information would not be required for certain domestic value transfers where the ordering institution would be able to provide full information upon request and incoming cross-border value transfers where the inclusion of all required information is currently precluded by technical limitation in existing payment systems (including the Bulk Electronic Clearing System).

What does the Bill propose?

While the Bill proposes to expand the travel rule obligations for each institution in the 'value transfer chain', it diverges from the Consultations in leaving a significant degree of the detail to the AML/CTF Rules.

In particular, although the Consultations had proposed to extend the travel rule obligation to the inclusion of payee information in transfers of value (currently required by FATF Recommendation 16), that reform has not carried over into the Bill. As FATF Recommendation 16 is currently under review by FATF, the Bill instead confers a rule-making power on the AUSTRAC CEO to establish what information should accompany value transfers once FATF has concluded its review.

The Bill repeals the existing concepts of 'required transfer information', 'complete payer information' and 'tracing information', and instead refers in each proposed section to "*the information specified in the AML/CTF Rules*".

Travel rule obligations by institution

Specific 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	Must collect, verify and pass on prescribed information
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:

Role of entity	Designated service	Travel rule
		• 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.

Modified obligations for virtual asset transfers

However, new section 66A modifies the obligations of ordering and beneficiary institutions in respect of **virtual asset transfers**. Before providing the relevant designated service, they must each conduct counterparty due diligence to determine on reasonable grounds whether the virtual asset wallet to which the virtual asset is being transferred (for the ordering institution) or from which the virtual asset has been transferred (for the beneficiary institution) is:

(a) a custodial wallet in the control of a person meeting certain conditions; or

(b) a self-hosted wallet controlled by the payer/payee.

If the custodial wallet is controlled by a person who is required to be licensed or registered under a law that gives effect to FATF Recommendations, and the person is not licensed or registered, the ordering institution is prohibited from accepting the instruction and the beneficiary institution is prohibited from making the transferred value available.

If the custodial wallet is controlled by a person who is required to be licensed or registered, and is so licensed or registered, or is not required to be licensed or registered, the ordering institution can accept the instruction and must pass on the travel rule information, and the beneficiary institution, subject to obtaining the required travel rule information, can make the transferred value available. These requirements are subject to exceptions, such that:

- an ordering institution can decline to pass on the travel rule information in certain circumstances, including that it believes the beneficiary institution is not capable of receiving the information securely; and
- a beneficiary institution can make the transferred value available without having obtained the travel rule information in certain circumstances, including that an institution in the value transfer chain is not capable of passing on the information securely.

Section 66A appears to qualify the obligations of the ordering institution in relation to the collection of travel rule information in respect of a self-hosted wallet controlled by the payee. Although the Explanatory Memorandum describes that there are "*limited travel rule obligations where virtual asset transfers are in relation to and from a self-hosted wallet, acknowledging the limitations in obtaining travel rule information in these scenarios*", it is not clear that an equivalent qualification is proposed to the travel rule obligations of a beneficiary institution in relation to virtual asset transfers from a self-hosted wallet controlled by the payer.

