HERBERT SMITH FREEHILLS

AML/CTF CONSULTATION COMMENTARY

MAY 2023

Contents

Introduction

The Commonwealth Attorney General's Department released its Consultation Paper, *Modernising Australia's anti-money laundering and counter-terrorism financing regime* on 20 April 2023 (**Consultation**). Since then the headlines have been captured by the long-awaited proposed extension of anti-money laundering and counter-terrorism financing (**AML/CTF**) regulation to cover certain activities of the so-called gatekeeper professions. If implemented, that extension will certainly have important implications for lawyers, accountants, real estate agents, corporate and trust service providers, and dealers in certain high value goods such as jewellers. The extension appears likely to increase the number of reporting entities by a factor of 10.

However, what is also deserving of interest is the potential significance of some of the other changes that are being considered as part of the Consultation. We discuss these below.

Move to a single program

Currently, the Australian AML/ CTF regime requires reporting entities to adopt and maintain a written AML/CTF program that is divided into a Part A (being a part that is required to address the majority of processes, systems and controls for identifying, mitigating and managing the entity's money laundering and terrorism financing risk) and a Part B (being a part that is focussed on customer identification and verification).

The Consultation proposes to dispense with the delineation between Parts A and B and instead to streamline the Part A and Part B AML/CTF program requirements into a single **obligation** to develop, implement and maintain an AML/CTF Program that is effective in identifying, mitigating and managing the relevant risks of a business.

Superficially, this proposal holds some attraction because the distinction between Part A and Part B can create challenges in practice. Aside from the confusion that can arise in determining whether a particular process, system or control is strictly something to be recorded in Part A or Part B (and the risk that such a debate promotes form over substance in any event), the distinction can lead to design inconsistency and operational complexity. For example, while there can be considerable overlap between applicable customer identification procedures and enhanced customer due diligence requirements, and both may be triggered at the time of on-boarding a customer, the fact that the relevant procedures are contained in different Parts of an AML/CTF Program, and are required to be in different Parts, can create confusion as to how the two requirements are intended to intersect in practice. Removing the delineation between Part A and Part B may provide reporting entities with more freedom to structure their AML/CTF processes, systems and controls in a way that makes better holistic sense for their organisation.

If implemented, the proposal would simplify the approach to an AML/CTF Program. However, the proposal does create further complexity for AML/CTF governance, and it would impact how an AML/CTF Program is managed. For example, traditionally the AML/CTF laws have not required a reporting entity's board of directors to approve or oversee the requirements contained in its Part B (many of the requirements of Part B are highly technical and operational in nature). If those requirements for customer identification procedures are embedded into the one AML/CTF Program, consideration would need to be given to how that Program is overseen and what Board approvals the board is expected exercise appropriate approval and oversight of them. Practically, if a board is required to approve matters relating to customer identification and verification processes, this may also reduce operational flexibility when updating customer identification procedures.

Formalising an assessment of risk

Consistent with the expectations of the Financial Action Task Force (**FATF**), Australia's AML/CTF regime was implemented on the basis of adopting a largely risk-based approach to AML/CTF compliance. FATF's recommendation is built on the expectation that steps should be taken to identify, assess and understand money laundering and terrorist financing (ML/TF) risk and, based on this assessment, a risk-based approach applied to ensure that commensurate measures are in place to prevent or mitigate ML/TF. It follows that having an appropriate risk assessment should be seen as foundational - unless an appropriate assessment of ML/TF risk has been conducted, it will not be possible for a reporting entity to demonstrate that the processes, systems and controls that is has implemented to manage and mitigate the ML/TF risk are commensurate with the risk that is faced. Therefore it will not be possible to demonstrate that the entity's program design is compliant.

While it is clear that AUSTRAC sees the importance of risk assessments through this lens, and indeed it has consistently taken enforcement action on that basis, Australia's AML/CTF laws do not currently contain an express obligation that reporting entities are to prepare an enterprise level written assessment of its ML/TF risks in its business. In practice, this has led to some confusion as to the nature and level of detail required for ML/TF risk assessment as a matter of law.

The Consultation proposes that there should be an express obligation to identify, assess and understand the ML/TF risks against certain specified criteria and to document the methodology for doing so. It also proposes that the AML/CTF Rules be expanded to specify a number of items including appropriate periods for review of an entity's risk assessments, trigger events for reviews, and implementing AUSTRAC guidance or feedback on risks. On one view, this may not create any additional obligations as it would appear to track AUSTRAC's existing expectations. However, in practice we see a need to consider this aspect of the proposal particularly carefully.

