gadens

Consumer Express

November 2026



Contents

Click title to jump to article

3 Consumer *Express* editor's letter

4 Unfair contract terms: Is Amazon Primed to be the first unfair contract terms decision under the new penalty regime?

7 Recent misleading misdemeanours: ACCC and Ad Standards pricing lessons

10 Higher penalties, higher stakes

12 The ACL's new subscription contract regime: Don't get trapped!

15 Online safety and privacy: Developments to watch

19 Security, pixels and consent: Preparing consumer and retail businesses for Tranche 2 Privacy Reforms

22 Product safety reform is back on the agenda

24 Wage compliance landscape: The growing cost of non-compliance for employers and franchisors

26 Retailers under pressure: Why tenant distress is increasing

This publication does not constitute legal advice and should not be relied upon as such. It is intended only to provide a summary and general overview on matters of interest to clients in the Consumer Goods sector, and it is not intended to be comprehensive. Careful consideration should be given to specific factual circumstances and the resulting legal implications. You should seek legal or other professional advice before acting or relying on any of the content. In NSW, QLD, SA, VIC and WA: Liability limited by a scheme approved under Professional Standards Legislation.

Copyright © Gadens 2026. All rights reserved.

Consumer *Express* editor's letter

Consumer-facing businesses are entering a period of significant regulatory change, with higher penalties, new obligations and increasing scrutiny of the practices that shape the customer experience.

In this edition of Consumer *Express*, we examine some of the key developments businesses should have on their radar. The ACCC's proceedings against Amazon put the strengthened unfair contract terms regime under the spotlight, particularly the use of unilateral variation clauses in consumer contracts. Separately, recent regulatory action and decisions concerning promotional pricing highlight the scrutiny being applied to 'was/now' pricing, discount claims and the overall impression advertising creates for consumers. Gadens experts also consider the new laws commencing in 2027 relevant to subscription contracts and the steps businesses can take now to prepare.

Technology and data remain another major area of change and Gadens is at the forefront of legal insight. We consider proposed privacy reforms, developments specific to children's online privacy and the Digital Duty of Care signal increasing expectations around privacy, security, consent and safety by design. Increasingly, compliance depends not only on contracts and policies, but on how websites, apps, advertising technology and customer journeys operate in practice.

We also examine the impact of higher competition and consumer law penalties, product safety reform, increasing wage compliance risk and the growing pressure facing retail tenants and their landlords.

Together, these developments reinforce the importance of staying ahead of regulatory change. Businesses should be reviewing existing practices now, identifying emerging areas of exposure and ensuring their compliance frameworks remain fit for purpose.



Breanna Davies
Partner and Editor
+61 2 9163 3017
+61 414 581 209
breanna.davies@gadens.com



Unfair contract terms: Is Amazon Primed to be the first unfair contract terms decision under the new penalty regime?

By Adam Walker, Partner, Breanna Davies, Partner, David Fleming, Partner, Lisa Haywood, Special Counsel and Phoebe Ralston, Graduate

On 29 June 2026, the Australian Competition and Consumer Commission (**ACCC**) commenced proceedings in the Federal Court of Australia against Amazon Commercial Services Pty Ltd (**Amazon AU**) and Amazon.com Services LLC (**Amazon US**) alleging contraventions of the unfair contract terms (**UCT**) regime under the Australian Consumer Law (**ACL**).

When Amazon AU introduced ads to Prime Video in July 2024, annual Prime subscribers had already paid $79 upfront. Amazon AU then told them that ad-free viewing would now cost an extra $2.99 per month. The ACCC alleges that Amazon AU could only do this because its Prime subscription contracts contained unfair terms. These terms allowed Amazon AU to unilaterally change the service mid-subscription without offering customers a remedy.

The proceeding is significant not merely because it concerns Amazon, but because it is one of the first opportunities for the Federal Court to consider the post-9 November 2023 UCT penalty regime in a contested case. Since 9 November 2023, businesses face civil penalties for proposing an unfair term in a consumer or small business standard form contract and for relying or purporting to rely on an unfair term. The ACCC is seeking penalties against both Amazon AU and Amazon US. Businesses that rely on unilateral variation rights, particularly in subscription contracts, should take close notice.

