AFMA

22 December 2020

Committee Secretariat
Select Committee on Financial Technology and Regulatory Technology
PO Box 6100
Canberra ACT 2600

By email: fintech.sen@aph.gov.au

Dear Sir/Madam

Second Issues Paper – AFMA Submission

The Australian Financial Markets Association (AFMA) represents the interests of well over 120 participants in Australia's wholesale banking and financial markets. Our members include Australian and foreign-owned banks, securities companies, treasury corporations, traders across a wide range of markets and industry service providers. Our members are the major providers of services to Australian businesses and retail investors who use the financial markets. We are pleased to provide a submission to the Select Committee on Financial Technology and Regulatory Technology ("the Committee") on its Second Issues Paper.

We note that the ambit of the Committee's Inquiry has broadened and the issues considered in the Second Issues Paper go to the competitiveness of Australia as a location conducive not just to Fintech and Regtech firms but also to the conduct of mobile financial service business in order to capitalise on opportunities arising from the increase in digitisation globally and the geopolitical turmoil in Hong Kong. In this light, AFMA is pleased to lodge a submission that considers the issues set out in the Second Issues Paper.

In responding to the Second Issues Paper, we note that AFMA has had significant engagement with respect to initiatives to promote Australia as a Financial Centre, including the recommendations of the landmark Johnson Report from 2009, the recommendations of which having bi-partisan support but remain largely unimplemented. It is noted that the issues relevant to the attraction and retention of mobile financial services business are aligned with those to develop and maintain Australia's Fintech and Regtech sectors, given the ability for providers to operate in a manner geographically separate from their customers.

Competitiveness of Australia's Corporate Tax Settings

The Second Issues Paper rightly highlights the uncompetitive nature of Australia's corporate tax settings as an inhibitor to attracting and retaining mobile business in

Australia. Further, we agree with the statement in the Second Issues Paper that the competitiveness of the corporate tax settings is not merely a function of the headline corporate tax rate but also goes to the structure of the system, including concessions and relief from double taxation.

Headline Corporate Tax Rate

AFMA has long maintained that Australia's high corporate tax rate, and indeed its high reliance on corporate tax as a revenue base, hinders the ability of Australia to attract foreign investment. This is particularly important in the context of attracting foreign capital to fund innovation where a high corporate tax rate exacerbates the risk associated with investment in companies in their formative stages. While the corporate tax rate alone is not the only tax disincentive for Australia as a destination for foreign capital, it is clearly an area where we have been slipping and tangible improvements can be made, as noted by the OECD in the statistics cited in the Second Issues Paper.

To the extent that Australia's dividend imputation system operates as a withholding tax as opposed to a final tax, at least in terms of resident shareholders receiving franked dividends, there is a discrepancy between the headline corporate rate of 30% and the actual amount of revenue raised that is referable to corporate taxation. However, this discrepancy only exists in relation to domestic shareholders that enjoy the benefits of imputation, and not the non-resident investors whose capital Australia is seeking to attract. Equity investors into Australian companies may be effectively taxed both in Australia (through the underlying corporate tax paid by the company) and in their jurisdiction of residence, to the extent that dividends paid by the company are not exempt from tax. It is for these foreign equity holders, therefore, that the high Australian corporate tax rate is the greatest disincentive for investment.

Offshore Banking Unit Regime

As previously advised to the Committee, AFMA has a number of members that are Fintech in nature, being innovative, highly technological companies that use Australia as a base from which to trade in international financial markets. These companies have developed trading technology and applications that are leading edge in global terms and have created sizeable businesses in Australia, employing a considerable number of staff. They are internationally mobile and choose to operate in Australia primarily to access a high-quality labour force and avail of the benefit of economic/political stability and a respected legal system. However, in order to maintain their competitiveness relative to competing firms in other jurisdictions in the Asia-Pacific region, these firms rely on the Offshore Banking Unit ("OBU") regime.

The OBU regime promotes Australia as a location from which to conduct mobile financial services business through providing a 10% corporate tax rate for eligible business, together with an interest withholding tax concession in respect of offshore borrowings. Contrary to its name, the OBU applies to a broad range of of financial service activities, including funds management and trading. The importance of the OBU regime was articulated in the Johnson Report into Australia as a Financial Centre, which stated:

> "the Forum believes that an effective OBU regime is a key element in ensuring that Australia's financial sector takes full advantage of opportunities to participate in international transactions."

As the Committee is aware, the OECD is currently conducting a review of the OBU regime and The Australian Government has, in October 2018, committed to amending the regime to ameliorate any concerns expressed by the OECD. At the time of writing, there was no clarity from the OECD as to the specific amendments to the regime that would be appropriate from an OECD perspective.

