Financial Services Newsletter

2020 . Vol 19 No 6

Contents

Information contained in this newsletter is current as at September 2020

LexisNexis® Butterworths

General Editor's note

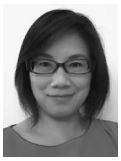
Karen Lee *LEGAL KNOW-HOW*

What do Australia's Privacy Act 1988, the European Union's General Data Protection Regulation, and the United States' California Consumer Privacy Act of 2018 have in common? These are examples of data protection legislation financial services lawyers' clients may be subject to. Over a series of articles, **Frank Downes** (Juris IT Services) gives us an overview of these and other legislative and regulatory frameworks that are relevant to financial institutions and financial firms. To kick off the series, Frank covers the key ones in the region of Asia, including Australia and the Pacific.

In recent times, we have seen regulators place more focus on cyber resilience. For example, not so long ago in December 2019, the Australian Securities and Investments Commission (ASIC) released Report 651 regarding cyber resilience of firms in Australia's financial markets.[1] This trend seems to be continuing. In August 2020, ASIC alleges that financial services licensee RI Advice Group Pty Ltd failed to implement adequate policies, systems and resources that were reasonably appropriate to manage risk in respect of cybersecurity and cyber resilience. This is one of the first times that ASIC has taken this type of enforcement action. **Alasdair McLean** and **Oscar Ruane** (Piper Alderman) walk us through the regulator's allegations and the declarations it is seeking, and importantly, provide some practical tips so financial services licensees and their advisors can better manage the compliance risks.

What do you know about litigation funding regulation? You may be aware that the government announced on 22 May 2020 that it would regulate litigation funders under the Corporations Act 2001 (Cth). From 22 August 2020, operators of litigation funding schemes are required to hold a financial services licence, and litigation funding schemes are generally subject to the managed investment scheme (MIS) regime in Ch 5C of the Corporations Act. On 21 August 2020, ASIC made the ASIC Corporations (Litigation Funding Schemes) Instrument 2020/787 to manage the transition to the new litigation funding regime. In their article, "More questions than answers: Treasury releases litigation funding regulations ahead of 22 August deadline", editorial board member **Andrea Beatty**, **Chelsea Payne** and **Chloe Kim** (Piper Alderman) take a look at the new regime, including the litigation funding schemes that are exempted from having to register as an MIS and from obtaining a financial services licence, and ASIC's relief announced on 21 August 2020.

Enjoy the issue. If you have any suggestions for topics you would like us to cover, please feel free to get in touch with me.



Karen Lee
Principal
Legal Know-How
karen.lee@LegalKnowHow.com.au

Karen Lee is the General Editor of the Australian Banking & Finance Law Bulletin and the Financial Services Newsletter. She also partners LexisNexis in other capacities, including as Specialist Editor for precedents in banking and finance, mortgages and options, and as contributing author of a number of other publications, including Australian Corporate Finance Law, Halsbury's Laws of Australia and Practice Guidance for General Counsel. Karen established her legal consulting practice, Legal Know-How, in 2012. She provides expert advice to firms and businesses on risk management, legal and business process improvement, legal documentation, regulatory compliance and knowledge management. Prior to this, Karen worked extensively in-house, including as Head of Legal for a leading Australasian non-bank lender, as well as in top-tier private practice, including as Counsel at Allen & Overy and Clayton Utz.

Footnotes

1. Australian Securities and Investments Commission *Cyber Resilience of Firms in Australia's Financial Markets: 2018–19* Report 651 (December 2019) https://download.asic.gov.au/media/5416529/rep651-published-18-december-2019.pdf.

Overview of Regional Data Protection Regulations — what financial services lawyers need to know

Frank Downes *JURIS IT SERVICES*

This series will review some of the legislative and regulatory frameworks that clients of financial services lawyers may be subject to under national, regional and industry-specific regulations governing the collection and use of personal information and data. Particular attention will be paid to regulations that could impact cloud service providers (CSPs). This month we will cover frameworks originating in the Asian region, including Australia and the Pacific area. Regulations that are considered global will be the subject of a separate article. This overview is focused on the compliance requirements for the financial services sector and should not be considered exhaustive.