The outcome is likely to provide important guidance on:

- the limits of unilateral variation clauses
- what constitutes a legitimate interest
- whether notice alone can address contractual imbalance
- the role of refunds or other meaningful redress.

Background

Amazon AU announced on 22 September 2023 that ads would come to Prime Video in 2024. On 21 May 2024, Amazon AU told subscribers that the change would take effect from 2 July 2024, that ad-free viewing would cost an extra $2.99 per month, and that no action was required. Prior to that, Prime Video was almost entirely ad-free. As of 2 July 2024, more than 850,000 annual subscribers had already paid for their subscription. Of these, more than 600,000 had subscribed or renewed since 9 November 2023.

The ACCC alleges that by introducing ads in this way, Amazon AU relied on the variation of services terms, contravening the UCT provisions of the ACL. As ACCC Chair Gina Cass-Gottlieb put it, *"Consumers who wanted to avoid ads were left with no choice but to pay more to maintain the service they'd initially signed up for."*

The ACCC further alleges that:

- Amazon AU relied, or purported to rely, on one or more of the unfair terms (set out below) to introduce the Prime Video ads in July 2024
- Amazon US was knowingly concerned in Amazon AU's conduct. The ACCC says Amazon US helped draft the Australian contracts containing the alleged unfair terms, decided to introduce advertising to Prime Video globally and helped implement that decision in Australia.

A notable feature of the proceeding is the ACCC's allegation that Amazon US was knowingly concerned in Amazon AU's conduct. The claim highlights that an overseas parent or group entity involved in drafting, approving or implementing Australian consumer contracting practices may itself face exposure under the ACL.

Under the ACL, each unfair term in a standard form consumer contract can give rise to a separate contravention. This could significantly increase Amazon

AU's exposure, as the ACCC alleges that Amazon AU contravened the ACL:

- each time it proposed an unfair term in a contract with an annual Prime subscriber, with each of the five terms counted separately
- each time it relied, or purported to rely, on those terms in relation to an annual subscriber who subscribed or renewed on or after 9 November 2023.

What terms is the ACCC concerned about?

The ACCC alleges that the following terms (collectively, the **Relevant Terms**) were unfair. They appear in Amazon's Conditions of Use (**Use Conditions**), Prime Video Terms of Use (**Video Terms**) and Prime Terms and Conditions (**Prime Terms**), as noted below.

a. **Use Conditions cl 15:** 'We reserve the right to cease providing any Amazon Service, or any part thereof, to discontinue any Amazon Service and to make changes to any Amazon Services, including adding or removing content from Amazon Services at any time. Where we make a materially adverse change to an Amazon Service, as reasonably determined by us, we will provide advance notice to you.'

b. **Video Terms cl 6(d):** 'Amazon may change any aspect of the Service in accordance with clauses 15 and 16 of the Amazon Conditions of Use. Where we make a materially adverse change to this Agreement or the Service, as reasonably determined by us, we will provide you with prior written notice via email or reasonably substitutable means.'

c. **Prime Terms cl 4:** 'We may in our reasonable discretion change these Terms, the Prime Service, or any part thereof in accordance with the Amazon Conditions of Use. Any changes implemented by Amazon will not affect your rights to cancel your membership auto-renewal at any time. Where we make a materially adverse change to these Terms or the Prime Service, as reasonably determined by us, we will provide you with prior written notice via email or reasonably substitutable means.'

d. **Use Conditions cl 16:** 'We reserve the right to make changes to any Conditions of Use and Service Terms at any time by posting the changes on Amazon.com.au, or such other website or application that is used to provide the Amazon Services. Where we make a materially adverse change to these Conditions of Use or any applicable Service Terms, as reasonably determined by us, Amazon will provide advance notice to you.'

e. **Video Terms cl 6(e):** 'Amazon reserves the right to amend any part of this Agreement in accordance with clause 16 of the Amazon Conditions of Use. Where we make a materially adverse change, as reasonably determined by us, we will provide you with written notice via email, or if no email is available, via reasonably substitutable means.'

Each of the Relevant Terms required Amazon AU to give advance notice of a 'materially adverse change, as reasonably determined by us', while the Prime Terms preserved the subscriber's right to cancel any auto-renewal at any time.