Key considerations in connection with the Travel Rule

Issue	Insights
AML/CTF Rules to provide more information	A significant amount of the detail in respect of the travel rule in Schedule 8 is left to the AML/CTF Rules in order to provide flexibility for any future changes once the current review of FATF Recommendation 16 by the FATF is completed. In particular, the precise content of the travel rule information and the nature of any proposed exemptions under section 67 have been left for future rule-making. This creates a level of uncertainty of the proposed amendments at this stage of the legislative process.
Expansion of travel rule obligations	While the exact parameters of the travel rule remain uncertain, it is clear that the Bill would increase the regulatory burden, particularly for the ordering institution in relation to the collection, verification and passing on of travel rule information. In respect of an ordering institution's own customers, for which CDD would already have been undertaken, the Explanatory Memorandum indicates that the burden is likely to be ameliorated under AML/CTF Rules that will not require such information to be collected and verified again. The Explanatory Memorandum also makes clear the legislator's expectation that, where an ordering institution is unable to include the required information with the value transfer, it should not pass on the transfer message for the transfer of value. Where civil penalties are proposed to apply to contraventions of these provisions, it will be important for reporting entities to implement robust systems, processes and controls to accurately operationalise the requirements.
Scope of obligation to take 'reasonable steps' to monitor	For beneficiary institutions and intermediary institutions, it will be important to understand the scope of the obligation to take 'reasonable steps' to monitor whether they have received the travel rule information and (for beneficiary institutions) whether the information about the payee is accurate. Like many of the provisions relating to the travel rule, the rule-making power has the potential to significantly alter the application of the relevant provisions. In this regard, it is encouraging that the Explanatory Memorandum emphasises that 'reasonable steps' may include "*sampling of transfer messages*" and not "*reviewing every transfer message individually*", recognising the volume of transfer messages handled by some institutions.
Scope of obligation to 'take such other action' as the beneficiary institution or intermediary institution 'determines'	When a beneficiary institution or an intermediary institution detects that it has not received all of the required travel rule information or (for beneficiary institutions) the information about the payee is not accurate, as an alternative to refusing to pass on the transfer message or make the transferred value available (as applicable), the Bill proposes that the institution would be entitled to 'take such other action' as it 'determines'. While the Explanatory Memorandum suggests that an institution acting under this provision in good faith will not be liable due to the protection from liability under section 235 of the AML/CTF Act, it will be necessary for reporting entities to carefully consider the nature of 'other action' that would be sufficient to ensure that they would be entitled to that protection.
Modification of travel rule for virtual asset transfers	The regime proposed by the Bill for travel rule obligations in respect of virtual asset transfers is detailed and imposes new requirements, including as to the conduct of counterparty due diligence to determine on 'reasonable grounds' the type of virtual asset wallet involved in the value transfer and certain exceptions. It will be necessary for institutions involved in virtual asset transfers to obtain a clear understanding of the standards expected in relation to the conduct of that due diligence and in satisfying the grounds for reliance on the proposed exceptions.

International value transfer services – the new IFTIs

What is currently required and what did the Consultation propose?

The AML/CTF Act currently contains reporting obligations attaching to international funds transfer instructions (**IFTIs**). If a person sends an instruction out of Australia or receives an instruction into Australia the reporting obligation applies. IFTI reporting obligations attach to financial institutions as well as those involved in designated remittance arrangements, though the 'sender' and the 'receiver' of an IFTI are not defined by reference to those institutions.

The Consultations proposed focusing on the movement of value, rather than the movement of instructions. Further, to simplify the reporting obligations, they proposed to shift the obligation to report an outgoing IFTI from the 'sender' to the ordering institution initiating a transfer of value under an instruction by a payer, and to shift the obligation to report an incoming IFTI from the 'receiver' to the beneficiary institution making the transferred value available to the payee.

Aligned with the introduction of the umbrella concept of 'value transfer services', the Consultations also proposed to collapse the distinction between 'IFTI-Es' and 'IFTI-DRAs' and introduce a streamlined new reporting framework.

What does the Bill propose?

As contemplated by the Consultations, the Bill rewrites the IFTI reporting regime to align with the new concepts of 'transfers of value' and the 'value transfer chain'. Instead of an IFTI, the relevant transfer is an 'international value transfer service' (**IVTS**). An IVTS is defined in a new section 45 as an item 29 or 30 designated service that results in the transfer of value into or out of Australia.

With the shift in emphasis to the transfer of value and the explicit reference to the roles of ordering institutions and beneficiary institutions in providing the designated services in items 29 and 30, the reporting obligation is also proposed to shift to those institutions as opposed to the 'sender' or the 'receiver' on the previous 'first in / last out' principle.