Australia

Australian Prudential Regulation Authority

The Australian Prudential Regulation Authority (APRA) oversees banks, credit unions, insurance companies, and other financial services institutions in Australia. Regulated entities must implement cloud-data strategy with effective governance, thorough risk assessment and regular assurance processes.

Regulated institutions must comply with the APRA *Prudential Standard CPS 231: Outsourcing*[1] when outsourcing a material business activity — any activity that has the potential, if disrupted, to have a significant impact on the financial institution's business operations or ability to manage its risks effectively.

Detailed guidance on utilising cloud computing services can be found in APRA's information paper, *Outsourcing Involving Cloud Computing Services*.[2] This paper will help regulated entities assess cloud providers and services more effectively and guide them through the regulatory issues of outsourcing to the cloud.

When outsourcing, including to a cloud service, regulated institutions must also review and consider their ongoing compliance with APRA *Prudential Standard CPS 234: Information Security*.[3]

Information Security Registered Assessors Program

The Information Security Registered Assessors Program (IRAP) provides a comprehensive process for the independent assessment of information and communications technology (ICT) security against Australian Government policies and guidelines. The assessment will suggest mitigations and highlight residual risks. The IRAP goal is to maximise the security of Australian federal, state and local government data by focusing on the ICT infrastructure that stores, processes and communicates it. The IRAP is governed and administered by the Australian Cyber Security Centre (ACSC).

Certified Cloud Services List

The Certified Cloud Services List (CCSL) identifies cloud services that have successfully completed an IRAP assessment by the Australian Government, and have been awarded certification by the ACSC.

The certification recognises the successful completion, review and acceptance of a comprehensive assessment undertaken by an information security registered assessor, so all Australian Government agencies can use it. The CCSL can also be referenced by the New Zealand Government organisations in conducting their risk assessments as the New Zealand Information Security Manual and the Australian Government Information Security Manual are aligned.

New Zealand

Cloud computing security and privacy considerations

The "cloud computing security and privacy considerations" is a whole-of-government ICT strategy that reaffirmed its "cloud first" policy on using IT across the public sector. The revised strategy retains the "Cloud Computing Risk and Assurance Framework" that was developed and implemented under the authority of the New Zealand Government Chief Information Officer (GCIO).

The government expects all New Zealand State Services agencies to work within this framework when assessing and adopting cloud services. Cloud services requirements outline what agencies must do when adopting cloud services along with an overview of the history of the government's cloud policy.

To assist New Zealand Government agencies in conducting consistent and robust due diligence on potential cloud solutions, the GCIO has published *Cloud Computing: Information Security and Privacy Considerations*[4] (the Cloud Computing ISPC). This document contains more than 100 questions focused on data sovereignty, privacy, security, governance, confidentiality, data integrity, availability, and incident response and management. Note that "Cloud Computing ISPC" does not define a New Zealand Government standard against which CSPs must demonstrate formal compliance.

Singapore

Multi-Tier Cloud Security Standard

The Multi-Tier Cloud Security Standard for Singapore (MTCS) was prepared under the direction of the Information Technology Standards Committee (ITSC) of the Infocomm Media Development Authority of Singapore (IMDA). The ITSC promotes and facilitates national programs to standardise IT and communications, and Singapore's participation in international standardisation activities.

The MTCS provides a common standard that CSPs can apply to address customer concerns about the security and confidentiality of data in the cloud, and the impact on businesses of using cloud services. MTCS is the first cloud security standard with different levels of security, so certified CSPs can specify which levels they offer.

The MTCS builds upon recognised international standards such as ISO/IEC 27001: Information Security Management, and covers such areas as data retention, data sovereignty, data portability, liability, availability, business continuity, disaster recovery and incident management. It also includes a mechanism for customers to benchmark and rank the capabilities of CSPs against a set of minimum baseline security requirements.

Monetary Authority of Singapore

In July 2016, the Monetary Authority of Singapore (MAS), the sole bank regulator in Singapore and its central bank, issued its *Guidelines on Outsourcing*.[5] In the Guidelines, the MAS set out its expectations for outsourcing cloud services by financial institutions in Singapore, including banks, insurance companies and trust companies.

