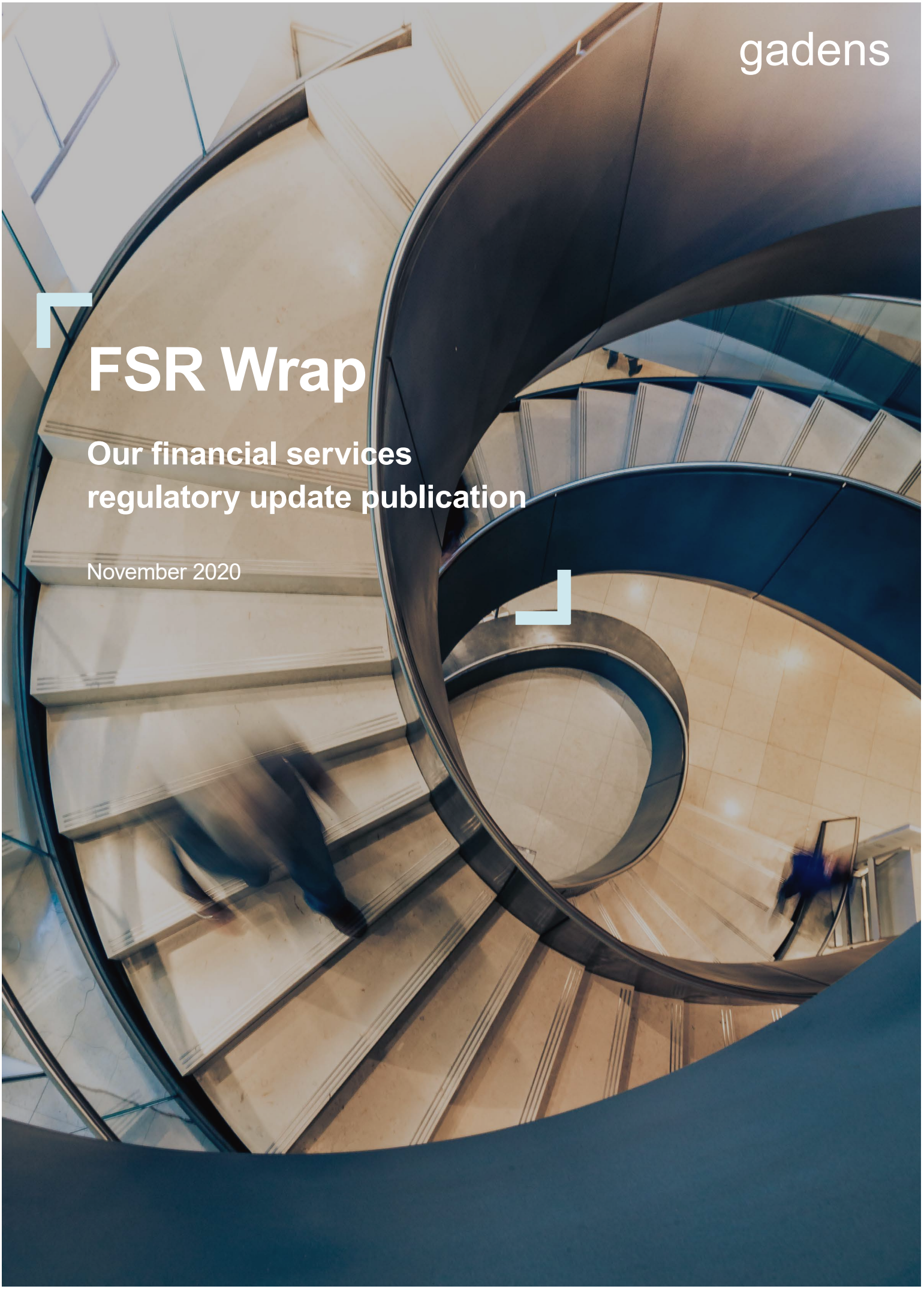
gadens



FSR Wrap

Our financial services regulatory update publication

November 2020

gadens

Welcome to the
November edition of

FSR Wrap

While the first edition of FSR Wrap focused on the impact of the COVID-19 pandemic on financial services regulation, we have decided to consider some more 'business as usual' regulations of importance to Australian financial services companies in this edition. As we approach the end of 2020 (phew!), it is a good time to think about issues that are important now and into the future before a slew of regulations that have been in coronavirus stasis (notably the new Financial Services Royal Commission legislation) come online in 2021.

An example of a somewhat overlooked matter of importance for financial services companies is the work of AFCA, which has now been in existence for two years. As an 'authority' whose work could be extremely significant for some financial services firms and the industry more broadly, AFCA's workload is continuing to increase.

In the world of non-coronavirus related 'watch this space' developments, members of our excellent class actions team have prepared a report on the regulation of the newest fully-fledged members of the financial services industry – litigation funders. Further, criminal corporate misconduct law has now had the attention of the ALRC and we could see a shake-up in that space soon.

ASIC has not slowed its strong enforcement agenda this year and has run some important litigation, in some cases, to provide clarity in developing areas of law. One that should be of particular interest to financial services providers is ASIC's case, currently before the courts, against RI Advice Group for failing to have adequate cyber security systems. Dudley Kneller and Lisa Haywood take us through the implications of this case.

An area where ASIC litigation has provided clarity this year is unfair contract terms (likely in insurers' minds at the moment) in the Bendigo and Adelaide Bank case. There are ongoing obligations such as UCT compliance, of which it will be important not to lose sight once what could be a particularly busy year for financial services firms is upon us. For that reason, we have also included an update on ASIC's guidance on the still new whistleblowing regime.

While 2020 has been exhausting, 2021 is shaping up to be a particularly busy one for financial services regulation. We're looking forward to it!

Please get in touch if you have any feedback or would like any further information on any issues discussed in this edition or what you might like covered in future editions.

Edward Martin
Editor
+61 2 9163 3086
+61 404 565 139
edward.martin@gadens.com

In this issue

Click to jump to article

ASIC flexes its cyber security muscles – AFS Licence holders under the spotlight

Authors: Dudley Kneller, Partner and Lisa Haywood, Associate

The Australian Securities and Investment Commission (**ASIC**) has commenced landmark proceedings in the Federal Court against RI Advice Group Pty Ltd (**RI**), an Australian Financial Services Licence (**AFSL**) holder, for failing to have adequate cyber security systems in place and to comply with its obligations under the *Corporations Act 2001* (Cth) (**Act**).

ASIC's action comes after a number of alleged cyber breach incidents occurred at certain authorised representatives (**ARs**) of RI. While cyber security and cyber resilience has been a focus of ASIC and other regulators, this is the first time that ASIC has taken action of this nature.

The proceedings demonstrate ASIC's appetite to take action where it considers companies have failed to meet reasonable standards in managing cyber risks and provides a timely reminder for all AFSL holders to undertake a 'health check' on their current AFSL compliance framework to ensure they meet 'reasonable standards'.

Background

RI holds an AFSL and is a financial services licensee within the meaning of the Act. The AFSL requires RI to establish and maintain compliance measures that ensure, as far as is reasonably practicable, that RI complies with the provisions of the financial services laws.