The ACCC argues that neither notice nor a right to terminate addressed the imbalance, because annual subscribers who had prepaid had no right to a pro rata refund.

The ACCC also contends that the Relevant Terms were not reasonably necessary to protect Amazon AU's legitimate interests. The ACCC says this is supported by the fact that Amazon AU subsequently amended clause 4 of the Prime Terms and clauses 6(d) and (e) of the Video Terms. The amended terms introduce a right to a pro rata refund where annual Prime subscribers cancel in response to materially adverse changes.

The ACCC says that, because of the breadth of the Relevant Terms, Amazon AU could change its Prime Video offering without any meaningful constraint. It says this allowed changes that significantly altered the services Amazon AU provided, the governing contractual framework, or both. The ACCC also says that, despite making a substantial prepayment for their subscription, annual Prime subscribers had no meaningful entitlement to redress.

The ACCC is seeking declarations, penalties, consumer redress, costs and other orders.

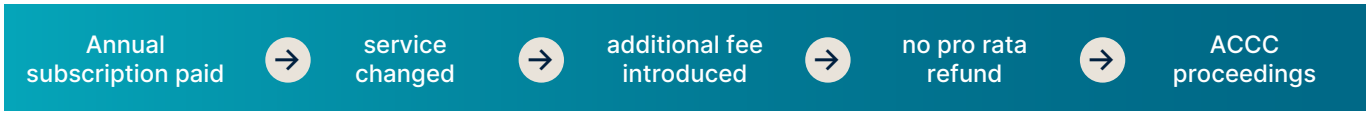
Aside from Amazon's broad variation powers, another question that may be explored is that the contractual safeguard itself depended on Amazon determining whether a change was materially adverse, leaving Amazon both to exercise the power and to assess whether the notification safeguard applied.

Treasury's review of the amended UCT protections

The Amazon proceedings come shortly after Treasury's May 2026 final report reviewing the 2022 UCT reforms. Treasury found that civil penalties had increased deterrence, with more businesses reviewing and amending their standard form contracts. However, it noted that no court had yet imposed penalties under the new regime and that visible enforcement remained critical. The report also recommended giving the ACCC and the Australian Securities and Investments Commission (**ASIC**) power to issue infringement notices for alleged UCT contraventions. It also recommended leaving the small business thresholds unchanged.

Separately, the express monetary maximum penalty under the ACL increased to $100m for companies from 28 March 2026. Against that background, the timing and scale of the Amazon proceeding reinforce the ACCC's focus on visible enforcement under the reformed regime.

The Federal Government has confirmed its intention to introduce infringement notice powers for the regulators. These powers will allow the ACCC and ASIC to respond more flexibly to lower-level breaches without the need



for lengthy court proceedings. The legislation has not yet been introduced into Parliament.

Once these powers are in place, businesses are likely to see wider enforcement action from both regulators in relation to unfair contract terms.

Practical implications for businesses

From a practical standpoint, the case against Amazon, in conjunction with the anticipated increased enforcement powers for regulators, should encourage businesses to check standard form agreements in use for any terms that might attract attention in relation to unfair contract terms. In particular, businesses should:

- **Audit standard form contracts:** Identify every standard form contract used with consumers and small businesses (including online terms, subscription terms and supplier agreements), and prioritise contracts made, renewed or varied since 9 November 2023, as these are exposed to penalties.
- **Look at one-sided terms:** Review broad limitations of liability, one-way indemnities, termination rights available only to you, and short timeframes for customers to raise disputes or defects.
- **Be able to justify each term:** A term is presumed not to be reasonably necessary to protect your legitimate interests, so document why any one-sided term is needed for your business.
- **Make terms transparent:** Use plain language, present key terms prominently, and avoid burying important terms across multiple linked documents.
- **Think before relying on a term:** Relying on an unfair term is a separate contravention, so before using a variation or termination right, consider whether the term could be unfair and how customers will be affected.
- **Review group and template terms:** If terms are prepared by an overseas parent or a template provider, check they comply with Australian law, as the involvement of Amazon US shows group companies may also be exposed.
- **Build in ongoing compliance:** Train staff who draft or change customer terms, review terms regularly, and seek legal advice before rolling out material changes.

