CULTURE-RELATED REGULATORY ENFORCEMENT: WHERE MIGHT THE AUSTRALIAN 'BEAR' GO HUNTING?

gadens

gadens

Part One

This two-part briefing has been prepared for in-house legal, risk and compliance professionals in financial services firms, including insurance and superannuation entities.

Part one of this briefing covers the following matters:

- Introduction to the "Banking Executive Accountability Regime" (**BEAR**)
- What is required under the regime and penalties for individuals and companies
- BEAR's imminent expansion to all financial services entities.

Part two of this briefing covers the following matters:

- Recent culture-related enforcement action under the United Kingdom's Senior Managers & Certification Regime, upon which the BEAR is modelled
- How the UK experience may inform how BEAR will evolve in the Australian enforcement context
- Practical steps for entities to take now to mitigate their risk.

TRACKING THE BEAR

Introduction

Australia is being hit by a regulatory wave in the wake of the Hayne Royal Commission's findings of widespread misconduct in the financial services industry, characterised by numerous new laws and increasingly hawkish enforcement regulators. The expansion of the BEAR, which was purposively designed to drive up standards of culture in financial services, forms the backbone of Commissioner Hayne's recommendations for improvement. That is not surprising.

In the wake of the global financial crisis, problematic corporate culture has been identified by policymakers and regulators as a key driver of poor conduct.[1] BEAR is a direct response within the financial services sector. However, while improving financial services culture is a commendable objective, there is rising concern given BEAR is formed of broadly constructed principles-based laws which are yet to be applied. There are very serious consequences, especially for individuals, for getting it wrong.

[1] See, for example, a speech by John Price, Commissioner, Australian Securities and Investments Commission at the AICD Directors' Forum: Regulators' Insights on Risk Culture (Sydney, Australia), 19 July 2017.

gadens

The Australian financial services industry does not know enough of what the future holds to efficiently mitigate the potential for breaching offences which are inherently subjective and difficult to define.

The issue is arguably not confined to the private sector alone; *first,* BEAR is about to be expanded across nearly the entire financial services sector, i.e. not just banks; and *second*, there are many Federal and State Government entities who are likely to be caught by this expansion, including public-sector investment corporations with subsidiaries who hold financial services licences and publicly owned superannuation funds.

Fortunately, the United Kingdom offers some tea leaves which can be read by the legal, risk and compliance functions in Australian financial services entities to enable them to best advise their executives and board members. This is because BEAR is modelled on the UK Senior Managers & Certification Regime (**SMCR**), and the UK Financial Conduct Authority (**FCA**) and Prudential Regulation Authority (**PRA**) are further along in their journey of culture-related enforcement actions. Examining their recent actions and key statements offers an insight for the Australian financial services industry as to the direction our regulators may take imminently. We cover this in part two of our briefing.

THE BEAR NECESSITIES

What is it

The BEAR is set out in Part IIAA of the *Banking Act 1959* (Cth) and establishes accountability obligations for authorised deposit-taking institutions, i.e. banks and their senior executives and directors. It also establishes deferred remuneration, and key personnel and notification obligations for banks. While important, they are not the focus of this paper. Currently administered by the Australian Prudential Regulation Authority (**APRA**), BEAR came into effect for large banks in July 2018 and medium / small banks in July 2019. Critically, it requires senior executives and directors (called "accountable persons") to set out their responsibilities in writing in so-called "accountability statements". The bank must also provide an "accountability map" to APRA of all accountable persons.

Accountable persons include specified functions, e.g. Head of Anti-Money Laundering and others captured on an evaluative basis, i.e. the individual has "*actual or effective senior executive responsibility for management or control of the bank… or a significant or substantial part or aspect of the operations of the bank...*". A simple example is the head of a wealth management subsidiary of a large bank. The real bite is in the new accountability obligations on both the accountable persons and bank itself. These are partly based on the FCA's 11 Principles of Business (**UK Principles**) which are general statements of the main obligations that apply to firms that are regulated by it.

While familiar to the UK financial services industry, it is important to highlight that these rules have arguably minimal - or at best oblique – heritage in Australia's financial services regulatory landscape.

They are new and uncertain and require individuals to conduct their set responsibilities:

(a) by acting with honesty and integrity, and with due skill, care and diligence;

(b) by dealing with APRA in an open, constructive and cooperative way; and

(c) by taking *reasonable steps* in conducting those responsibilities to prevent matters from arising that would adversely affect the prudential standing or prudential reputation of the ADI.