The MAS Guidelines substantially streamline the process for technology adoption, provide clarity on the regulator's expectations and address many of the misconceptions that had previously slowed the financial industry's adoption of cloud solutions.

In contrast to the APRA regulations, there is no notification requirement for any significant material outsourcing commitments. Instead, MAS-regulated institutions are expected to refine their risk-based approach when assessing material outsourcing and conduct a self-assessment of all outsourcing arrangements against these guidelines.

Association of Banks in Singapore

Shortly after the release of the MAS Guidelines, the Association of Banks in Singapore, a non-profit organisation representing the interests of local and foreign banks operating in Singapore (but not other financial institutions), introduced a non-binding practical guide, *ABS Cloud Computing Implementation Guide 2.0 for the Financial Industry in Singapore*.[6] It is designed to help banks implement outsourcing arrangements following the MAS Guidelines.

South Korea

Korea-Information Security Management System

The Korea-Information Security Management System[7] (K-ISMS) is a country-specific ISMS framework, which defines a stringent set of control requirements designed to help ensure that organisations in South Korea consistently and securely protect their information assets.

To obtain the certification, a company must undergo an assessment by an independent auditor that covers both information security management and security countermeasures.

The K-ISMS framework is built on successful information security strategies and policies, as well as security countermeasures and threat response procedures to minimise the impact of any security breaches.

Next month we will continue our review covering China, Japan and India.

Frank Downes
CEO
Juris IT Services
frankd@jurisit.com.au
www.jurisit.com.au

About the author
Frank Downes is the CEO of Juris IT, an IT services company that assists organisation with information security and successfully implementing, securing and maintaining remote work environments.

Disclaimer: *This document is part of our commitment to assist lawyers understand the information technologies that will impact them and their clients. It is not legal or regulatory advice and it does not constitute any warranty or contractual commitment on our part. If you have any questions, please contact us.*

Footnotes

1. Australian Prudential Regulation Authority (APRA) *Prudential Standard CPS 231: Outsourcing* (July 2017) www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf.
2. APRA *Outsourcing Involving Cloud Computing Services* Information Paper (24 September 2018) www.apra.gov.au/sites/default/files/information_paper_-_outsourcing_involving_cloud_computing_services.pdf.
3. APRA *Prudential Standard CPS 234: Information Security* (July 2019) www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf.
4. New Zealand Government *Cloud Computing: Information Security and Privacy Considerations* (April 2014) www.digital.govt.nz/assets/Documents/1Cloud-Computing-Information-Security-and-Privacy-Considerations-FINAL2.pdf.
5. Monetary Authority of Singapore *Guidelines on Outsourcing* (27 July 2016) www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/ Outsourcing%20Guidelines_Jul%202016.pdf.
6. This is an updated version of the initial release in June 2016: Association of Banks in Singapore *ABS Cloud Computing Implementation Guide 2.0 for the Financial Industry in Singapore* (2019) https://abs.org.sg/docs/library/abs-cloud-computing-implementation-guide.pdf.
7. Korea Internet & Security Agency, System Introduction, https://isms.kisa.or.kr/main/isms/intro/.

ASIC cybersecurity enforcement action against an AFSL holder

Alasdair McLean *and* ***Oscar Ruane*** *PIPER ALDERMAN*

Introduction

On 21 August 2020, the Australian Securities and Investments Commission (ASIC) announced that it was commencing Federal Court proceedings against RI Advice Group Pty Ltd (RI), an Australian Financial Services Licence (AFSL) holder, in respect of alleged breaches of the Corporations Act 2001 (Cth) by failing to have adequate cybersecurity systems.[1] This is one of the first times that ASIC has taken this type of action and it is a clear sign of the regulator's increased focus on cybersecurity and cyber resilience. It is a timely reminder of the broad scope of obligations that are imposed on licensed entities and the increasing need to actively engage in cybersecurity risks as part of an AFSL holder's compliance framework.

What are the allegations?