Regardless of the outcome, the proceeding provides a clear indication of the ACCC's enforcement priorities. Businesses should treat unilateral variation rights, cancellation mechanisms, subscription terms and customer remediation rights as priority review areas, rather than waiting for judgment before addressing potential exposure.



Recent misleading misdemeanours: ACCC and Ad Standards pricing lessons

By Marina Olsen, Partner, Annika Dunlop, Senior Associate and Tess Nossal, Graduate

Sections 18 and 29 of the Australian Consumer Law (**ACL**), contained in Schedule 2 to the *Competition and Consumer Act 2010* (Cth), are the main rules governing advertising in Australia. These provisions prohibit entities from engaging in misleading or deceptive conduct in trade or commerce and from making false or misleading representations about certain matters relating to goods or services. The Australian Competition and Consumer Commission (**ACCC**) is the independent Commonwealth statutory authority responsible for enforcing the ACL. Supplementary to the ACL are various industry-led codes of practice designed to regulate advertising standards and ensure consumer protection. The Australian Association of National Advertisers (**AANA**) is a self-regulatory body which has developed rules for advertising that are expressed in Advertising Codes.

Like the ACCC, Ad Standards plays a central role in holding advertisers to account, administering the complaints process for the AANA's Advertising Codes. The Ad Standards Community Panel assesses complaints from members of the community. Its members are drawn from a broad range of age groups, backgrounds and occupations, and are independent of the advertising industry. Complaints submitted by competitors are assessed by the Ad Standards Industry Jury, a panel comprising three lawyers who specialise in advertising law and/or competition and consumer law and are selected on a case-by-case basis from a register of lawyers.

Although both bodies aim to prevent misleading or deceptive advertising, they do so in different ways. The ACCC enforces relevant legislation against Australian entities, whereas Ad Standards operates as a self-regulatory complaints system without applying legal tests. In this article, we look at recent matters across two current focus areas for advertising compliance, pricing and environmental claims (greenwashing), to show how each body determines whether advertising crosses the line.

digiDirect: enforceable undertaking over strikethrough pricing

Between at least 1 May 2024 and 8 November 2025, Digital Imaging Express Pty Ltd trading as digiDirect, advertised certain electronic products on its website as being discounted from a higher price. Products including wireless keyboards, cameras and camera accessories were advertised with a higher price in strikethrough and the lower price accompanied by the words 'prices slashed'.

The ACCC investigated the strikethrough discount claims and considered that the electronic items were almost never sold or advertised at the higher price. As a result, consumers may have been misled into thinking they were receiving a genuine discount when the products were regularly sold at the lower price.

In an enforceable undertaking given to the ACCC on 17 September 2026, digiDirect admitted that its discount claims were false or misleading, in breach of contravened sections 18 and 29(1)(i) of the ACL. Among other things, digiDirect undertook not to make these, or similar, representations again. digiDirect also paid five infringement notices totalling $99,000.

Misleading price reduction claims: When is a 'was/now' discount genuine?

'Was' pricing, strikethrough prices and 'price drop' promotions are only lawful under the ACL if the discount claim is genuine. A 'was' price, or a claim that a price has been 'dropped' or 'slashed', tells consumers they are saving money compared to the price usually charged. If the higher price was rarely charged or charged for only a short time before the 'discount', the saving may be illusory. The claim may then contravene section 18, section 29(1)(i), or both. The ACCC's proceedings against Australia's two largest supermarkets show its focus on this issue.

ACCC v Coles

Earlier this year, in *ACCC v Coles Supermarkets Australia Pty Ltd* [2026] FCA 598, the Federal Court found that Coles had contravened the ACL in its well-known 'Down Down' promotion. The ACCC alleged that, between February 2022 and May 2023, Coles temporarily raised the price of 245 common household products by at least 15% for a short period. It then placed them on a 'Down Down' promotion at a price that was the same as, or higher than, the pre-increase price. The 'Down Down' tickets used 'was/is' comparative pricing, where the new 'discounted' price was shown next to a higher 'was' price. The tickets did not tell shoppers that the 'was' price had applied for only a short time, or that the product had sold for less before that. Typically, a product was sold at one price for a median of a year, increased for a median of 28 days, then reduced again to a third price that was equal to or higher than the original price.