RI had authorised individual and corporate representatives to provide financial services on its behalf (approximately 293 ARs as at 1 May 2020). RI's ARs received and stored, electronically, confidential and sensitive client information and documents, including relating to financial matters.

Landmark proceedings

Proceedings being brought by ASIC

Between 2016 and 2020, a number of RI's ARs experienced a range of cyber breach incidents. Some of the incidents identified by ASIC in the proceedings included:

a. ransomware attacks on their technology infrastructure;
b. local network hacking through a remote access port;
c. a malicious agent obtaining and retaining unauthorised remote access to a file server (for a period of more than 155 hours). This cyber breach incident resulted in a Notifiable Data Breach which was notified to the Office of the Australian Information Commission (**OAIC**); and
d. unauthorised email access.

According to ASIC, during the relevant period, RI failed to implement adequate and tailored cyber security documentation and controls, including cyber security risk management systems and resources with respect to ensuring appropriate levels of cyber security and cyber resilience.

ASIC alleges that as a result of RI's failure to have and to have implemented (including by its authorised representatives) policies, plans, procedures, strategies, standards, guidelines, frameworks, systems, resources and controls, which were reasonably appropriate to adequately manage risk in respect of cyber security and cyber resilience, RI failed to:

a. do all things necessary to ensure that the financial services covered by its licence are provided efficiently, honestly and fairly;
b. comply with the conditions of its licence requiring it to establish and maintain compliance measures to comply with financial services law;
c. comply with the financial services laws;
d. have available adequate resources (including financial, technological and human resources) to provide the services covered by the license and to carry out supervisory arrangements; and
e. failed to have adequate risk management systems,

and as a result it was in contravention of sections 912A(1)(a), (b), (c), (d) and (h) and (5A) of the Act.

Penalties being sought by ASIC

ASIC is seeking:

a. a declaration that RI contravened the Corporations Act (specifically the sections set out above);
b. orders that RI pay a civil penalty in an appropriate amount to be determined by the Court. The maximum pecuniary penalty being the greater of:
    i. 50,000 penalty units (offences committed between 1 July 2017 and 30 June 2020 have a penalty unit of $210 each being a maximum of $10.5 million);
    ii. three times the benefit obtained and detriment avoided; or
    iii. 10% of annual turnover, capped at 2.5 million penalty units;
c. compliance orders (including that within three months of the date of the orders, RI have implemented (including by its authorised representatives) policies, plans, procedures, strategies, standards, guidelines, frameworks, systems, resources and controls which are reasonably appropriate to adequately manage risk in respect of cyber security and cyber resilience; and
d. payment of ASIC's legal costs for bringing the proceedings.

This litigation takes place in a landscape of increased regulatory action and focus by different regulators in connection with cyber security and infrastructure. This case highlights the importance of implementing appropriate cyber security measures and responding/adapting appropriately when cyber security incidents do occur.

Key takeaways

All AFSL holders are strongly encouraged to undertake a review of their current risks and protection measures (including those of any authorised representatives) to ensure they comply with applicable law and meet reasonable standards for managing cyber security risks. What are appropriate and 'reasonable' standards for cyber security measures will depend on the organisation.

As a starting point, AFSL holders should:

- review their cyber security policies, plans, procedures, strategies, standards, guidelines, frameworks, systems, resources and controls and ensure they are appropriately tailored to their particular business (including for any authorised representatives);
- review the controls of any authorised representatives;
- establish and maintain controls designed to manage or mitigate those risks;
- if a cyber security incident occurs, within the organisation, or externally (e.g. at an authorised representative):
    - properly review the effectiveness of cyber security controls relevant to these incidents across their network, including account lockout policies for failed log-ins, password complexity, multi-factor authentication, port security, log monitoring of cyber security events, cyber training and awareness, email filtering, application whitelisting, privilege management and incident response controls; and
    - ensure controls are remedied internally and across any authorised representative network where necessary in a timely manner, in order to adequately manage risk with respect to cyber security and cyber resilience moving forward;
- ensure that all of the above comply with applicable law.

The proceedings demonstrate ASIC's willingness to take enforcement action against AFSL holders in relation to cyber security compliance. While it is arguable that this case may have presented 'low hanging fruit', it serves as a timely reminder that AFSL holders need to properly manage and ensure they implement and maintain effective cyber security controls within their organisation moving forward.

ASIC has provided some helpful resources for the purposes of cyber security and cyber resilience on its website.

Contents

One-stop-shop: The two year anniversary of AFCA – Australia's external dispute resolution authority

Author: Edward Martin, Partner

The Australian Financial Complaints Authority (**AFCA**) was born of the Ramsay Review in 2017 as part of a number of attempts to resist a financial services royal commission. Against some objections and over other potential external dispute resolution models, the Financial Services Ombudsman, Credit and Investments Ombudsman and Superannuation Complaints Tribunal were dissolved into AFCA to create a one-stop-shop for financial services complaints not resolved by a financial services company's internal dispute resolution processes.

It was to provide free, fast and binding dispute resolution, higher monetary limits and compensation caps (intended to allow more cases that would otherwise have gone to court to be heard by AFCA).

Importantly, however, AFCA is not a court or Tribunal (with a capital 'T') but an 'authority' with a wider role across the financial services sector. It is important for financial services providers to be cognisant of AFCA's operations and strategy when engaging with it.

The two year anniversary of when AFCA was established was on 1 November 2020 and AFCA released its FY20 Annual Review on 6 November 2020. It is reasonable to expect an increase in complaints given the economic pressures created by the coronavirus pandemic. Now is a good time to reflect on AFCA's operations, impact and how financial services firm engage with it.

Stats from the FY20 Annual Review

In its first full year of operation, AFCA received 80,546 complaints from consumers and small businesses (a 14% increase in the monthly average compared to the last financial year) with 58% of complaints being banking and finance related, 24% general insurance, 9% superannuation, 6% investments and advice and 2% life insurance.

It awarded or obtained **$258.6 million in compensation** or refunds to complainants.

It also identified and investigated 1,531 potential systemic issues and reported 92 definite systemic issues to regulators. AFCA delivered more than **$179 million in refunds** to consumers and small businesses following direct AFCA involvement in resolving systemic issues.

These are not insignificant outcomes and it is useful in the context of financial services regulation to consider how AFCA achieves them.

Financial services external dispute resolution body

AFCA's primary function is as a dispute resolution body – resolving customer complaints. It is a financial industry ombudsman service and it provides fair, free and independent solutions to financial disputes. Its website clarifies that:

"AFCA is not a government department or agency, and we are not a regulator of the financial services industry. We are a not-for-profit company, limited by guarantee that is governed by a Board of Directors, which includes equal numbers of industry and consumer representatives."

AFCA's complaint resolution powers are based in contract. AFCA's rules are approved by the Australian Investments and Securities Commission (**ASIC**), which together with AFCA's Constitution dated 1 March 2018 form part of a contract between AFCA and Financial Firms and Complainants. Membership of AFCA is a requirement of holding an Australian Financial Services Licence.