Similar obligations are placed on the bank. As one example illustrating this point, what does it mean in practice to deal with APRA in an "*open, constructive and cooperative way*"?

While this does not explicitly displace legal professional privilege, how will that play out in future practice in circumstances where other global regulators are now making it a requirement for cooperation credit, e.g. UK Serious Fraud Office? And to what extent does the obligation undermine the privilege against self-incrimination, which is not a basis to refuse to comply with this new obligation?

There are significant penalties for breaching BEAR, including disqualification for individuals and up to $210 million in penalties for large banks, which place these uncertainties and more besides in a discomforting light. This is even more so when factoring in aggressive regulatory enforcement appetites (i.e. ASIC's "*Why not litigate*?" public mantra) and ASIC's recent "*stepping stones*" approach to enforcement, i.e. using failures at an entity level such as a breach of continuous disclosure obligations to target directors at a personal level.[2]

WHERE THE BEAR IS NOW

Imminent expansion

Like the UK SMCR, BEAR's defining purpose is to improve the culture within the broader financial services industry. This is directly stated in clause 1.7 of the BEAR Bill's Explanatory Memorandum. Both regimes embody prevailing regulatory theories in the wake of the global financial crisis that more flexible principles-based rules and a greater focus on individuals are pivotal to improving corporate culture. (The United States went down a different path with the more organic "Yates' Memo".)

Originally, BEAR only applied to banks and was to be enforced through a prudential lens by APRA. In his final report dated February 2019, Commissioner Hayne recommended that BEAR be expanded to all APRA-regulated financial services institutions, e.g. insurance and superannuation firms, and be dually administered together with the conduct regulator, ASIC. He also recommended that there be an accountable person "…*for all steps in the design, delivery and maintenance of all products offered to customers by the ADI and any necessary remediation of customers in respect of any of those products*" which is a huge responsibility.[3]

The Morrison Government agreed to these recommendations and went further, promising to "…*introduce a similar regime for non-prudentially regulated financial firms focused on conduct*… [which] *will apply to all* [Australian Financial Services Licence holders] and [Australian Credit Licence holders], *market operators, and clearing and settlement facilities*".[4] The Australian Treasury is working on a proposal paper for release later in 2019 and draft legislation is intended to be consulted on and introduced by the end of 2020.[5] Consultation time is expected to be limited. At the time of writing, APRA had not taken any actions under the BEAR – though we understand that it has opened at least one investigation under the regime.

In summation, the Australian financial services industry is to be tested with unfamiliar broad obligations – at least in the UK the SMCR was built on a comparable earlier regime the "Approved Persons Regime" – with severe personal and firm consequences being wielded by a newly hawkish APRA and ASIC. (This is also against the backdrop of an arguable juridical trend emphasising "fairness" as a regulatory standard, though that is for another article.)[6] One silver lining, however, is that the UK is further along in its journey of regulating culture. Examining the recent culture-related enforcement actions and statements by the UK regulators, including under the SMCR, offers financial services entities a possible insight into the direction the Australian regulators may take in the coming years and a chance to get on the front foot in mitigating their risk.

[2] See *Australian Securities and Investments Commission v Vocation Limited (in liquidation) [2019]* FCA 807

[3] The Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, Final Report dated 1 February 2019, Recommendations [1.17], [6.6] and [6.8].

[4] Government response to the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, February 2019

[5] Treasury, Financial Services Royal Commission Implementation Roadmap, 19 August 2019.

[6] For e.g., see *Australian Securities and Investment Commission v Westpac Securities Administration Limited [2019]* FCAFC 187 at 170.

gadens

Part Two

BEAR'S BRITISH RELATIONS

Recent UK culture-related enforcement

It is worth starting with the enforcement statistics from the FCA in its Enforcement Annual Performance Reports for 2017/2018 and 2018/2019. At 1 April 2017, there were 15 culture and governance related cases open. At 31 March 2019, there were 70 culture and governance related cases open – a 367% increase in two years. In part, this is likely to be due to the FCA's increasing use of the SMCR as an enforcement tool in the banking sector.