In addition, although the particular risks facing gatekeeper professions are otherwise discussed in the Consultation, there is no discussion within the Consultation of the challenges that will be faced by these potential new reporting entities in assessing risks of their businesses. Many of this proposed new cohort of reporting entities will be comparatively small businesses which may regard the relevant risks as more remote for them than, say, the risks confronted by a provider of banking services. For these reasons we would expect there to be calls for the expectations and regulation of these businesses to be more prescriptive and less dependent on self-assessment which could be perceived as potentially more time consuming, resource dependent and expensive.

Mitigating risk

Once ML/TF risk is assessed, the foundation principle of a risk-based compliance framework is that measures are then put in place to mitigate and manage that risk. The Consultation proposes that the AML/CTF regime contain an express obligation to mitigate risks including obligations to apply internal controls.[1] The Consultation proposes the introduction of a clearer distinction between the obligation to develop and apply internal controls unique to the reporting entity, and a set of prescribed minimum risk mitigation measures which will be of general application. Nevertheless, it is proposed in the Consultation that the Rules could specify minimum categories of internal controls. This may be difficult to achieve in a uniform manner because internal controls will vary according to product type, customer type and jurisdictional risks. We expect that risk consultants both within reporting entities and those working as external consultants in the area of ML/TF risks will be making submissions on these complex topics.

Designated business groups

Section 123 of the AML/CTF prohibits "tipping off". It was amended in 2019 to allow a reporting entity to disclose to a related company that is a reporting entity that it had made a suspicious matter report in relation to a person or matter. This recognised that corporate groups often include entities that are not part of a designated business group but which provide services relating to AML/CTF compliance or to the supply of designated services by another reporting entity. For similar reasons, it is now proposed that a related company should be permitted to be part of a designated business group even if it is not a reporting entity.[2] This would be helpful to multinational corporate groups which often centralise global compliance functions in one company which may not be a reporting entity. That company may wish to receive information about the lodging of a suspicious matter report by an Australian reporting entity in the group because the compliance function will wish to support the Australian reporting entity in its dealings with the relevant customer.

Foreign branches and subsidiaries

Currently, a permanent establishment of an Australian resident entity in another jurisdiction (in effect a foreign branch of that entity) or a foreign subsidiary is subject to the Australian AML/CTF Act in relation to designated services that the branch/subsidiary provides in that foreign jurisdiction (through that branch or foreign subsidiary).[3] The relevant Australian entity or its foreign subsidiary (as applicable) must enrol with AUSTRAC and adopt an AML/CTF Program covering those designated services. Currently this obligation is modified in two important ways:

[1] Mitigating risk in Consultation Paper at page 8.

[2] Group wide risk management for designated business groups in Consultation Paper at page 9.

[3] Section 6(6) of the AML/CTF Act and see section 21 for the definition of "permanent establishment".

1 There are a number of specific exemptions in respect of particular AML/CTF requirements (for example, obligations to conduct an applicable customer identification in accordance with Part 2 of the AML/CTF Act do not apply).[4]

2 Where the permanent establishment of the reporting entity (which is the foreign subsidiary or the foreign branch) in the foreign jurisdiction is regulated by anti-money laundering and counter-terrorism financing laws 'comparable' to Australia, only minimal additional systems and controls need to be considered.[5]

In the Consultation, under the stated purpose of simplifying obligations, it is proposed that Australian businesses operating overseas should apply measures consistent with their Australian AML/CTF Programs in their overseas operations, to the extent permitted by local law (in those overseas places)[6]. This is controversial and will not be welcomed by Australian headquartered groups. No case is made for what the policy benefits of this approach would be for operations that are regulated according to local laws in another jurisdiction that is FATF compliant. Rather than simplifying obligations, it seems to complicate compliance for some Australian businesses because processes from two jurisdictions would be mandatory in the overseas jurisdiction. It would therefore appear to have an unwarranted anti-competitive effect by potentially making the Australian business more complex for customers to deal with, as well as adding a cost burden as a result of the duplication.

We expect that affected Australian businesses will argue that the Australian AML/CTF Act should not apply where operations in another jurisdiction are subject to comparable laws, on the basis that regulation by Australian laws does not serve any purpose in that situation.