AFCA does not operate using a traditional judicial process and has been found by the Full Federal Court not to exercise judicial power. It has broad powers to make a decision and need only 'have regard to' legal principles when coming to a decision. Earlier this year, in Investors Exchange Limited, the Supreme Court of Queensland indicated in relation to AFCA's decisions:

"It is possible that, having had regard to legal principles, the decision-maker decides to not apply them because the strict application of those legal principles would lead to an outcome which is unfair in all the circumstances..." and

"An error in construing a document considered in the course of performing the task of arriving at an opinion as to what is fair in all the circumstances does not mean that the decision-maker misconceived the task that it was required to undertake or that the decision is not in accordance with the contract."

This provides AFCA with a great deal of flexibility in resolving complaints and it does so using an array of techniques ranging from negotiation to determination and at the speed appropriate to each case.

Financial Services Authority

AFCA's stated strategy is to be a world-class ombudsman service: raising standards and minimising disputes, meeting diverse community needs and trusted by all stakeholders. To achieve that goal, AFCA has wider functions beyond case-by-case independent dispute resolution.

Of particular note is AFCA's work around systemic issues. AFCA is required under the *Corporations Act 2001* (Cth) and ASIC's RG 267 Oversight of the Australian Financial Complaints Authority to *"Identify, refer and report systemic issues."* This involves investigating issues that affect more than one complainant, many similar complaints, all complainants at a particular firm or more than one firm. Potentially, that covers quite a lot of the complaints that AFCA handles.

Definite systemic issues are reported to ASIC, APRA or the ATO and the subject financial firm is identified to the regulator. In addition, AFCA's own systemic issues team seeks to work collaboratively with financial firms to resolve such issues, including the implementation by those firms of changes to their systems and processes to avoid the recurrence of the issues identified.

In a number of instances, AFCA has seen the implementation of significant remediation programs.

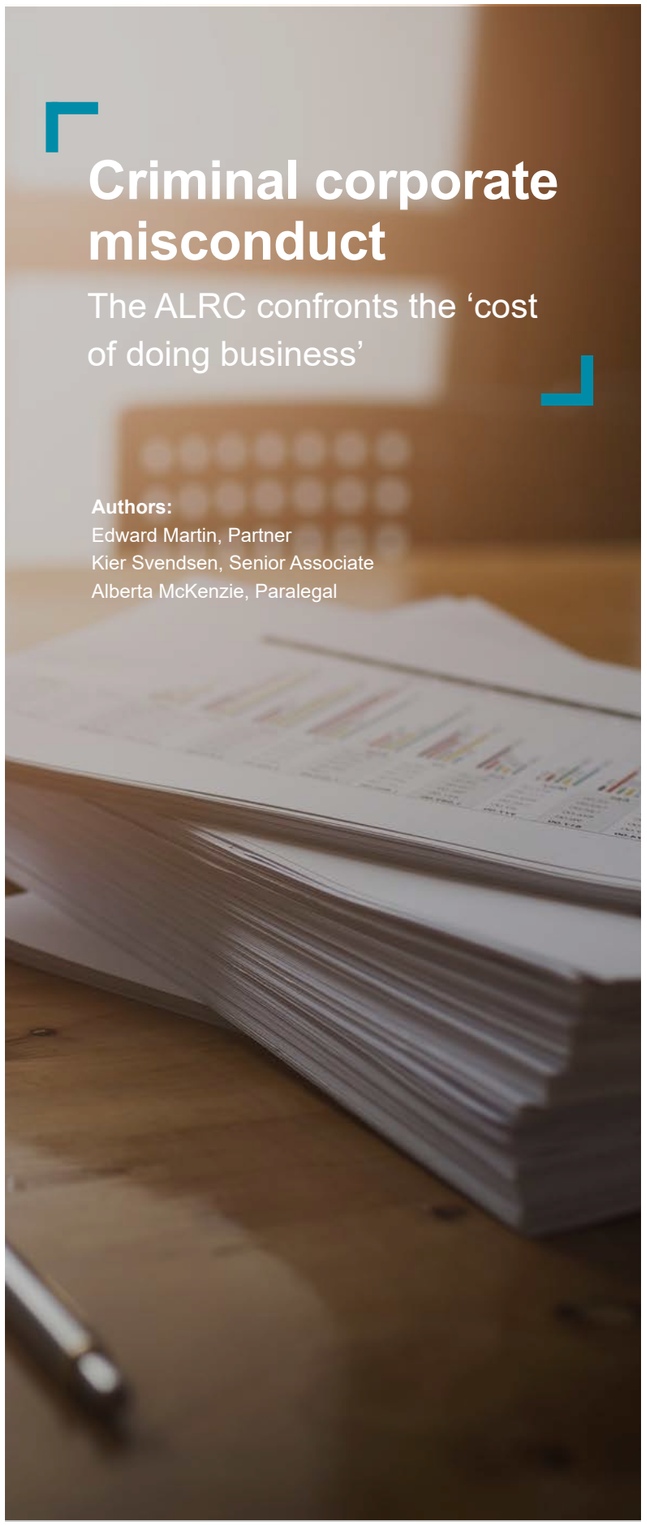
Conclusion

While AFCA was not conceived with the Financial Services Royal Commission's final report in mind, its current work (similar to the financial conduct regulators) is informed by Commissioner Hayne's findings, particularly as to past conduct in the financial services sector, and the implications of those findings on the industry.

It is unsurprising that AFCA is proving to be highly utilised and very active.

Its primary role as a dispute resolution body is only part of its story. Financial firms should not approach it as they would a court and should keep in mind AFCA's wider role, strategy and connection with the conduct regulators when engaging with it.

Contents



Criminal corporate misconduct

The ALRC confronts the ‘cost of doing business’

Authors:
Edward Martin, Partner
Kier Svendsen, Senior Associate
Alberta McKenzie, Paralegal

In February 2019 in the immediate aftermath of the Financial Services Royal Commission (**FSRC**), there were significant increases to penalties for corporate and financial sector misconduct, such as tripling the maximum prison term for serious offences to 15 years. Those measures sought to address widespread concerns that corporations, and their senior officers, were not being adequately held to account for serious misconduct.

The Australian Law Reform Commission (**ALRC**) has recently, however, put Australia’s corporate criminal liability regime under the microscope. Its final report, publicly released on 31 August 2020, set out 20 recommendations to improve and narrow the scope and prosecution of criminal corporate conduct.

The ALRC’s report is a set of proposed reforms for the Government’s consideration. The Government is yet to release any responsive paper to the report although the Attorney-General is considering it. Significant changes, which may increase risks of and around the prosecution of financial services firms may be on the cards and having an effective compliance function will be more important than ever.

Snapshot of the ALRC Report

- The ALRC’s overarching recommendations are that the laws governing corporate misconduct are too broad, criminal prosecutions are seldom brought and are not focused on the most egregious misconduct.
- The key takeaway is that criminal prosecutions should be reserved for the most egregious misconduct, and that the penalties for those offences ought to be strengthened.
- A significant constraint on the ALRC’s research was the ‘lack of complete, timely and accessible data relating to corporate crime in Australia’.
- The ALRC concluded that often the corporate response to dealing with civil or criminal actions is that it is merely ‘the cost of doing business’.
- Its recommendations are aimed at re-balancing what civil actions, and correspondingly, what criminal prosecutions should or should not be brought.