Turning to culture-related UK enforcement actions and key statements:

1. On 11 May 2018, the FCA and PRA jointly fined Mr. Staley, Barclays Bank plc's CEO, £642,430 and placed special requirements regarding whistleblowing systems and controls on the bank under the first SMCR action. The regulators found that Mr. Staley breached the individual requirement to act with "*due skill, care and diligence*" by attempting to identify the author of an anonymous letter received by the bank in June 2016. That letter claimed to be from a shareholder and made various allegations, primarily about the recruitment of the head of the bank's financial institutions group in New York (who was highly regarded by Mr. Staley). Instead of trying to uncover the whistle blower, the regulators alleged (and Mr. Staley agreed) that he should have passed the matter to those with expertise and responsibility for whistleblowing within the bank.

2. On 13 March 2019, the FCA fined The Carphone Warehouse £29 million for failings that underpinned the widescale mis-selling of mobile phone insurance and a technical support product. The FCA found that the company did not give its sales consultants the right training to give suitable advice to customers when purchasing the products (they were trained to recommend insurance to those who already had cover), many of which were later cancelled (which the FCA said should have been a clear indicator to management of mis-selling). The FCA found that The Carphone Warehouse did not "*organise and control its affairs responsibly and effectively, with adequate risk management systems*" or "*pay due regard to the interests of its customers and treat them fairly*" or "*ensure the suitability of its advice and discretionary decisions for any customer who is entitled to rely upon its judgement*" (Principles 3, 6 and 9 of the UK Principles.)

3. On 13 May 2019, in *Andrew Tinney v The Financial Conduct Authority*[7], the Upper Tribunal (which is similar to the Australian Appeals Tribunal), found Mr. Tinny, the former COO of the Wealth and Investment division for Barclays Bank plc, had acted without integrity and should be publicly censured. (This conduct happened before the SMCR so did not fall within the regime). Mr. Tinney obtained a report from an external professional services firm which was quite critical of the culture in the Wealth and Investment division. After this an anonymous email emerged which alleged that the external consultant's report had been suppressed.

Mr. Tinney then drafted a note to the bank's senior management, in connection to which he was found to have been reckless regarding whether it would give them the impression that the report did not exist and whether it would provide accurate detail about the external professional firm's involvement in the report. The critical issue was one of transparency within the bank's governance framework. The case was interesting in setting out this conception of the obligation of "*integrity*" (which forms part of Australia's BEAR responsibilities) at paragraph [13] of the judgment:

> ***"...A lack of integrity does not necessarily equate to dishonesty. While a person who acts dishonestly is obviously also acting without integrity, a person may lack integrity without being dishonest. One example of a lack of integrity not involving dishonesty is recklessness as to the truth of statements made to others who will or may rely on them or wilful disregard of information contradicting the truth of such statements..."***

4. On 29 May 2019, FCA fined R. Raphael & Sons plc, a UK-based independent bank, a total of £775,100 for breaches of its duty to "*conduct its business with due skill, care and diligence*" and to "*organise and control its affairs responsibly and effectively, with adequate risk management systems*" (Principles 2 and 3 of the UK Principles). The fine arose from circumstances where customers were unable to use prepaid and charge cards due to a technology incident which was shown to partly stem from problems with the bank's governance arrangements over outsourced services and procured service suppliers. (The PRA, not to be outdone, then fined the bank £1.1 million.) This action followed a similar fine of over £5 million on an insurer, Liberty Mutual Insurance Europe, regarding their governance oversight of a service provider which handled complaints made against it on its behalf on 30 October 2018.

[7] [2019] UKUT 0227

5. On 23 July 2019, the FCA fined Standard Life Assurance Limited over £30 million for failures to "*organise and control its affairs responsibly and effectively, with adequate risk management systems*" and for not having "*due regard to the interests of its customers and treat them fairly*" regarding circumstances where the bank sold annuities (generally a lifetime or fixed-term pension) to non-advised customers. The bank did not have adequate systems and controls to manage the risk of its interests taking precedence over fair customer outcomes. In part, this was because at the time it offered its front-line staff large financial incentives to sell annuities which encouraged them to place their interests ahead of their customers (as part of the sales process for non-advised annuities, firms are required to explain to customers that they may get a better rate if they shop around on the open market). Standard Life Assurance Limited also did not monitor the quality of calls between call representatives and non-advised customers and the management information it generated was inadequate for the purpose of allowing senior management to identify these problems.