Proposed application of IVTS reporting requirement

Under the Bill, reporting entities have the following reporting requirements in respect of IVTS:

Role of entity	Designated service	IVTs reporting requirements
Ordering institution	Item 29	Must report to AUSTRAC within 10 business days after the reporting entity passes on or receives the transfer message for the transfer of value unless certain exceptions apply
Beneficiary institution	Item 30	
Intermediary institution	Item 31	May be appointed under agreement to discharge obligations of ordering or beneficiary institution, or as specified in the AML/CTF Rules

Modified application to transfers to or from unverified self-hosted virtual asset wallets

The Bill also introduces separate reporting requirements in relation to the provision of an item 29 or 30 designated service which involves a transfer of virtual assets to or from an unverified self-hosted virtual asset

wallet. The relevant report must be provided to AUSTRAC within 10 business days after providing the service and the content of the report will be specified in the AML/CTF Rules. It is important to note that this separate reporting regime for the transfer of virtual assets to and from an unverified self-hosted virtual asset wallet is being introduced in recognition of the technical challenges that can militate against the identification of such transfers as international in character. It applies to all such transfers, whether or not they are domestic or cross-border.

Trigger for reporting

The trigger for reporting outlined in the Bill departs somewhat from what was proposed in the Consultations. While Consultation Paper 2 suggested that the reporting obligation would be triggered when an ordering institution had initiated the process of transferring value or a beneficiary institution had made the transferred value available to its customer, the Bill refers instead to the ordering institution having "passed on" and the beneficiary institution having "received" the transfer message for the transfer of value.

Exceptions, amendments and withdrawals

The Bill proposes exceptions to the reporting obligation where, within the 10 day period, the reporting entity either reasonably determines that the transfer of value will not occur, or takes reasonable steps to ensure that the transfer of value will not occur.

The Bill also proposes that the AML/CTF Rules may provide for the amendment or withdrawal of an IVTS report or a report in respect of a transfer of value involving an unverified self-hosted virtual asset wallet.

Key considerations in connection with international value transfer services

<table>
<tr><th>Issue</th><th>Insights</th></tr>
<tr><td>Value "in" Australia and ending up "in a foreign country"</td><td>Reporting entities will need to appreciate the wide-reaching implications for the reporting of international transfers of the shift in emphasis proposed by the Bill from the transfer of instructions to the transfer of value. The new formulation for an IVTS to arise – of value being "in" Australia and "as a result of the provision of the service" being in a foreign country (and vice versa for incomings) – may significantly broaden the net to capture many more products and services where reporting of IVTS is required.

By way of example, under the current regime an IFTI may not arise when a payer does not 'control' the money to be transferred, or when it is difficult to identify a relevant 'instruction' (for example in respect of a payment using a credit card). Given the potential for a significant increase in reporting requirements, and the civil penalties that apply for contraventions, reporting entities will require clear guidance as to their obligations under the new regime.</td></tr>
<tr><td>Change in the entities to have reporting obligations</td><td>The other key change is a shift in which entity is required to report the international value transfer. See below:

<table>
<tr><th>Transfer</th><th>Current AML/CTF Act</th><th>Proposed change in the Bill</th></tr>
<tr><td>Into Australia from a foreign country</td><td>Sender of the IFTI transmitted out of Australia</td><td>Ordering institution which accepts an instruction to transfer value out of Australia</td></tr>
<tr><td>From a foreign country to Australia</td><td>Receiver of the IFTI transmitted into Australia</td><td>Beneficiary institution which makes the transferred value available in Australia</td></tr>
</table>

Note: intermediary institutions may also have reporting obligations in certain circumstances, as noted above.</td></tr>
</table>