Financial services providers should be alive to an emerging legal landscape in which there is greater risk of being prosecuted and receiving significant punishment for serious corporate misconduct.

This article covers some of the ALRC’s most relevant recommendations and comments on how financial services providers can prepare in anticipation of any government response.

Significant recommendations

Prosecute only the most egregious cases

The ALRC’s recommendations are based on what it calls the ‘distinct purpose’ of corporate criminal responsibility – namely, it should be reserved for misconduct, which cannot be adequately regulated by civil penalties. The ALRC recommends that the de facto regulatory position should be – bring civil cases in the main; commence criminal prosecutions as the exception for serious and morally culpable misconduct.

The ALRC recommends quarantining the criminal law in that way to enhance the deterrent effect of those laws, and thus reduce what is often a blurred line between a civil action and a corporate criminal offence. A pragmatic example is the ALRC recommendation to abolish infringement notices as an enforcement response for criminal offences.

A single attribution of responsibility model

The ALRC says that the law is inconsistent on when a corporation will be held responsible, or ‘attributed’, for a crime (rather than individuals such as its directors or managers). It therefore recommends one streamlined method for determining whether corporate criminal liability should be imposed.

Broadly, it recommends that the new test should be whether the person in question was acting ‘on behalf of’ the corporation. This approach moves away from the current Criminal Code model, which typically attributes fault via a company’s board or a high managerial agent.

Under the ALRC’s proposed model, the physical element of the offence (that is, the act of doing or not doing something) will be satisfied if the agent[1] of the company (or any person acting with at least implied consent of the agent) was acting within actual or apparent authority of the company.

The mental element of the offence (that is, the intent to do or not do something) would be made out via one of two suggested recommendations – (1) removing the requirement for fault to be at a high managerial level so that more misconduct across the company’s operations could be captured, or (2) attributing fault through the state of mind of the relevant officers who engaged in the conduct.

Importantly, the ALRC proposes a new defence if the company took ‘reasonable precautions’ to prevent the misconduct. As referred to below, one of the guiding themes to arise from the ALRC’s report is the measures (or lack thereof) put in place by the company to prevent misconduct.

System of conduct offence

The ALRC recommends that a system of conduct or pattern of behaviour, which breaches or causes the contravention of two or more civil penalty provisions, be classified as a ‘system of conduct’ criminal offence. The offence asks whether the corporation intentionally or recklessly, by reference to their corporate behaviour, allowed a concerning system of conduct to continue unchecked.

These offences, according to the ALRC, would cover systematic and repeated instances of misconduct by corporations and, accordingly, target failures in the corporation’s systems, practices, procedures and policies.

This recommendation appears to target the misconduct that was the focus of the FSRC.

Risk management and next steps

The ALRC’s report contains a focus on ‘corporate culture’ when framing the approach to criminal conduct, and accordingly the defence of ‘reasonable precautions’ means that the systems, protocols and compliance measures that a company puts in place to prevent and manage corporate misconduct by its officers, will matter more than ever before. An effective compliance function could be the difference between severe criminal penalties and no penalties (or no prosecution).

[1] The reference to ‘agent’ is not exclusive, but used here for brevity.

Contents

The new focus on litigation funders:

Funding and Class Actions in Australia post the Parliamentary Inquiry

Authors:
Glenn McGowan QC, Partner
Rebecca Di Rago, Associate
Jonathon Ferraro, Lawyer

Litigation funders are the latest addition to the Australian financial services market. Before 2020, the question of whether they required an Australian Financial Services License (**AFSL**) had been resolved – they did not. Under the *Corporations Regulations 2001*, litigation funders were specifically exempted from the requirement to hold an AFSL and were not classed as managed investment schemes (**MIS**) or credit facilities.

However, on 24 July 2020, the *Corporations Amendment (Litigation Funding) Regulations 2020* were enacted to implement changes foreshadowed by the Federal Treasurer, including the requirement for litigation funders to hold an AFSL. Further changes are expected when the Parliamentary Joint Committee on Corporations and Financial Services inquiry into litigation funding and class actions hands down its final report in December 2020.

In this note, we set out the background to the changes and what we anticipate will be the likely impacts of the changes as litigation funders and ASIC adjust to the new regulatory requirements.

Litigation funders do not face the same regulatory scrutiny and accountability as other financial services and products under the Corporations Act. The removal of these exemptions will require litigation funders to obtain an Australian Financial Services License from the Australian Securities and Investments Commission.

Introduction

Following the announcement of the Parliamentary Joint Committee on Corporations and Financial Services inquiry into litigation funding earlier this year, the Federal Government has implemented a raft of new measures to regulate Australia's litigation funding and class action industry. Litigation funders will now be required to hold an AFSL and will be subject to the obligations imposed on financial services providers by the *Corporations Act 2001* (Cth) (**Corporations Act**).

Treasurer Josh Frydenberg has explained the rationale behind the changes:

"Litigation funders do not face the same regulatory scrutiny and accountability as other financial services and products under the Corporations Act. The removal of these exemptions will require litigation funders to obtain an Australian Financial Services License from the Australian Securities and Investments Commission. AFSL holders are obligated to:

- *act honestly, efficiently and fairly;*
- *maintain an appropriate level of competence to provide financial services; and*
- *have adequate organisational resources to provide the financial services covered by the licence.*

Removal of these exemptions will also require greater transparency around the operations of litigation funders in Australia."

In addition to being required to hold an AFSL, class actions will, unless exempt, be required to operate as a MIS and comply with the obligations of any ordinary MIS under the Corporations Act. As such, litigation funders will be required to, among other things:

a. be registered with ASIC and be operated by an Australian public company;

b. issue a product disclosure statement (**PDS**), together with a constitution and a compliance plan (all of which must be lodged with ASIC); and

c. hold adequate capital to manage their financial obligations, and audit compliance with such requirements annually or upon request by ASIC.

ASIC to oversee funders

Despite its initial resistance, ASIC has been appointed as the regulatory body with jurisdiction to monitor and enforce litigation funders' compliance with the new regime. ASIC has established the *ASIC Corporations (Litigation Funding Schemes) Instrument 2020/787* (commenced on 22 August 2020) (**Instrument**) to manage the transition to the new regulatory regime. The instrument includes relief from:

- the obligation to give a PDS to 'passive' members of open litigation funding schemes — on the condition the PDS is available on the scheme operator's website and referred to in advertising material;
- the obligation to regularly value scheme property;
- the statutory withdrawal procedures for members who withdraw from a class action under court rules; and
- the requirement to disclose detailed fees and costs information and information about labour standards or environmental, social or ethical considerations.

ASIC has also issued a 'no-action' position in relation to the obligation under Chapter 2C of the Corporations Act to establish and maintain a register of members of a registered litigation funding scheme. That is, ASIC will not take regulatory action if a funder of an open class action fails to comply with Chapter 2C.