Coles denied the discounts were illusory, arguing that the price increases were the result of supplier cost pressures and inflation, and that it sold the higher-priced items in substantial volumes before discounting them.

On 14 May 2026, the Federal Court found that Coles had increased its prices 'in a commercially justifiable manner' and did not choose artificially high 'was' prices to inflate the apparent discount (at 39). However, the question was whether the 'was' price had been properly established as the ordinary price before the promotion began. Justice O'Bryan held that ordinary customers would not carry out an intellectualised analysis of the ticket. Instead, they would absorb its 'immediate and dominant' messages. If customers had known that the product was sold at the 'was' price for such a short period, they would not have considered the 'Down Down' price a genuine discount.

The liability hearing examined an agreed sample of 14 'Down Down' tickets. The Court held that 13 of them conveyed misleading representations to consumers. The Court will decide penalties and other orders at a later date, and the ACCC has said it will seek a 'substantial penalty'.

ACCC v Woolworths

The ACCC has brought similar proceedings against Woolworths, in ACCC v Woolworths Group Ltd (Federal Court of Australia, VID 974 of 2024), over its 'Prices Dropped' program. A seven-day hearing, also before Justice O'Bryan, concluded in April 2026. Judgment has been reserved and is expected shortly.

> The key question to be determined by the Court is likely to be whether the higher price had been legitimately established in the market.

The proceedings concern 276 promotions run between September 2021 and May 2023, as Woolworths phased out its 'Prices Dropped' program in around December 2024. The tickets in question showed the 'dropped' price alongside a 'was' price and a date and were designed to look different from regular 'specials'. The relevant products had been sold at one price for at least 180 days, then rose by at least 15% for 45 days or less. They then went onto 'Prices Dropped' at a price higher than the original price in most promotions and at the same price in a small number. The parties agree that, in 262 promotions, the price rise followed a supplier's cost increase request that Woolworths had accepted. In 245 of those, Woolworths and the supplier had agreed the later 'Prices Dropped' arrangements before the higher price took effect.

Woolworths denies that the discounts were illusory. It maintains that its tickets were accurate, and that the earlier prices were no longer relevant given significant supplier cost increases during a period of high inflation. Woolworths has argued that its price establishment periods, which ranged from 19 days to more than six weeks, were reasonable.

The key question to be determined by the Court is likely to be whether the higher price had been legitimately established in the market.

Misleading price reduction claims: Black Friday and Cyber Monday

The ACCC first became aware of digiDirect's misleading strikethrough pricing during a sweep of retailers' sales claims made during the 2025 Black Friday sales. The regulator has recently announced another crackdown on misleading pricing claims made during this year's Black Friday and Cyber Monday sales period. It will be conducting a sweep of advertising and promotions across websites, email promotions and social media posts, focusing on certain types of misleading conduct, including the use of:

- promotions which claim that sales are 'sitewide' or 'storewide' when in fact many products are excluded
- offers which are claimed to be time-limited, when in fact the offers continue beyond the stated end date
- tactics which impose time pressure on shoppers to buy, including false claims that stock levels are low
- 'was/now' pricing.

Ad Standards and the AANA Advertising Codes

Alongside the ACL, advertising in Australia is subject to a self-regulatory system. As outlined above, the AANA sets the Advertising Codes, Ad Standards administers the complaints process and the Community Panel or, for competitor complaints, the Industry Jury, independently determines the complaints. Complainants and advertisers can request a review by an Independent Reviewer if they are not satisfied with a decision of a Community Panel. However, an Independent Reviewer will only look at a decision if there is new or additional relevant evidence, a substantial flaw in the decision (because, for example, evidence was clearly misinterpreted) or a substantial flaw in the process.

The system applies to all consumer advertising, whether or not the advertiser is an AANA member, and covers everything from television and print to social media.

The AANA has developed five codes:

1. Code of Ethics (the overarching code that applies to all advertising)
2. Food and Beverages Advertising Code
3. Children's Advertising Code
4. Environmental Claims Code
5. Wagering Advertising Code.