It is AFMA's view that Australia needs to ensure tax settings that apply to Fintech/Regtech businesses with offshore counterparties, and financial services businesses more generally, are sufficiently competitive so as to allow Australia to leverage its other advantages to attract and retain business, such as the Rule of Law, access to talent and relative legal and economic stability. AFMA's preference with respect to such settings is that any amendments to the OBU regime do not undermine the competitiveness of the regime but satisfy any OECD concerns, just as occurred with respect to the Singaporean Financial Sector Incentive (FSI) regime, which was also reviewed by the OECD but approved with only minor amendment. In the case that the amendments to the OBU regime do undermine its competitiveness, it is incumbent on the Government to implement settings that are at least competitive, if not preferable, to key regional competitor jurisdictions if Australia is going to be able to attract and retain mobile financial businesses, including Fintech. This may include providing concessional tax rates to mobile businesses with both domestic and offshore customers.

Regulation

Consumer Data Right

AFMA has long supported a consumer data right as a means of giving consumers greater control over their data and to move away from non-secure screen-scraping practices. In this regard AFMA has been an active participant in the Consumer Data Right (CDR) design process for many years. AFMA's contributions to the scheme have included making the case for a longer implementation period than was initially proposed and highlighting some early design issues regarding privacy aspects of the scheme, both matters that were subsequently addressed to the benefit of the scheme. We have also noted some security concerns around the differing standards applied to non-ADI participants in the scheme.

Consistent with our submissions to the policy processes around the Consumer Data Right, AFMA would have preferred the CDR to be implemented by a market-based and industry-led solution. We believe private-sector implementation would offer greater flexibility and lower cost and would encourage the Government to continue look for opportunities to move the scheme back to industry as it matures.

AFMA notes that we are still in the initial phase of CDR implementation in the banking sector. This has been a larger project than was anticipated. Ensuring the risks to privacy and data were properly identified by the sector and by government sponsored studies, and then appropriately addressed in the scheme design and implementation has taken considerable time and resources. Implementation of CDR for firms entails significant additions to the technological, human resources, compliance and business governance burdens on firms; it also increases the risks in the business environment with a punitive enforcement regime.

At this point while many of the costs have been realised in the deployment of CDR for ADIs the benefits are still yet to fully develop for consumers. AFMA suggests that further expansion of the CDR scope within banking (to write phase) and incremental sectoral applicability should follow only if an independent, contestable cost-benefit analysis suggests it would be of net benefit.

The Government is making welcome moves in its deregulation agenda which we believe will assist economic growth. Unnecessary intervention by regulation in the harmonising of electronic connections between businesses risks conflict with this agenda.

Data Standards and Blockchain

AFMA, through its Information Security Committee, has been actively and constructively engaged over the last two years with the development of the information security framework for the financial services industry through participation in multiple consultations and engagements with regulators and departments.

Thematically the key concerns that have emerged from our work in this area include:

- The information security regulatory framework requires consistency and rationalisation both in terms of:
    - overlapping and inconsistent regulatory standards for information security;
    - multiple regulators implementing these differing standards for the same firms and in some cases the same data with different approaches;
- The need for increased consistency with, and use of, international standards; and
- The need to move to a consistent accommodative regulatory stance for implementation of security standards.

In our view these changes are required in order to meet the Government's objectives around consistent information security outcomes. They would also have the benefit of reducing duplicative and unnecessary regulatory administrative burdens for business. This has potential to free up security budgets for more constructive work, and more generally to minimise the additional burden on the economy of the important uplift that is required in information security.

Multiple overlapping standards

Regulators are incentivised by their structures and exposure profiles to each take a fresh look at information security, come up with their own standard and implement the standard in accordance with their standard practices for other matters they regulate.

The result for financial firms can be that they may face siultaneous implementation of APRA's CPS/CPG 234, ASIC's cyber security standards, requirements under the Privacy Act Guidelines, RBA requirements (e.g. for RITS access) and ACCC's bespoke CDR standard. Recently the Government consulted on potentially introducing a further 'top-up' standard for some of these standards for firms deemed critical infrastructure. Given the maturity of the information security profile of the ADI sector, the result of the consultation was that it did not proceed with this proposal for now, however, around 10 ADI firms, some market infrastructure firms, insurance and superannuation firms that are captured by the proposed Rules threshold will be subject to additional positive security obligations.

ADI firms will also face mandatory external tripartite security audits under the recently announced APRA policy, and may be required to participate in cyber security drills under the Enhanced Security Obligations. Firms may also be required to participate in the Cyber Operational Resilience Intelligence-led Exercises (CORIE) scheme.