6. On 23 May 2018, Megan Butler, the FCA's Director of Supervision - Investment, Wholesale and Specialist, advised a UK House of Commons' committee that the SMCR may be used to hold financial services firms to account for sexual harassment issues. Ms. Butler stated that:

> ***"From our perspective misconduct is misconduct, whether it is financial or non-financial. The key tool that we deploy in this area is what we call the senior managers and certification regime…We do not believe that a culture that tolerates sexual harassment and other forms of behavioural misconduct is a culture that will encourage a 'safe to speak up' environment, an environment where the best business decisions get taken, the best risk decisions get taken…. We do not compartmentalise that away from a consideration of what makes an individual fit and proper, and we expect firms to take all those aspects into account when they look at whether their key individuals are fit and proper to do their roles [for the purpose of the SMCR]"***

WHERE THE BEAR MAY GO

What the UK experience tells us

As with BEAR in Australia, the SMCR initially commenced in the banking, building society and credit union sector in March 2016 and later expanded. From 9 December 2019, it will apply to most FCA-regulated entities, including banks, building societies, asset managers, investment firms, insurers, mortgage providers, consumer credit firms and sole traders. There is no doubt that culture and governance cases will continue to rise as the SMCR expands and the FCA and PRA become more comfortable with these enforcement tools. Based the rise of culture and governance related cases in the UK, and the hardening domestic regulatory environment, we consider that Australia can likewise expect appreciable early use of the BEAR by APRA (and ASIC when it starts administering it).

In terms of the enforcement cases themselves, there are several interesting overarching takeaways. They include how broadly the UK is interpreting terms which also underpin our BEAR regime, e.g. "*integrity*" (expect ASIC to have paid attention to this case), the regulatory interplay between their key financial services regulators (ASIC and APRA are increasingly co-operating these days, and have just signed a new Memorandum of Understanding to facilitate information sharing and enforcement action) and the scope the FCA considers the SMCR will address, which may be thought outside the traditional domain of financial services regulators, e.g. sexual harassment.

In addition, there has also been a focus placed on training, systems and controls for customer-facing staff (which is a well-documented emerging ASIC theme already) and the perils associated with getting governance right around outsourcing arrangements. Also relevant is the focus on individuals; there has only been one SMCR sanction against an individual, i.e. Mr. Staley, since the introduction of the SMCR three years ago. That may suggest it is more difficult than originally anticipated to attribute a large company's failures to an individual. Our sense is that it remains too early to tell how this aspect will play out in the UK, let alone in Australia under the BEAR.

gadens

BEAR SAFETY

What to practically do now

The Australian financial services regulatory landscape is fluid. Banks subject to BEAR should consider their framework in light of the developments in the UK and continue to stress test their implementation. Are there any gaps in governance and controls? Would executives benefit from a "*reasonable steps*" review in their function area to increase assurance? Will significant incoming laws change the status quo, e.g. the new product design and distribution obligations? Vigilance is a necessity.

For those entities yet to face BEAR, including investment, insurance and superannuation entities, early engagement will pay dividends. The consultation period for the extended BEAR, now being colloquially called "FEAR" (Financial-services Executive Accountability Regime), may be short if the last consultation periods are to be taken as a guide (and, compounding matters, could occur over the upcoming Christmas / New Year period). In terms of black-letter requirements (mainly the development of the accountability statements listing individuals' responsibilities and an accountability map), BEAR appears deceptively simple, though in our experience its implementation can be quite challenging if not structured tightly from the start. (A common issue is the division of responsibilities between the IT and front-line functions, and the inclusion of General Counsel's division given their unique role.)

With this said, there is enough design detail from both the existing BEAR (and expanded UK SMCR), to meaningfully commence preparations. This will include an analysis of governance frameworks to determine the likely accountable person population and their key responsibilities. Ultimately, for accountable persons, one of their key concerns will be "*Do I have the necessary information* **and** *control to discharge my specified responsibilities, for which I am now personally responsible to the regulators?*" If not, and a problem later arises in their function area, they may run the risk of BEAR coming too close for comfort...

CONTACT US

LIAM HENNESSY
Financial Services Specialist
T: +61 7 3114 0291
E: liam.hennessy@gadens.com

Liam is a Financial Services specialist at Gadens. He is well-versed with both the UK SMCR and the BEAR. Additionally, he has significant experience in financial services compliance / risk matters, regulatory inquiries and disputes, and has practised in Brisbane, Sydney, Melbourne and London. He is also the primary author of the Australian regulators weekly wrap.