Depending on the product advertised and the audience, one or more specific codes may apply in addition to the Code of Ethics.

The Code of Ethics contains no general prohibition on misleading advertising that community complainants can rely on. Its prohibition on misleading advertising (section 1) applies only to competitor complaints and section 2.7 deals only with disclosure. Ad Standards therefore assesses community complaints about misleading advertising under the product-specific codes. For advertising that makes claims about the environment, this is the Environmental Claims Code (**Code**), which reflects the growing attention to greenwashing, which the ACCC has also named as a 2026–27 compliance and enforcement priority.

Under that Code, environmental claims in advertising must be truthful, factual and must not be, or be likely to be, misleading or deceptive to the 'Target Consumer'. The Code also requires environmental claims to be supported by evidence. Unlike the ACCC and the Courts, the Community Panel does not apply legal tests. Instead, it looks at whether the 'Target Consumer', being the audience the advertisement is likely to reach, would be likely to be misled by the overall impression of the advertisement. The Salmon Tasmania case shows how the principles operate in practice.

Salmon Tasmania Ads

Salmon Tasmania ran advertisements on Facebook, other online platforms and in cinemas across Tasmania that featured underwater footage filmed beneath salmon farm pens in Nubeena in February 2026. The advertisements included the co-managing director of an underwater robotics company, who said: *"People are under the perception that underneath the pens is just a wasteland of sludge. It's not that at all... No build-up of any biomass, thriving marine environment"* and *"Don't just believe everything you hear"*. Community complaints alleged that the advertisement was unrepresentative of the conditions under salmon pens. Salmon Tasmania responded that the footage was genuine and taken under stocked pens in Nubeena and relied on independent environmental monitoring data.

On first assessment, the Community Panel found a breach of the Code. It accepted that the footage reflected the conditions in Nubeena but considered that the overall impression went beyond Nubeena and that the average member of the community would likely understand the footage to be representative of salmon farming across Tasmania. Apart from the advertisements' claim that it was the case, the Community Panel decided there was no material before it to objectively show this. On the basis of the Community Panel's finding, Salmon Tasmania withdrew the advertisements.

Salmon Tasmania then requested an Independent Review, which found substantial flaws in the Community Panel's original reasoning and that the advertiser had provided supporting evidence that the conditions at Nubeena were typical of salmon farms in Tasmania. Importantly, the Independent Reviewer noted that, under the Code and its practice notes, evidence of claims 'are not necessarily required to include that supporting information in the advertisement unless it is required to make the claim true.' The original complaint included the allegation that the advertisement constituted 'greenwashing' because the advertiser's business includes mining and it did not acknowledge the pollution caused by its mining operations. To address this, the Independent Reviewer highlighted earlier panel decisions regarding environmental claims which were assessed by reference to what the advertisement itself actually depicted, not the advertiser's business as a whole.

On reconsideration on 22 July 2026, the Community Panel overturned its decision, finding the claims were specific to Nubeena and the evidence provided was sufficient to justify the claims and unlikely to mislead. Salmon Tasmania was entitled to continue using the advertisements.

Key takeaways

Misleading pricing and greenwashing claims will remain a clear focus for both the ACCC and Ad Standards. For businesses, the key lessons are:

If advertising price reductions, establish 'was' prices properly. A reference price must have applied for a reasonable period before the promotion, with the appropriate period depending on the product and the market.

Commercial justification is not a defence. A genuine reason for a price increase, such as supplier cost pressures, won't save a discount claim if the higher price was not charged for a reasonable period before the promotion.

Consider the overall impression. Regulators also look at the message an advertisement conveys as a whole, not just whether each individual statement is accurate, so make it clear what the claim relates to.

Be able to substantiate environmental claims. Keep objective evidence in supporting any environmental claim. While this does not always need to appear in the advertisement itself, it must be available when a complaint is made.

Take particular care in regulated categories. Specific codes apply when advertising to children, advertising alcohol and gambling or food and beverages or when making environmental claims.



Higher penalties, higher stakes

By Breanna Davies, Partner, Brittany Dorney, Senior Associate and Eva Zofrea, Graduate

Corporations now face significantly higher financial penalties for breaches of Australia's competition and consumer laws following Parliament's passing of the *Treasury Laws Amendment (Doubling Penalties for ACCC Enforcement) Act 2026* (Cth).