ASIC's Deputy Chair Karen Chester has given some indication of the initial approach ASIC intends to take:

"As was contemplated in the Government's Explanatory Statement, ASIC has … concentrated on the relief required for Day 1 of the new regime. ASIC may provide additional relief or modify the relief we have made today as we and the litigation funding industry experience the new regulatory regime, and as the industry continues to evolve. ASIC will work to ensure that the Corporations Act operates effectively for litigation funding schemes."

ASIC will review the initial relief program in due course, after taking into account the Parliamentary Joint Committee Inquiry's final report into litigation funding and regulation of the class action industry, which is due to be published on 7 December 2020.

Implications for the class action landscape

As with any nascent regulatory regime, some of the practical implications of the new requirements are immediately apparent, such as the requirement to hold an AFSL and operate a litigation funding scheme as a MIS. The longer-term implications for the funding industry may take some time to manifest, as the sector recalibrates and ingests the full extent of changes to the operating environment.

We anticipate the following impacts are likely:

- operators of litigation funding schemes will be keen for guidance from ASIC in preparing their product disclosure statements, funding scheme constitutions, and compliance plans;
- imposing further red tape on litigation funders will see at least a temporary reduction in the number of funders operating in the Australian class action market;
- there will likely be a temporary pause on the number of new funded class actions being filed;
- there may be decreased interest from international funders entering the market other than the larger players;
- prospective litigants may need to wait until the 'dust settles' to access existing funding in the Australian market; and
- the increased costs of compliance may need to be passed on to group members, which may present a further disincentive for some group members to join a class action and shave margins which have, over the last five years, become increasingly narrow.

Given the new regulatory regime does not apply to litigation funding schemes entered into before 22 August 2020, it is unlikely there will be immediate impacts to existing funded actions.

Conclusion

The new regulatory regime is primarily aimed at strengthening protections for public companies from the increasing risk posed by class actions. So much is apparent from the Treasurer's remark:

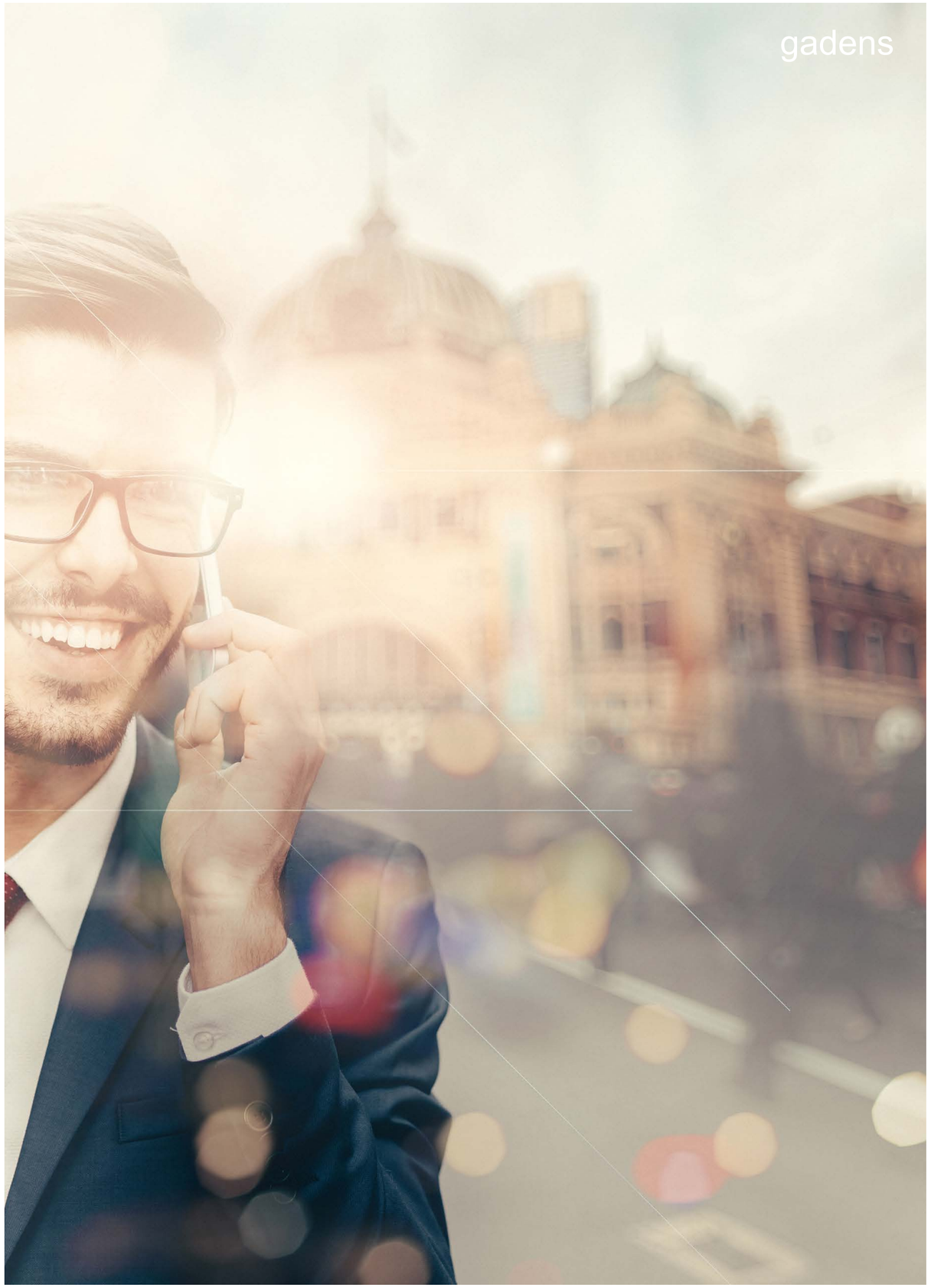
"We want Australian businesses staying in business, and focused on keeping people in jobs, rather than fending off class actions funded by unregulated and unaccountable parties."