<table>
<tr><th>Issue</th><th>Insights</th></tr>
<tr><td>AML/CTF Rules to provide more information</td><td>As with other reforms contained in Schedule 8, a significant amount of the detail relating to IVTS is left to the AML/CTF Rules, including:
• the form of the IVTS report and the manner in which it is to be submitted to AUSTRAC
• the information that is to be included in the IVTS report
• the circumstances in which the obligations on the reporting entity must be discharged by the intermediary institution
• the manner in which the intermediary institution must discharge the reporting obligation
• the types of IVTS and the circumstances in which an IVTS may be subject to an exception to the operation of the reporting obligation
• provisions for the amendment or withdrawal of an IVTS report or a report of a transfer of value involving an unverified self-hosted virtual asset wallet
This creates a level of uncertainty in relation to our understanding of the proposed amendments at this stage of the legislative process. Institutions impacted by these proposed amendments should carefully consider the detail of the AML/CTF Rules when they are released so as to ensure that the requirements are accurately operationalised.</td></tr>
<tr><td>Exceptions to reporting obligation and the provisions for withdrawal and amendments</td><td>The reforms proposed by the Bill have the potential to resolve much of the regulatory confusion around whether a report should be submitted when the transfer instruction is withdrawn or aborted and the circumstances in which a report that has already been submitted should be withdrawn or amended.
As with other aspects of Schedule 8, much of the detail will be contained in the AML/CTF Rules, so it will be important to keep these provisions under close review as the legislative process continues.</td></tr>
<tr><td>Transfers of virtual assets</td><td>The separate reporting obligation to apply to transfers of value to and from unverified self-hosted digital wallets signals the legislature’s focus on ensuring that regulation keeps step with modern payment services and demonstrates an awareness that there are technical difficulties in determining whether such transfers originate from, or are intended to go, offshore.
The challenges with virtual asset transfers are also reflected in an additional rule-making power in section 45(2) that is intended to allow the AML/CTF Rules to specify the circumstances in which value is “in” a country, for the purpose of satisfying the definition of an IVTS. As the Explanatory Memorandum notes, the intention is that, given the non-physical nature of value, the rules will enable the location of value to be determined by reference to matters such as the location of the permanent establishment of the institution at which the value is held or dealt with.</td></tr>
</table>

Key insights

In many ways, the revised regime will be a welcome change as it provides far more flexibility for legitimate information sharing than has historically been the case.

However, some challenges will remain.

Issue	Insights
Scope of information	The scope of information covered by the offence is now much narrower. While it still includes that a reporting entity has given, or is required to give, a report

Issue	Insights
	under section 41 (as well as a copy of the report itself), or information or documents in connection with a 'section 49' notice, the 'inference' material has been limited to a "*document purporting to set out information (including the formation or existence of a suspicion) contained in such a report*" (emphasis added). This should substantially restrict the breadth of documents to which this subsection applies, predominantly to those that expressly or apparently convey the details of the SMR or underlying suspicion.
Prejudice to an investigation - application where exemptions previously provided protection	Sharing information within a reporting group, with legal advisors or in connection with program audits does not appear intended to constitute tipping off under the reframed offence because these sorts of disclosures would not ordinarily be expected to prejudice an investigation. Even so, the reframed offence (the fault element for which includes recklessness) will still require careful assessment. It would be prudent to document any such assessment. It would also be prudent to consider implementing safeguards for routine disclosures (such as intra-group disclosures) e.g. restricting the audience to whom the information is shared, taking steps to minimise the risk of inadvertent on-disclosure (such as through password protection) and tightening polices for disclosure to third parties.
Prejudice to an investigation – wider application	In the (less usual) event that information falling under the reduced scope may need to be disclosed to other third parties (such as to customers or litigants), the question of prejudice will need to be considered on a case by case basis. The Bill and Explanatory Memorandum (**EM**) provide only limited guidance as to the circumstances that would or could reasonably be expected to prejudice an investigation. Noting that the restriction is intended to cover investigations regardless of whether they have in fact commenced, this does raise questions as to how a reporting entity might reasonably be expected to know whether they can safely proceed. Further guidance on this from AUSTRAC would be useful.

Rewrite of tipping off offence

What is the current state?

The current tipping off regime has been notoriously challenging for reporting entities to navigate.