Customer due diligence

The Consultation summarises the various obligations of a reporting entity relating to customer due diligence in the form of knowing the customer's identity, ongoing customer due diligence, enhanced customer due diligence and simplified due diligence. There is a proposal for the AML/CTF Rules to include high level standards for risk-based customer due diligence policies, procedures and controls[7]. This suggests that the expectations of AUSTRAC may become more prescriptive in relation to these matters.

It is contemplated that there will continue to be specified circumstances where identification and verification can be carried out ***after*** a reporting entity provides a designated service. With the growth of digital services, this is an area where we can expect submissions to be made which will make the case for on-boarding customers before completion of KYC, if this can be justified on the basis of a ML/TF risk assessment.

The Attorney General's Department will also be revisiting existing safe harbour and permitted simplified due diligence processes which were found not to meet international best practice in Australia's 2015 FATF Mutual Evaluation, on the grounds that they were insufficiently risk based. The relevant processes under the current AML/CTF Rules do make it considerably easier and faster for reporting entities to verify identity and other relevant matters in many circumstances for individuals, listed companies and their subsidiaries, certain companies with regulated activities, and some categories of trust which are subject to regulatory oversight.

In making changes to the current regime to meet FATF requirements, in our view regard should also be had to ensuring that there are not unintended adverse effects on timing and cost for many forms of transaction. We expect that reporting entities will make submissions focussing on the benefits of these methods and weigh them against the applicable ML/TF risks.

At a minimum, as part of proposed reforms, it seems that reporting entities may be asked to consider certain specified factors, including (presumably) risk factors, before relying on any simplified due diligence formula.[8] We expect that there will be strong support for the Consultation's proposal of providing ongoing flexibility in connection with online and remote service delivery.[9]

---

[4] Section 39(5) of the AML/CTF Act.

[5] See Parts 8.8.3 and 9.8.3 of the AML/CTF Act.

[6] Foreign branches and subsidiaries in Consultation Paper at page 9.

[7] Know your customer in Consultation Paper at page 11.

[8] Simplified due diligence in Consultation Paper at page 12.

[9] Revised obligations during COVID-19 pandemic in Consultation Paper at page 16.

Tipping off

AUSTRAC receives many requests for exemptions from the prohibition on disclosure of information indicating, or from which it could be inferred that, a suspicious matter report had been lodged by a reporting entity. The existing prohibition in section 123 of the AML/CTF Act includes a patchwork of permitted disclosure circumstances. The Consultation is now proposing to modernise the approach to the prohibition and points to a different model which targets and prohibits conduct or an intention to compromise a law enforcement investigation.[10] It appears that this model has been adopted in the United Kingdom and in Canada. We expect that this matter will be the subject of many submissions about practical barriers which arise in the existing prohibition and the benefits of modernising these provisions.

Assisting an investigation of a serious offence

Under the current regime, if a suspicious matter report is made to AUSTRAC by a reporting entity, it triggers an obligation for the entity to conduct enhanced customer due diligence (**ECDD**) under its AML/CTF Program. Chapter 15 of the AML/CTF Rules specifies principles for ECDD and these include a requirement that ultimately the reporting entity must decide whether a designated service should continue to be provided to the customer[11]. Reporting entities are frequently concerned that terminating services to a customer will alert the customer to the likelihood that there will be a criminal investigation, and result in *tipping off* the customer. This has resulted in numerous case-by-case applications for exemptions by reporting entities which the Department describes as administratively burdensome and inefficient[12].

The Consultation proposes that “eligible agencies” (although not stated, these appear to be law enforcement agencies) would be permitted to issue a “keep open” notice given directly to a reporting entity and copied to AUSTRAC. In that case the reporting entity would take the benefit of an exemption so that further customer identification steps are not needed if the reporting entity has a reasonable belief that CDD measures would alert the customer to the existence of a criminal investigation. We expect that entities will submit that this exemption needs to extend to any steps that the reporting entity takes, including the continued supply of designated services (e.g. under a transaction account with an ADI), where the reporting entity has a reasonable belief that an alternative approach would alert the customer to the existence of a criminal investigation.

Digital currency exchanges

Digital currency exchanges are currently regulated only for transactions which exchange fiat currency to digital currency (and vice versa). The Department is proposing extension of the AML/CTF Act to the following services[13]:

- exchanging one digital currency for another;
- transferring digital currency on behalf of a customer;
- safekeeping or administration of digital currency; and
- financial services relating to the issue and sale of a digital currency (including initial coin offerings).