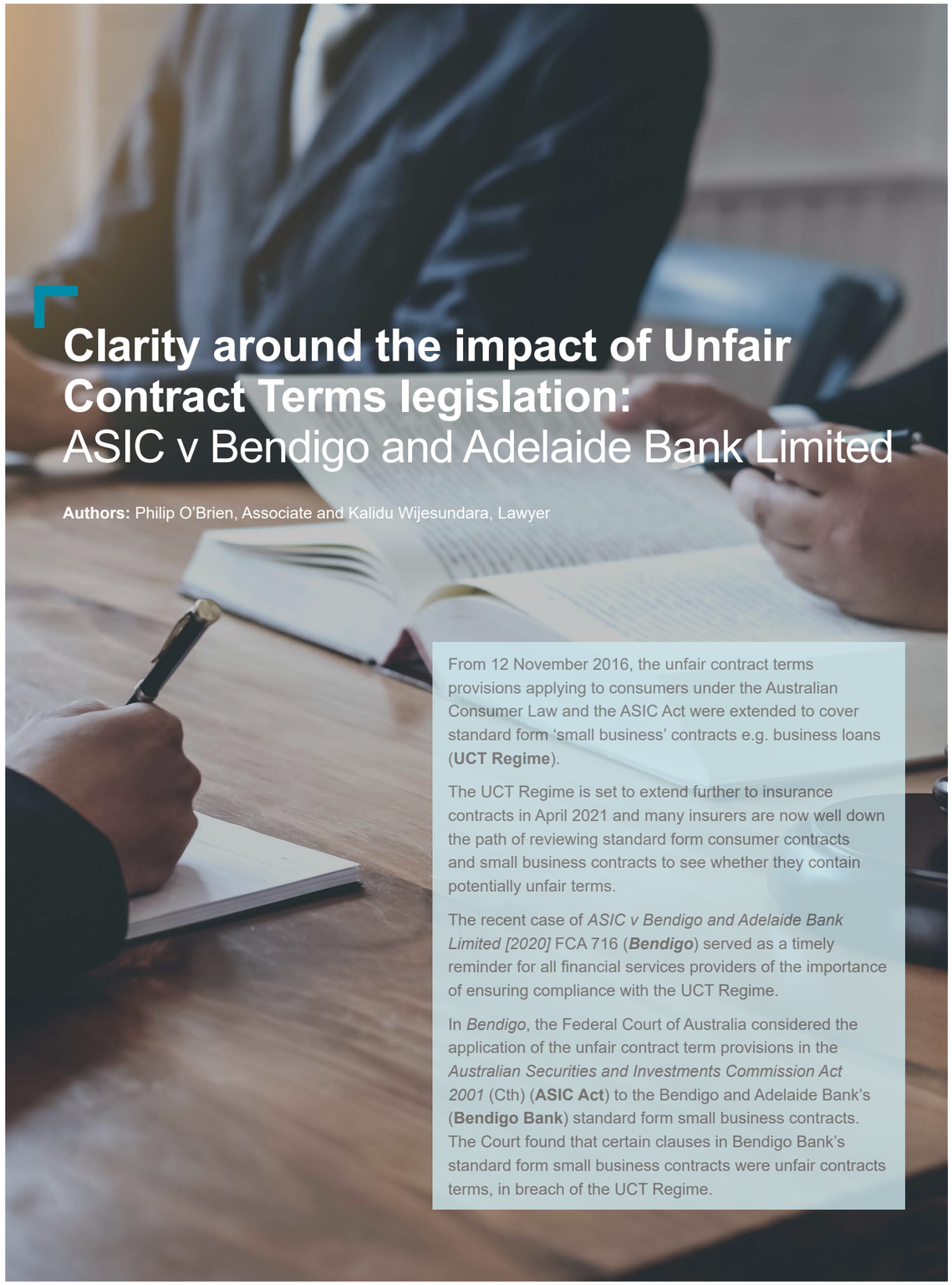
Recent market activity, or the lack thereof, indicates that the changes have gone some way to constricting the present operations of funders. A significant decrease in class actions in 2020 suggests that funders are exercising greater caution when contemplating funding actions, though this could potentially also be attributed in part to the current moratorium on actions for breaches of continuous disclosure obligations under the *Corporations (Coronavirus Economic Response) Determination (No. 4) 2020*.

It is anticipated that additional regulations will be introduced following the delivery of the Parliamentary Committee's report and recommendations on 7 December 2020.

While there remains considerable uncertainty around the long-term impact of the suite of reforms, company boards can take some comfort from the prospect of reduced class action activity as a result of increased regulatory oversight of litigation funders.

Contents





Clarity around the impact of Unfair Contract Terms legislation: ASIC v Bendigo and Adelaide Bank Limited

Authors: Philip O'Brien, Associate and Kalidu Wijesundara, Lawyer

From 12 November 2016, the unfair contract terms provisions applying to consumers under the Australian Consumer Law and the ASIC Act were extended to cover standard form 'small business' contracts e.g. business loans (**UCT Regime**).

The UCT Regime is set to extend further to insurance contracts in April 2021 and many insurers are now well down the path of reviewing standard form consumer contracts and small business contracts to see whether they contain potentially unfair terms.

The recent case of *ASIC v Bendigo and Adelaide Bank Limited [2020]* FCA 716 (***Bendigo***) served as a timely reminder for all financial services providers of the importance of ensuring compliance with the UCT Regime.

In *Bendigo*, the Federal Court of Australia considered the application of the unfair contract term provisions in the *Australian Securities and Investments Commission Act 2001* (Cth) (**ASIC Act**) to the Bendigo and Adelaide Bank's (**Bendigo Bank**) standard form small business contracts. The Court found that certain clauses in Bendigo Bank's standard form small business contracts were unfair contracts terms, in breach of the UCT Regime.

Overview of UCT Regime

Under s12BF of the ASIC Act, a contract is a 'small business contract' where:

- at the time the contract is entered into, at least one party to the contract is a business that employs fewer than 20 persons; and
- the upfront price payable under the contract does not exceed $300,000, or $1 million if the contract is for more than 12 months.

For the UCT Regime to apply, the small business contract must also be a 'standard form contract' for a financial product or the provision of financial services, such as business loans, credit cards and overdraft arrangements.

Financial services providers should note that a small business contract is presumed to be a standard form contract unless the financial services provider proves otherwise (s12BK of the ASIC Act).

Section 12BF(1) of the ASIC Act provides that a term in a standard form small business contract for a financial product or service is **void** if the term is 'unfair'.

What is an 'unfair' contract term?

Section 12BG of the ASIC Act defines the term 'unfair'. A term in a contract is 'unfair' if:

- it would cause a significant imbalance in the parties' rights and obligations arising under the contract;
- it is not reasonably necessary to protect the legitimate interests of the party who would be advantaged by the term; and
- it would cause financial or other detriment to a party if it were to be applied or relied on.

The court can take into account any matter it thinks relevant in determining whether a term in a contract is unfair. However, the court must take into account the transparency of the term and the contract as whole.

Pursuant to sections 12BF and 12GND of the ASIC Act, if the court determines that a term in a standard form contract is unfair, it makes a declaration to that effect and declares the term void (i.e. as if it never existed). The remainder of the contract will continue to operate between the parties if the contract can operate without the unfair term.

The *Bendigo* case

The Court in *Bendigo* declared several terms within six standard form small business contracts used by Bendigo Bank to be unfair and void from the outset. ASIC was also successful in obtaining a declaration that applies to those same terms where they appear in any other standard form small business contract used by any financial services provider.

In doing so, ASIC and the court have made it clear that financial institutions should pay particular attention to the following.

Indemnity clauses

The indemnity clauses required the small business customer to compensate Bendigo Bank for any liability incurred by the bank in relation to circumstances that were not of material risk to the bank, not within the customer's control, and could have been mitigated by the bank.