ASIC's action follows a number of alleged cyber breach incidents by certain authorised representatives of RI, including an alleged cyber breach incident at Frontier Financial Group Pty Ltd as trustee for The Frontier Trust (Frontier) over a 6-month period in late 2017 to early 2018. One of ASIC's allegations is that Frontier was subject to a "brute force" attack that resulted in an unauthorised user gaining remote access to Frontier's database of sensitive client information for more than 155 hours.

After becoming aware of the breach at Frontier, and with knowledge of other cybersecurity incidents within its authorised representative network, ASIC alleges that RI contravened key provisions of the Corporations Act by failing to maintain adequate policies, systems and resources to manage risk in respect of cybersecurity and cyber resilience. These obligations arise as part of the requirements under the Corporations Act that an AFSL holder:

- does all things necessary to ensure that the financial services covered by its licence are provided efficiently, honestly and fairly
- complies with the financial services laws
- takes reasonable steps to ensure that its authorised representatives comply with the financial services laws
- has adequate resources (including financial, technological and human resources) to provide the financial services covered by its licence and to adequately supervise the arrangements in place and
- puts in place adequate risk management systems

What is ASIC seeking?

ASIC is seeking declarations that RI contravened various provisions of the Corporations Act, pecuniary penalty orders and compliance orders that RI implements systems that are reasonably appropriate to adequately manage risk in respect of cybersecurity and cyber resilience (which ASIC is seeking to have confirmed by an independent expert report once implemented).

Practical tips for AFSL holders to manage compliance risks

It is recommended that all AFSL holders undertake a regular "health check" of their risk assessments and the measures that they have in place to mitigate or avoid those risks. In this regard, cyber risks are obviously an increasing risk for all financial service providers. As ASIC has previously identified, an adequate risk management system will need to:

- be based on a structured and systematic process that takes into account the key risks to the AFSL holder's business in light of its obligations under the Corporations Act
- focus in particular on risks that adversely affect consumers or market integrity
- establish and maintain controls designed to manage or mitigate those risks and
- fully implement and monitor those controls to ensure they are effective

A regular review of the adequacy of an AFSL holder's technological resources, including IT system security, disaster recovery systems and business recovery, is another important component of an effective risk management system. The case against RI also evidences the importance of implementing appropriate steps to

respond adequately when cybersecurity incidents reveal gaps in an entity's risk management systems and resources, including in relation to its authorised representative network.

For responsible entities, the disclosure of any identified cyber risks will need to be carefully considered in any product disclosure statement that is published.

Finally, all AFSL holders need to be conscious of their breach reporting obligations in the event that a cybersecurity breach is identified.

Alasdair McLean
Principal
Piper Alderman
amclean@piperalderman.com.au
www.piperalderman.com.au

Oscar Ruane
Associate
Piper Alderman
oruane@piperalderman.com.au
www.piperalderman.com.au

Footnotes

1. Australian Securities and Investments Commission "ASIC commences proceedings against RI Advice Group Pty Ltd for alleged failure to have adequate cyber security systems" media release (21 August 2020) https://asic.gov.au/about-asic/news-centre/find-a-media-release/2020-releases/20-191mr-asic-commences-proceedings-against-ri-advice-group-pty-ltd-for-alleged-failure-to-have-adequate-cyber-security-systems/.

More questions than answers: Treasury releases litigation funding regulations ahead of 22 August deadline

***Andrea Beatty**, **Chelsea Payne** and **Chloe Kim** PIPER ALDERMAN*

Since 22 August 2020, litigation funding schemes are subject to the Australian Financial Services Licence (AFSL) requirements and the managed investment scheme (MIS) regimes set out in the Corporations Act 2001 (Cth). The perception for the regulation is to ensure consumer protection and pricing fairness.

Treasurer Josh Frydenberg was quoted in an article in the *Australian Financial Review* published on 25 August 2020 as explaining the justification for the regulation of litigation funders: "litigation funders do not face the same regulatory scrutiny and accountability as other financial services and products under the Corporations Act" and:

> . . . 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.[1]

However, the changes have been criticised for being implemented prior to a federal parliamentary committee inquiry looking into the litigation industry handing down its final report later this year.