This list of services is consistent with FATF Recommendation 15 and FATF’s “Guidance for Risk-Based Approach to Virtual assets and Virtual Asset Service Providers”. FATF’s expectation is that virtual asset service providers are licensed or registered and subject to regulation for AML/CTF purposes. On one view, amendments to the AML/CTF regime may not be necessary for the purpose of satisfying this requirement because digital currency has been held to be “property”[14] in other jurisdictions which, in our experience, the Australian market adopts, so other designated services may already be enlivened in practice in relation to digital currency exchanges.

It is therefore not immediately clear why a transfer of digital currency would require regulation additional to what already exists in item 29 of the table in section 6(2) of the AML/CTF Act which applies to acceptance of

[10] Proposed model in Consultation Paper at page 13.

[11] See paragraph 15.10(6) of the AML/CTF Rules.

[12] Exemption for assisting an investigation of a serious offence in Consultation Paper at page 15.

[13] Regulation of digital currency exchanges in Consultation Paper at page 13

[14] See, for example, *David Ian Ruscoe and Malcolm Russell Moore v Cryptopia Limited (in liquidation) [2020] NZHC 728* (8 April 2020).

an instruction to transfer "money or property" in a remittance arrangement, save for, perhaps, absolute clarity.[15]

Similarly, since digital currency is likely to be held to be property in Australia, an arrangement for its safekeeping would be providing a custodial or depositary service that is a designated service for the purposes of item 46 of the table in section 6(2) of the AML/CTF Act. The expression "providing a custodial or depositary service" is defined inclusively in section 5 of the AML/CTF Act and must therefore be taken to have its ordinary meaning which appears to cover safekeeping of property.

Travel rule

For information that is to accompany a transfer of funds or value (for example in an international transfer of funds), the Consultation proposes to require that[16]:

- payer information be verified; and
- payee information be included.

This requirement could be extended to remitters and to digital currency exchange providers. These changes would align Australia with FATF recommendations. It will be important to clarify the relevant obligations of a sender of funds which is an interposed institution which does not have a direct relationship with a payer or ultimate payee.

Repeal of the Financial Transactions Reports Act 1988 (FTRA)

The FTRA was the legislation governing AML/CTF matters prior to the adoption of the AML/CTF Act. It was adopted at both State and Federal level. It continues to contain obligations for "cash dealers" (as defined) to report to AUSTRAC:

(a) any significant cash transactions (of $10,000 or more)[17]; and

(b) any suspect transactions to which the cash dealer is a party[18].

This obligation covers a wide range of businesses including AFSL holders and solicitors. No report needs to be lodged if a suspicious matter report has been lodged under the AML/CTF Act in respect of the same matter.

The Consultation proposes that the FTRA might be repealed as first recommended by the 2016 Statutory Review conducted by AUSTRAC[19].

A cash dealer has immunity from suit for lodging a suspect transaction report (**STR**) in the same way that a reporting entity has immunity for lodging a suspicious matter report (**SMR**). In the face of the proposed repeal of the FTRA, submissions from reporting entities are therefore likely to probe the distinction between the circumstances when a STR can be made when compared with a SMR. In the FTRA, it is sufficient that there is a transaction that is suspect if a cash dealer is a party to it. In the case of a SMR, the reporting obligation under section 41 of the AML/CTF Act arises where a reporting entity commences to provide, or proposes to provide, a designated service, and the suspicions are of a specified kind. It might be argued that there are some circumstances where the AML/CTF Act may not require a SMR where a suspicion arises in relation to an event that occurs after a designated service has been provided in relation to a transaction to which the reporting entity is a party.

Where to from here?

The Consultation closes on 16 June 2023 for submissions. Further consultation by the Department is expected later in the year on the specifics of the proposals.

We are happy to assist with preparing submissions for our clients or to respond to any specific questions you may have.

---

[15] A designated remittance arrangement is also defined in section 11 of the AML/CTF Act to apply to money or property.

[16] Modernising the travel rules obligations in Consultation Paper at page 14.

[17] Section 7 FTRA.

[18] Section 16 FTRA.

[19] Repeal of the Financial Transactions Reports Act 1988 in Consultation Paper at page 16.

Key contacts

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

Charlotte Henry
Partner
T +61 2 9225 5733
Charlotte.Henry@hsf.com

Alice Molan
Partner
T +61 3 9288 1700
Alice.Molan@hsf.com

Juliana Warner
Partner
T +61 2 9225 5509
Juliana.Warner@hsf.com

Tony Coburn
Consultant
T +61 2 9322 4976
Tony.Coburn@hsf.com