- The Court held that the indemnity clauses were unfair because the bank could hold the customer liable for loss or costs incurred by the bank that the customer did not cause, or where the loss was caused by the bank's mistake, error or negligence, or the loss could have been avoided or mitigated by the bank. This satisfied the 'detriment' requirement in section 12BG(1)(c) of the ASIC Act.
- The Court also held the clauses created a significant imbalance in the parties' rights and obligations, in breach of section 12BG(1)(a) of the ASIC Act as, amongst other things, the customer did not have any corresponding rights under the contract.

Event of default clauses

The impugned Bendigo Bank default clauses included terms which:

- created a default event arising from matters that did not involve any credit risk to the bank (e.g. where a customer makes an untrue or misleading statement which is not material to the contract);
- allowed the bank to take disproportionate enforcement action (e.g. the bank could cancel a loan facility even if the customer was meeting all obligations and making timely repayments);
- did not allow the customer an opportunity to remedy the default; and
- were based on the bank forming a unilateral opinion on the matter and expressed in vague and largely undefined circumstances.

The Court held that the clauses were unfair as they created a significant imbalance in the rights and obligations of the parties that would cause detriment to the customer.

Unilateral variation or termination clauses

Unilateral termination and variation clauses were held to be unfair and void. The clauses caused a significant imbalance in the parties' rights and obligations as they entitled Bendigo Bank unilaterally to:

- vary the financial services and reduce the amount of funds available to the customer;
- vary terms of the contract at will; and

- terminate the contract if the customer did not accept any proposed new terms, or alternatively charge fees if the customer elected to terminate.

The Court was satisfied that these terms, together with the lack of any corresponding rights afforded to the customer under the contract, caused detriment to the customer and breached the UCT Regime.

Conclusive evidence clauses

The conclusive evidence clauses in Bendigo Bank's contracts provided that the bank's certificate would be conclusive proof of any amount owed by the customer unless the customer proved otherwise.

The clauses created a significant imbalance and caused detriment because the bank was permitted, by issuing a certificate, to impose an evidential burden on the customer to disprove matters about which the bank was best placed to provide primary evidence. As a result, the Court found that these clauses also breached the UCT Regime.

Key takeaways

The use of the same terms in any future small business contracts by Bendigo Bank or any other financial services provider is prohibited.

Financial institutions' contracts are critical to their proper risk management. Including and intending to rely on clauses that do not comply with the UCT Regime creates significant risk and unnecessary exposure for such institutions.

Financial services providers who get their UCT Regime compliance wrong will likely be required to expend considerable internal time and resources addressing UCT issues. Prevention will almost certainly be better than cure when it comes to UCT Regime compliance.

Insurers in particular can learn from the Bendigo case and consider:

- undertaking a comprehensive review of all standard form small business contracts (particularly by reference to the terms addressed above); and
- where any potentially problematic terms are detected in existing contracts with customers, seeking the customers' written consent to vary those terms to ensure compliance.

A Refresher on Australia's Whistleblower Laws: What do Company Officers, Senior Managers and Auditors need to know?

Authors:
Nicholas McKenzie-McHarg, Partner, Stephanie Rawlinson, Associate and Katie White, Lawyer

Following the significant changes to Australia's whistleblowing regime last year with the passing of the *Treasury Laws Amendment (Enhancing Whistleblower Protections) Act 2019* (**Whistleblower Regime**), earlier this year the Australian Securities and Investments Commission (**ASIC**) released a series of information sheets to help company officers, senior managers and company auditors better understand and comply with their respective obligations under the new corporate whistleblower protection regime.

In the wake of the Financial Services Royal Commission, financial services companies must be completely conversant with Whistleblower Regime and requirements if a whistleblower comes forward. This article provides a recap of the Whistleblower Regime, and summarises the key takeaway points from the information sheets released by ASIC earlier this year.

Key takeaways

- ASIC's information sheets are a useful reminder of the significance of the protection of the whistleblower's identity and the victimisation provisions of the new Whistleblower Regime.
- A year on from introduction of the Whistleblower Regime, it is worth revisiting Whistleblower Policies and training, particularly by reference to ASIC's guidance.
- A key legal objective of the Whistleblower Regime is to ensure the protection of whistleblowers who come forward with information that contains a "qualifying disclosure".
- Maintaining anonymity and confidentiality of the whistleblower is paramount without express consent from the whistleblower to disclose their identity. In order to avoid penalties under the Whistleblower Regime, persons receiving a disclosure should assume that the whistleblower wants to remain anonymous.

Contents

Australia's Whistleblower Regime

The Whistleblower Regime, now Part 9.4AAA of the *Corporations Act 2001* (**Act**), aimed to strengthen existing protections offered to whistleblowers who come forward with their concerns of misconduct in the corporate and financial sectors.

For a disclosure of information to be afforded protection under the Act, it is required to have been made by an 'eligible whistleblower', which includes past or present officers, employees, contractors, suppliers and individual associates of the regulated entity (or a related entity), as well as their current or former relatives or dependents (including spouses)[1].

The disclosure of information must also be received by ASIC, APRA, a prescribed Commonwealth authority such as the Australian Taxation Office, or an 'eligible recipient' as defined by section 1317AAC of the Act.

Notably, an eligible recipient includes:

- **company officers**, including a director or company secretary;
- **senior managers**, being persons other than directors or company secretaries who make or participate in decision making that affects the whole, or a substantial part of, the business of the company or organisation, or has the capacity to significantly affect the company or organisation's financial standing (for example, a CEO); and
- **auditors**, or a member of an audit team conducting an audit of the company, (including both internal and external auditors).

Identifying 'Qualifying Disclosures'

As eligible recipients, company officers, senior managers and auditors must be able to identify the type of disclosure of information that has been made to them, as not all complaints amount to a disclosure worthy of protection under the Act.

The eligible whistleblower's disclosure must meet certain criteria in order to be considered a 'qualifying disclosure', and to be afforded the necessary protection under the regime.

A qualifying disclosure is information that an eligible whistleblower 'has reasonable grounds to suspect' concerns:

- misconduct (including fraudulent behaviour, negligence default, breach of trust and breach of duty[2]);
- an improper state of affairs or circumstances;
- conduct that represents a danger to the public or the financial system; or
- a contravention of any laws.

Prior to the current Whistleblower Regime, it was necessary for a disclosure of information to have been made in 'good faith' in order to amount to a qualifying disclosure. Now, the motivation of the eligible whistleblower is irrelevant, and an eligible whistleblower needs only to have a 'reasonable ground to suspect' that the information concerns at least one of the factors listed above.

For a company officer, senior manager or auditor, the information disclosed must be about the entity that is the subject of audit, an officer or employee of that entity, a related entity, or an officer or employee of the related entity.

Importantly, the whistleblower provisions do not cover disclosures that relate exclusively to a 'personal work-related grievance' unless:

- the person suffers, or is threatened with, detriment for making the disclosure;
- the disclosure includes information about misconduct, an improper state of affairs or; circumstances, a breach of the law, or danger to the public or the financial system, in addition to the personal work-related grievance; or
- the disclosure suggests misconduct that has significant implications for the company beyond the discloser's personal circumstances.

Protecting the Identity of the Whistleblower

One of the key legal obligations for company officers, senior managers and auditors is to protect the eligible whistleblower's identity.