On 23 July 2020, the government released the Corporations Amendment (Litigation Funding) Regulations 2020 (Cth) (Regulations) which came 2 months after Treasurer Josh Frydenberg first announced the Regulations in May. The intention of the Regulations is to subject class action litigation funders to regulatory oversight by removing their Corporations Act exemption from needing an AFSL and requiring them to comply with Pt 7.9 of the Corporations Act regarding financial product disclosures. The Regulations came into force on 24 July 2020 and will be enforceable for new litigation funding schemes entered into on or after 22 August 2020.

Overview

The seminal *Brookfield Multiplex Ltd v International Litigation Funding Partners Pte Ltd*[2] (*Brookfield*) case was used as a guide to discuss whether arrangements for funded class actions were an MIS under the Corporations Act. The Full Federal Court's 2:1 majority decision made in 2009 held that a third-party litigation funding arrangement met the definition of an MIS and did not fall into any of the specific exemptions applying at that time. Consequently, an express exemption for all litigation funding schemes and arrangements from the MIS definition and an exemption from having to obtain an AFSL were implemented. The Regulations repeal and replace certain of those exemptions.

On 25 August 2020, Shadow Attorney-General Mark Dreyfus announced Labor Party's intention to disallow the Regulations in the Senate, claiming the strict requirements on litigation funders would prevent Australians' access to justice.[3]

There are grandfathering provisions for schemes formed before 22 August 2020. Once at least two claimants are signed up to a funding agreement as at 22 August 2020, the scheme is in existence as at 22 August 2020 and therefore is not an MIS under the current Corporations Regulations 2001 (Cth) (Current Regulations). It is not necessary for the litigation fund to have commenced court proceedings.

Litigation funding scheme — class action and multi-plaintiff claims

The Regulations (as well as their preceding provisions in the Current Regulations) are best viewed as a safe harbour from the MIS regime. The Regulations do not actually deem litigation funding schemes to be an MIS. They only deem insolvency litigation funding schemes and litigation funding arrangements not to be an MIS if the relevant tests are met.

In the case of matters that meet the definition in the Corporations Act of litigation funding scheme, they were formerly deemed not an MIS under the previous regime. Now under the Regulations they are no longer deemed not an MIS. The definition in reg 7.1.04N of the Current Regulations of a litigation funding scheme is only to make the scheme a financial product. Whether they are an MIS depends on the underlying law and definition in the Corporations Act, with *Brookfield* being used as a guide.

Litigation funding schemes that are an MIS which have retail clients will be required to be registered under Ch 5C of the Corporations Act and will need to be operated by a "responsible entity". This is a public company (which may be unlisted) that holds an AFSL with an authorisation to operate the scheme.

Litigation funding schemes will also now be subject to the AFSL regime. As an AFSL holder, operators of class action and multi-plaintiff litigation funding schemes will be required to abide by their licence conditions and the general rights and obligations under s 912A of the Corporations Act. A key duty is the duty to act efficiently, honestly and fairly. This duty could feature in any disputes concerning plaintiff recovery amounts and funding costs.

Carve-outs

The Regulations preserve and exempt three types of litigation funding schemes and arrangements from having to register as an MIS and from obtaining an AFSL. They are insolvency litigation funding schemes, litigation funding arrangements — proof of debt arrangements and litigation funding arrangements — single plaintiff schemes.

Insolvency litigation funding scheme

An insolvency litigation funding scheme relates to funds, indemnities or both (including through a trust) provided by creditors or members of the body corporate to the body corporate or external administrator. This scheme is not affected by the Regulations and remains exempt from both the MIS and AFSL regimes, despite interests in the scheme being considered a financial product.

Litigation funding arrangement — proof of debt arrangements

The litigation funding arrangement in reg 5C.11.01(4) captures proof of debt arrangements under Div 6 of Pt 5.6 of the Corporations Act that were covered by the previous litigation funding arrangement in reg 5C.11.01(1)(d) of the Current Regulations.

The operation of proof of debt litigation funding arrangements has not been affected by the Regulations. They remain exempt from both the MIS and AFSL regimes, despite interests in the arrangement being considered a financial product.