In its current form, s 123 of the Act prohibits a reporting entity from disclosing any of the following to a person other than an AUSTRAC entrusted person (subject to certain limited exceptions for (a) and (b) below):

(a) that it has issued, or is required to issue, a suspicious matter report;

(b) any information from which (a) could reasonably be inferred;

(c) certain other information relating to notices issued under subsection 49(1) of the Act.

This framework has given rise to a range of practical difficulties. For example:

- it can be extremely hard to identify (and therefore to contain) the precise nature and scope of information that could give rise to a reasonable inference that a suspicious matter reporting obligation has arisen. This has sometimes impeded entities in seeking to best mitigate and manage their ML/TF risk because they have felt understandably constrained in terms of what can safely be communicated to the customer or other third parties when seeking to undertake enhanced due diligence, terminate relationships or justify other good faith decision-making;
- the current range of exemptions is not broad enough to allow information to be disclosed to related bodies corporate that are not themselves reporting entities. This is particularly problematic for companies whose AML/CTF programs are overseen by parent companies that do not themselves provide designated services or whose operations are performed by services entities;
- there are substantial limitations on the intelligence that can be shared between organisations (for example, between unrelated financial institutions); and
- there can be significant cost and risk associated with the exercise of complying with court orders (for example, to provide discovery or respond to subpoenas) in a manner that is consistent with tipping off obligations.

What does the Bill propose?

The Bill proposes a complete rewrite of the tipping off regime with a view to facilitating more flexibility in sharing information for legitimate purposes.

Under the revised regime:

(a) the prohibition is expanded to apply not only to reporting entities but also to their relevant personnel and others in their reporting groups;

(b) the restriction on disclosing “inference” material has been removed and replaced with a restriction on the disclosure of documents purporting to set out the contents (including formation and existence of a suspicion) of a suspicious matter report;

(c) the previous exceptions that expressly permitted disclosure for legal advice, audits and intra-group intelligence have been removed and replaced by a caveat that disclosure is only prohibited where it *would or could reasonably be expected to prejudice an investigation*; and

(d) there are now two express exemptions:

 (1) one that applies to tranche 2 entities (which allows those entities to communicate certain tipping off information to their client if done in a good faith effort to dissuade them from illicit activity); and

 (2) one that facilitates communications to other reporting entities for the purposes of detecting, deterring and disrupting financial crime.

Key insights

In many ways, the revised regime will be a welcome change as it provides far more flexibility for legitimate information sharing than has historically been the case.

However, some challenges will remain.

Issue	Insights
Scope of information	The scope of information covered by the offence is now much narrower. While it still includes that a reporting entity has given, or is required to give, a report under s 41 (as well as a copy of the report itself), or information or documents in connection with a 'section 49' notice, the 'inference' material has been limited to a "document *purporting* to set out information (including the formation or existence of a suspicion) contained in such a report" (emphasis added). This should substantially restrict the breadth of documents to which this subsection applies, predominantly to those that expressly or apparently convey the details of the SMR or underlying suspicion.
Prejudice to an investigation - application where exemptions previously provided protection	Sharing information within a reporting group, with legal advisors or in connection with program audits would not appear intended to constitute tipping off under the reframed offence because these sorts of disclosures would not ordinarily be expected to prejudice an investigation. Even so, the reframed offence (the fault element for which includes recklessness) will still require careful assessment. It would be prudent to document any such assessment. It would also be prudent to consider implementing safeguards for routine disclosures (such as intra-group disclosures) e.g. restricting the audience to whom the information is shared, taking steps to minimise the risk of inadvertent on-disclosure (such as through password protection) and tightening polices for disclosure to third parties.
Prejudice to an investigation – wider application	In the (less usual) event that information falling under the reduced scope may need to be disclosed to other third parties (such as to customers or litigants), the question of prejudice will need to be considered on a case by case basis. The Bill and Explanatory Memorandum (**EM**) provide only limited guidance as to the circumstances that would or could reasonably be expected to prejudice an investigation. Noting that the restriction is intended to cover investigations regardless of whether they have in fact commenced, this does raise questions as to how a reporting entity might reasonably be expected to know whether they can safely proceed. Further guidance on this from AUSTRAC would be useful.