It is important that whistleblowers are made aware that they do not have to provide their name or contact details when making a disclosure, and can choose to remain anonymous. However, organisations must ensure appropriate measures are in place within the organisation so as to safeguard against any breach of disclosure of confidential information.

It is a criminal and civil offence if an eligible recipient makes an unauthorised disclosure of the whistleblower's identity, or discloses information that is likely to lead to their identification, gained directly or indirectly from the whistleblower's qualifying disclosure[3]. Disclosing a whistleblower's identity without their consent could result in a fine of up to $1,050,000 for an individual and up to $10,500,000 for a company.

In addition, a company may be liable to compensate a whistleblower if they suffer loss, damage or injury caused by the 'detrimental conduct' of a person within the company who made their report. 'Detrimental conduct' can include damage to the whistleblower's reputation, which could result from a breach of their confidentiality.

To the extent that is possible and appropriate, it may be prudent for organisations to consider seeking a whistleblower's consent to make any necessary disclosures of their identity.

When is a disclosure of the Whistleblower's identity allowed?

The eligible whistleblower's identity or confidential information may be lawfully disclosed in the following circumstances:

- if the whistleblower consents;
- if disclosure is made to ASIC, APRA or the Australian Federal Police; or
- to a legal practitioner in the course of obtaining advice about the whistleblower provisions.

Further, an auditor may be unable to disclose the whistleblower's details to their audit partner, other members of the audit team or other eligible recipients.

Section 1317AAE(1) of the Act also provides an exception known as the 'investigation defence', which may be relied upon by a company or auditor if the whistleblower's confidential information has been compromised during the investigation into their complaint. It may only be relied upon where:

- the information does not disclose the whistleblower's identity specifically but rather, information that may lead to their identification;
- the disclosure is 'reasonably necessary' for investigating the whistleblower's concerns; and
- 'all reasonable steps' have been taken to reduce the risk that the whistleblower will be identified as a result of the disclosure.

Protecting the Whistleblower from Victimisation or Detriment

Company officers, senior managers and auditors must not cause or threaten to cause detriment to (or victimise) a whistleblower for making their disclosure of information.

Detriment includes actions or other conduct against a whistleblower or potential whistleblower to:

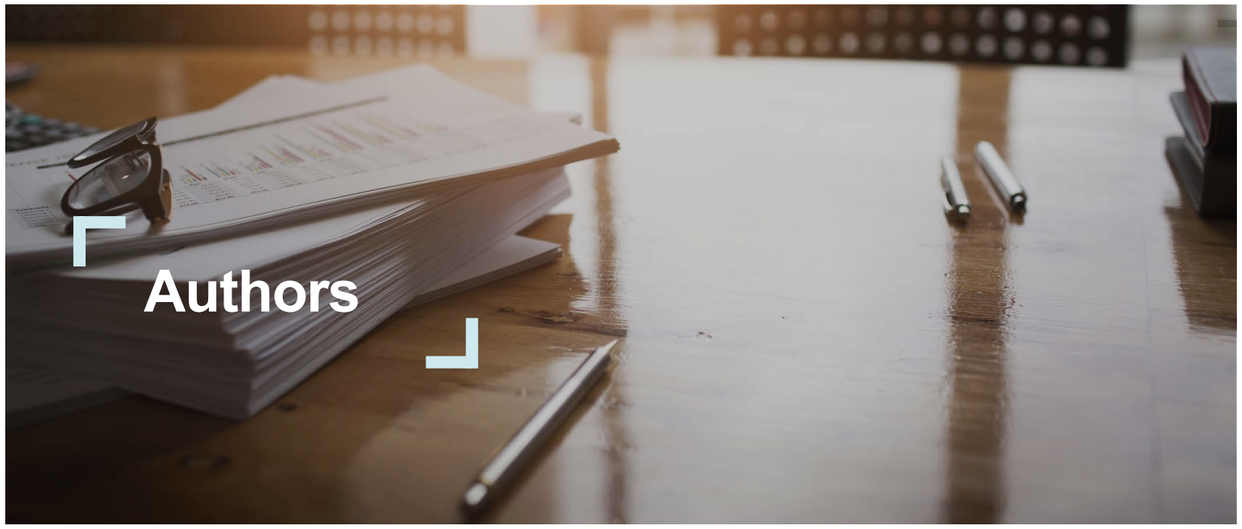
- dismiss them from their employment;
- injure them in their employment;
- alter their position or duties as an employee to their disadvantage;
- discriminate between them as an employee and other employees of the same employer;
- harass or intimidate them;
- harm or injure them, including causing them psychological harm;
- damage their property;
- damage their reputation;
- damage their business or financial position; or
- cause them any other damage.

Managing Compliance

Most financial services firms will have whistleblower policies in place by now (if not this should be a priority as it is a legislative requirement). However, the emerging ASIC guidance shows that it is important to keep the policy under review and ensure that it is ready to operate seamlessly if a whistleblower comes forward.

[1] s 1317AAA, *Corporations Act*, s 14ZZU *Taxation Administration Act*
[2] s 9, *Corporations Act*
[3] s 1317AAE, *Corporations Act*

Contents



Authors

Dudley Kneller
Partner
+61 3 9252 7748
+61 438 363 443
dudley.kneller@gadens.com

Glenn McGowan QC
Partner
+61 3 9252 2587
+61 412 263 691
glenn.mcgowan@gadens.com

Kier Svendsen
Senior Associate
+61 3 9252 2588
kier.svendsen@gadens.com

Philip O'Brien
Associate
+61 3 9252 2549
philip.obrien@gadens.com

Stephanie Rawlinson
Associate
+61 3 9612 8363
stephanie.rawlinson@gadens.com

Edward Martin
Partner
+61 2 9163 3086
+61 404 565 139
edward.martin@gadens.com

Nicholas McKenzie-McHarg
Partner
+61 3 9252 2535
+61 410 602 263
nick.mcharg@gadens.com

Lisa Haywood
Associate
+61 3 9252 7798
lisa.haywood@gadens.com

Rebecca Di Rago
Associate
+61 3 9252 7710
rebecca.dirago@gadens.com

With special thanks to our other contributors:

Jonathon Ferraro, Lawyer
Kalidu Wijesundara, Lawyer
Katie White, Lawyer
Alberta McKenzie, Paralegal

Design: Pamela Orola, Business Development & Marketing

gadens

Adelaide
Level 1
333 King William Street
Adelaide SA 5000
T + 61 7 3231 1666

Brisbane
Level 11, ONE ONE ONE
111 Eagle Street
Brisbane QLD 4000
T + 61 7 3231 1666

Melbourne
Level 13, Collins Arch
447 Collins Street
Melbourne VIC 3000
T + 61 3 9252 2555

Perth (Lavan)
Level 20, The Quadrant
1 William Street
Perth WA 6000
T +61 8 9288 6000

Sydney
Level 20, MLC Centre
19 Martin Place
Sydney NSW 2000
T +61 2 9231 4996

gadens.com

Gadens is an association of independent firms.