Litigation funding arrangement — single plaintiff claims

The litigation funding arrangement in reg 5C.11.01(5) captures single plaintiff claims that were covered by the previous litigation funding arrangement in reg 5C.11.01(1)(d). This arrangement exactly mirrors litigation funding schemes for class actions and multi-plaintiff claims but refers only to a single party and removes the requirements in reg 7.1.04N(3)(b).

The operation of litigation funding arrangements has not been affected by the new Regulations. They remain exempt from both the MIS and AFSL regimes, despite interests in the arrangement being considered a financial product.

AFSL and MIS requirements

If a litigation funding scheme's purpose is for the same, similar or related transactions or circumstances that give rise to a common issue of law or fact or different transactions or circumstances, but the claims of the general members can be appropriately dealt with together and consequently do not fall under the three exemptions listed above, it will be required to register under Ch 5C of the Corporations Act as an MIS. It will need to be operated by a "responsible entity", being a public company that holds an AFSL with an authorisation to operate the scheme. It is currently unclear as to whether it is the intention of Treasury to capture multi-plaintiff matters within the definition of "litigation funding scheme".

As an AFSL holder, schemes will be required to have adequate arrangements regarding conflict management, reporting significant breaches of financial services laws and acting in a fair, efficient and honest manner. There are also other AFSL and MIS obligations.

Product disclosure statement

If the financial product offered is for retail clients, the MIS would also be subject to other obligations such as providing a product disclosure statement (PDS). The PDS should outline prescribed disclosures regarding fees, risks and benefits. General members of a litigation funding scheme will also be required to be provided with periodic statements in accordance with Pt 7.9 of the Corporations Act.

Design and distribution obligations

AFSL holders need to comply with the new design and distribution obligations enforceable from 5 October 2021. Offerors of financial products to retail clients must consider the intended clients of their product and whether the design of the products would be appropriate for their intended clients. They must ensure that products are not offered to persons outside their target market.

Insurance and compensation

As an AFSL holder, proper compensation and insurance arrangements are required to be in place for retail

clients to remunerate the possible losses which they could suffer as a result of a breach by the licensee or its representative as per s 912B of the Corporations Act.

Anti-hawking

In accordance with the new Regulations' anti-hawking provisions, unsolicited offers to issue or sell a financial product as outlined in s 992A(3) of the Corporations Act will be prohibited. "Hawking" conduct includes unsolicited telephone calls or meetings with another person in the course of issuing or selling financial products.

The exception is if the other person has provided a positive, clear and informed request for a call or meeting, for example by completing an online inquiry form on the law firm or funders' website.

The government's intention to implement stringent anti-hawking legislation, Financial Sector Reform (Hayne Royal Commission Response — Protecting Consumers (2020 Measures)) Bill 2020: Hawking of Financial Products from 1 January 2021 to regulate unsolicited offers could pose potential issues in obtaining interest in a class action in future class action proceedings. This will require litigation funders to:

- keep the form of communication requested by the claimant consistent so other mediums are not utilised unless specifically requested
- make contact with potential claimants within the 6-week period from when the request was made and
- be wary that the request for communication has not been varied or withdrawn prior to the contact occurring as they are able to do so at any time

Conflicts of interest

Previously, the exemption for litigation funders from the AFSL regime required funders to have adequate arrangements in place to address conflicts of interest in accordance with *Regulatory Guide 248: Litigation Schemes and Proof of Debt Schemes: Managing Conflicts of Interest*[4] (RG 248). This obligation in relation to class actions and multi-plaintiff actions is now removed as these arrangements will be subject to the conflicts of interest provisions applicable to AFSL holders. Insolvency litigation funding schemes and litigation funding arrangements that are exempt from the requirement to hold an AFSL will be required to continue to comply with the existing requirements under RG 248.

AFCA membership

AFSL holders for litigation funding schemes will be required to become members of the Australian Financial Complaints Authority (AFCA) if they obtain an AFSL for the provision of financial services to retail clients. Section 912A(1)(g) of the Corporations Act requires retail AFSL holders with retail clients to become a member of AFCA.