Assisting an investigation of a serious offence

Current state

Where a reporting entity forms a suspicion for the purposes of s 41 of the AML/CTF Act, it is required by the AML/CTF Rules to undertake enhanced customer due diligence, which may involve seeking senior management approval for withdrawing the designated services from the relevant customer.

Given the offboarding of a customer may be contrary to the interests of law enforcement who could obtain further useful intelligence and/or evidence if the designated services continue, chapter 75 of the AML/CTF Rules provides a mechanism by which law enforcement can obtain exemptions for the reporting entity from certain of its AML/CTF obligations where compliance may otherwise alert the customer to the investigation.

What does the Bill propose?

The Bill seeks to amend the current mechanism under the AML/CTF Rules and bring it under the Act. It empowers agencies to issue 'keep open' notices directly to a reporting entity without the need for involving AUSTRAC in the granting of exemptions. Those notices can be issued (copied to AUSTRAC) by a "senior member" of specified agencies for investigations into "serious offences". It also enables the agency to extend the notices twice for a total period of 18 months (unless further authorised by AUSTRAC).

The Bill specifies that:

- the 'keep open' notice only entitles reporting entities to avoid compliance with the requirements of their AML/CTF policies, initial and ongoing customer due diligence obligations, 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";
- receipt of a 'keep open' notice does not compel a reporting entity to continue to provide a designated service to a customer and nor does the mere receipt of such a notice mean a suspicious matter reporting obligation arises for the reporting entity (albeit if there are other circumstances that result in a suspicion arising, the obligation remains);
- the form of and necessary content for the 'keep open' notice will be specified in the Rules; and
- AUSTRAC has the power to revoke a 'keep open' notice or a notice extension.

The Bill also includes an express exemption from compliance with the requirements of AML/CTF policies, initial and ongoing customer due diligence obligations, 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 reporting entity's suspicion where a suspicious matter reporting obligation arises".

Key insights

The proposed changes do not significantly differ from the current regime and so they should be familiar to those reporting entities currently within scope of the AML/CTF Act, albeit they may expose newly in-scope entities to unfamiliar lines of communication with law enforcement.

Issue	Insights
Narrow scope of the exemptions	The exemptions permit a reporting entity to not comply with certain obligations, but only in narrow circumstances. This underscores the importance for reporting entities to carefully assess which of their obligations will be impugned and the steps taken and matters they have considered to form that view.
Expiry or revocation of a 'keep open' notice does not mean no tipping off	The Bill makes clear that, for the purpose of the reframed tipping off offence, whether an investigation has commenced is immaterial to a reporting entity's assessment of whether disclosure of information would or could reasonably be expected to prejudice an investigation. In a similar vein, reporting entities should be careful to avoid placing undue reliance on the expiry or revocation of a 'keep open' notice in its tipping off assessments.

New AUSTRAC investigation and enforcement powers

Current state

The AML/CTF Act currently grants powers to AUSTRAC to compel the production of information or documents relevant to the operations of the Act, Rules or regulations (i.e. to assist AUSTRAC fulfil its role as the AML/CTF regulator). It also imposes a separate regime in which it can seek and obtain additional information from reporting entities in connection with reports made by them to AUSTRAC.

What does the Bill propose?

The Bill retains and amends AUSTRAC's existing information gathering powers, but it significantly expands upon them. Leaving to one side amendments that are introduced in the context of tranche 2 entities (particularly as to privilege), the expanded powers include:

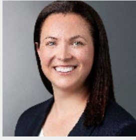
- **New intelligence-related powers under ss 49B and 49C:**
  - AUSTRAC has been given broader information-gathering powers in connection with supporting efforts to combat money laundering, terrorism financing, proliferation financing or other serious crimes, including to assist it with identifying trends, patterns, threats or vulnerabilities in relation not the same. Similar to the powers under s 49, AUSTRAC may give a written notice for the supply of information or documents, however these powers may be exercised by AUSTRAC without needing to be predicated by a report to it.
  - AUSTRAC has also been given the power to authorise others to supply it with information or documents of this kind, enabling the providing entity to overcome restrictions such as privacy and confidentiality.
- **Broadening of regulatory information-gathering powers under s 167:**
  - AUSTRAC's existing powers under this section have been expanded to enable the compelled production of information and documents relevant to the compliance with or enforcement of an offence or civil penalty provision of the AML/CTF Act or regulations, or an offence provision in the *Commonwealth Crimes Act 1914* or the *Commonwealth Criminal Code*, to the extent it relates to the AML/CTF Act.
  - The scope of the self-incrimination protections has also been narrowed to exclude protection in proceedings for money laundering, terrorism financing or proliferation financing.
- **New powers to obtain information/documents and examination power under Part 14, Division 3:**
  - The new examination regime is intended to be similar to that available to ASIC under Part 3, Division 2, of the *ASIC Act 2001*. It enables AUSTRAC to compel the production of documents and conduct examinations in relation to compliance with the AML/CTF Act, regulations or Rules, or an offence provision in the *Commonwealth Crimes Act 1914* or the *Commonwealth Criminal Code*, to the extent it relates to the AML/CTF Act, regulations or Rules.
  - There are several protections in relation to the new regime, including:
    - examinations are to take place in private, but may take place in-person or virtually;
    - an examinee's lawyer is entitled to attend (but it is a strict liability offence for an examinee's lawyer to continue to address or examine the examinee if requested by the examiner to stop doing so);
    - a written record of the examination must be made, if requested by the examinee; and
    - there are limited self-incrimination protections if the examinee claims in advance that the answer may tend to incriminate them.
  - At least currently, unlike with the exercise of similar powers by ASIC, there is no obvious carve-out with the AML/CTF Act for non-compliance where the person has a reasonable excuse.

Key insights

The need for broader AUSTRAC powers was raised in the April 2016 Statutory Review of the AML/CTF Act but not canvassed in any detail in the 2023 and 2024 consultations.

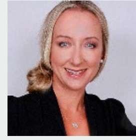
Issue	Insights
An area to watch	As the Bill progresses through Parliament, we anticipate that the expansion of AUSTRAC's investigation powers to be closely scrutinised and further amendments may be made prior to receiving royal assent.
Potential for more active intelligence-gathering and enforcement	Many of the amendments proposed by the Bill, such as to the tipping off offence and the introduction of the 'keep open' notice regime, should reduce the need for reporting entities and law enforcement to seek exemptions and modifications from AUSTRAC. These changes, coupled with bolstered powers for intelligence-gathering and enforcement, may enable AUSTRAC to redeploy resources from time-consuming administrative tasks to assume a more active role.

Key Contacts



Alice Molan
Partner

T +61 3 9288 1700
alice.molan@hsf.com



Charlotte Henry
Partner

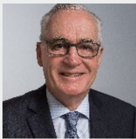
T +61 2 9225 5733
charlotte.henry@hsf.com

Bryony Adams
Partner

T +61 2 9225 5288
bryony.adams@hsf.com

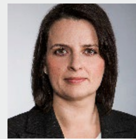
Kate Cahill
Partner

T +61 2 9322 4413
kate.s.cahill@hsf.com



Tony Coburn
Consultant

T +61 2 9322 4976
tony.coburn@hsf.com



Julia Massarin
Special Counsel

T +61 3 9288 1117
julia.massarin@hsf.com

Alix Conybeare
Senior Associate

T +61 2 9225 5476
alix.conybeare@hsf.com

Daniel Hyde
Senior Associate

T +61 2 9225 5480
daniel.hyde@hsf.com

Nicola Holdsworth
Senior Associate

T +61 2 9322 45551
nicola.holdsworth@hsf.com

For a full list of our global offices visit **HERBERTSMITHFREEHILLS.COM**