International standards
APRA's cyber security standard while sound is distinct from international standards such as the NIST framework from the United States and ISO 27001. ASIC in contrast supports NIST and is expected to release updated cyber security guidance as part of the response to its consultation CP314 in 2021, which might be further adjusted by the outcomes of its first prosecution for alleged licence condition breaches in relation to cyber resilience. The ACCC implemented a bespoke security standard for CDR, despite representations from industry of the importance of being consistent with other regulators, most notably APRA. The standard is based on a cut-down version of the APRA standard with a selection of guidance from the Australian Cyber Security Centre's recommendations. The ACCC has recently partially recognised ISO 27001 for some purposes when complemented with other audits.

Need for harmonisation
There is a high degree of overlap between these standards, but they are far from harmonised. A single graded national standard that recognises international standards such as NIST would be more likely to deliver consistently high security outcomes in comparison to the current multiplicity of standards. We note that many firms conform to these international standards in their home jurisdictions and there would be some efficiencies in using those same standards locally.

We understand the Council of Financial Regulators Cyber Working Group is working to harmonise the RBA, ASIC and APRA cyber requirements. We support this work and encourage the Government to require other regulators in financial services to also conform their requirements to the harmonised standards.

Regulatory stances
The regulators who enforce these standards have variant enforcement stances which vary from accommodative through 'responsive' to punitive. While most regulators in the space nominally adopt a responsive regulatory stance, in reality many regulators have tended towards more punitive stances.

We are of the view that an accommodative regulatory stance is more appropriate for enforcement of information security. An effective national information security response requires a joint effort that relies on firms promptly sharing information and while this can be mandated, it works less effectively in a punitive regime as firms will be more cautious about what they share. A punitive stance will also develop requirements slowly over many years as cases are resolved in court. This may not be an optimal approach for a rapid and comprehensive response to national security challenges.

An accommodative stance would recognise that this is a national problem and that all stakeholders are on the same side with good intentions. There are parallels with the approach taken to aviation safety:

- All parties are already heavily incentivised to ensure security arrangements are effective;
- Achieving full security is a highly complex and dynamically changing task that is difficult even for state actors to achieve; and
- A punitive regulatory stance will discourage information sharing and openness and may be damaging to security outcomes, harm the working relationship with business, increase business costs, and decrease the attractiveness of the jurisdiction.

Know Your Customer Regulations

The Second Issues Paper notes that the Committee has received feedback on the "current status of KYC obligations in relation to financial services providers, and the potential for streamlining some of these obligations while retaining adequate protections against fraud and other criminal activity."

In terms of streamlining effort with respect to KYC, it is appropriate to draw the Committee's attention to the amendments contained in the *Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Bill 2019* which received Royal Assent in December 2020. Specifically, the provisions contained in the Bill expand the circumstances in which a Reporting Entity may rely on another Reporting Entity having undertaken customer due diligence, thereby mitigating duplication of effort.

Under the reforms, Reporting Entities may rely on the customer identification procedures undertaken by another reporting entity as long as certain circumstances are satisfied. These reforms give potential for the centralisation of customer identification processes. It is noted that the reforms contained in the Bill require that the party on whom the reporting entity is seeking to rely is also subject to appropriate AML/CTF regulation and supervision, as required by FATF, and accordingly it will be open to the Committee to enquire further as to the appropriate legislative framework for centralisation of KYC obligations.

Access to Capital

Interest Withholding Tax

In the Second Issues Paper, the section on Access to Capital appears to focus purely on equity investment into companies. It would also be appropriate for the Committee to consider frictions that may hinder companies accessing debt funding from offshore, with the key friction being the imposition of interest withholding tax.

Under Australia's taxation legislation, generally payments of interest, amounts in the nature of interest or amounts in substitution for interest are subject to withholding tax when paid to an overseas lender. Generally, the rate of withholding tax is 10% of the amount of the interest payment and, commercially, it may be the case that the lender will require the borrower to "gross up" for the withholding tax such that the payer receives the full amount free and clear of any withholding tax.

AFMA has consistently argued against the imposition of interest withholding tax for amounts paid from Australia, particularly in the context of payments made by financial institutions that may act as intermediaries between the companies seeking to attract capital and the offshore investors. These views are consistent with recommendations from the Henry Tax Review and the Johnson Report into Australia as a Financial Centre and observations from the Financial System Inquiry. Further, the appropriateness of interest withholding tax has been considered by recent Government inquiries such as the inquiry on the development of the Australian corporate bond market.

Accordingly, in AFMA's view it would be appropriate for the Committee to inquire as to whether the imposition of interest withholding tax on payments made by Fintech and Regtech companies is hindering the availability of debt capital for such companies and/or increasing the cost of such funding through the gross-up requirement.

* * * * * *

Please contact me on 02 9776 7996 or rcolquhoun@afma.com.au if you have any queries about this submission.

Yours sincerely,

Rob Colquhoun
Director, Policy