ASIC's relief

On 21 August 2020, the Australian Securities and Investments Commission (ASIC) announced their "Day 1 relief" through implementing the ASIC Corporations (Litigation Funding Schemes) Instrument 2020/787 (Instrument) to assist in transitioning to the new litigation funding regime. The Instrument provides the relief outlined below:

- PDS — conditional relief from s 1012B of the Corporations Act which would have required the responsible entity of a litigation funding scheme to provide a PDS to a passive general member of the litigation funding scheme. However, the PDS is still required to be made publicly available for general transparency and referred to in advertising material. It also must be given to any active participants in the open class action such as any plaintiffs who have signed a retainer or a funding agreement
- valuations — relief from having to value scheme property at regular intervals in accordance with s 601FC(1)(j) of the Corporations Act
- members' register — relief from the obligations contained under ss 168 and 169 of the Corporations Act to maintain a register of members' names and addresses. ASIC has outlined their "no-action" position in regard to this requirement, meaning strict compliance with the member registration will not be regulated or enforced as it is impractical to expect responsible entities of registered litigation funding schemes that have one or more passive members in an open litigation funding scheme to maintain it
- member withdrawals — relief from the requirement that withdrawal by a member from a litigation funding scheme would be required to comply with Pt 5C.6 of the Corporations Act. Without this relief, a non-liquid scheme may only permit its members to withdraw as per the Pt 5C.6 guidelines. Members must be allowed to withdraw from the scheme if they have opted out in accordance with the court rules or any order of the court in the proceedings or if they cease to have an interest in the outcome of the proceedings
- costs and standards — relief from having to detail any detailed fees and costs information and disclose labour standards and environmental, social and ethical considerations in accordance with

reg 7.9.16N(2) of the Current Regulations and s 1013D(1)(l) of the Corporations Act

Disallowance of regulations

The *Australian Financial Review* reported on 25 August 2020 that Labor will seek to quash the regulation of litigation funding by moving a disallowance motion for the Regulations in the federal Senate. The Shadow Attorney-General Mark Dreyfus claimed: "Labor will stand up for the rights of ordinary Australians seeking access to justice by moving to disallow the Morrison government's attempt to cripple class actions by regulation", and "[l]itigation funding and class actions provide a vital path to justice for Australians trying to uphold their rights against wealthy defendants with vastly greater resources".[5]

Andrea Beatty
Partner
Piper Alderman
abeatty@piperalderman.com.au
www.piperalderman.com.au
www.andreabeatty.com.au

Chelsea Payne
Associate
Piper Alderman
cpayne@piperalderman.com.au
www.piperalderman.com.au

Chloe Kim
Law Graduate
Piper Alderman
ckim@piperalderman.com.au
www.piperalderman.com.au

Footnotes

1. R Mizen "Labor seeks to quash litigation funding rules" *Australian Financial Review* 25 August 2020. See The Hon J Frydenberg "Litigation funders to be regulated under the Corporations Act" media release (22 May 2020) https://ministers.treasury.gov.au/ministers/josh-frydenberg-2018/media-releases/litigation-funders-be-regulated-under-corporations.
2. *Brookfield Multiplex Ltd v International Litigation Funding Partners Pte Ltd* (2009) 180 FCR 11; 260 ALR 643; [2009] FCAFC 147.
3. Mizen, above n 1.
4. Australian Securities and Investments Commission *Regulatory Guide 248: Litigation Schemes and Proof of Debt Schemes: Managing Conflicts of Interest* (April 2013) https://download.asic.gov.au/media/1247153/rg248.pdf.
5. Mizen, above n 1.

For editorial enquiries and unsolicited article proposals please contact Shomal Prasad at shomal.prasad@lexisnexis.com.au.
Cite this issue as (2020) 19(6) *FSN*
SUBSCRIPTION INCLUDES: 10 issues per volume plus binder www.lexisnexis.com.au
SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067
CUSTOMER RELATIONS: 1800 772 772
GENERAL ENQUIRIES: (02) 9422 2222
ISSN: 1035-2155 Print Post Approved PP 25500300764