For conduct occurring from 28 March 2026, the fixed limb of the three-limb pecuniary penalty applicable to corporations has doubled from $50m to $100m under the *Competition and Consumer Act 2010* (Cth) (**CCA**) and the Australian Consumer Law (**ACL**).

Crucially, a single compliance failure now has the potential to attract greater financial exposure than under the previous deterrence regime.

The revised three-limb test

While the headline change is the increase from $50m to $100m, the broader penalty framework remains unchanged.

For corporations, this means that under the three-limb test, the maximum pecuniary penalty for breaches of the CCA or ACL is the greater of:

1. $100m
2. if the court can determine the value of the benefit obtained, three times the value of the benefit obtained
3. if the court cannot determine the value of the benefit obtained, 30% of the company's (and related bodies corporate's) 'adjusted turnover' during the 'breach turnover period'.

The doubling penalties reforms reinforce the Australian Government's position that penalties must outweigh any commercial benefit derived from the contravention.

Policy response to community concerns

The ACCC has steadily increased its enforcement focus in recent years. The fixed limb of the three-limb test only increased from $10m to $50m in 2022 as part of the more competition, better prices reforms.[1]

While the doubling penalties reforms were prompted by concerns about rising fuel prices and alleged price gouging during recent periods of global instability,[2] the amendments are not confined to any particular industry.

Corporations in all consumer-facing markets must take note that the increased penalties apply to a wide range of competition and consumer law breaches including, cartel conduct, exclusive dealing and resale price maintenance, false or misleading representations, unfair contract terms and product safety breaches.

Before 2022 $10m	**2022** increased to $50m	**28 March 2026** increased to $100m

1 *Treasury Laws Amendment (More Competition, Better Prices) Act 2022*.
2 *Parliamentary Debates*, House of Representatives, 26 March 2026, (Tim Wilson and Jo Briskey, Second Reading Cognate Debate on the Treasury Laws Amendment (Doubling Penalties for ACCC Enforcement) Bill 2026 and Fair Work Amendment (Fairer Fuel) Bill 2026).

Why 'per contravention' matters

As the pecuniary penalties attach to each act or omission, the doubled penalties pose significant financial exposure for corporations operating recurring campaigns and suites of standard form contracts. In those settings, each instance of non-compliance may count as a separate contravention.

The doubling penalties reforms reinforce the Australian Government's view that penalties should not be just a cost of doing business.

Even prior to the latest reforms, the Federal Court has demonstrated its willingness to enforce significant financial penalties for breaches of competition and consumer laws. Notably, in 2024 the Federal Court ordered Qantas to pay $100m in penalties for engaging in misleading or deceptive conduct, making false or misleading representations and engaging in conduct liable to mislead the public.[3]

Implications for corporations

In an environment of higher penalties and increased regulatory scrutiny, the cost of getting compliance wrong has never been greater.

Recent ACCC proceedings against major supermarkets concerning false or misleading representations also demonstrate that, beyond regulatory consequences, the fallout from consumer law breaches can also extend to share prices and reputational damage.

Corporations must take the opportunity to review their compliance programs to ensure that existing compliance frameworks and board reporting processes are capable of identifying and managing risk in light of the higher stakes.

3 *Australian Competition and Consumer Commission (ACCC) v Qantas Airways Ltd* [2024] FCA 1219.



The ACL's new subscription contract regime: Don't get trapped!

By Adam Walker, Partner, Breanna Davies, Partner, Lisa Haywood, Special Counsel and Phoebe Ralston, Graduate

The *Competition and Consumer Amendment (Unfair Trading Practices) Act 2026* (Cth) (**Competition and Consumer Amendment Act**) received Royal Assent on 6 July 2026 and will commence on 1 July 2027. Principally amending the Australian Consumer Law (**ACL**), the Act introduces three key reforms: a general prohibition on unfair trading practices, new disclosure requirements for transaction-based charges and, as the focus of this article, specific obligations for subscription contracts targeting what are commonly described as 'subscription traps'.

Subscription-based business models are now commonplace and provide businesses with recurring revenue. For consumers, sign-up can be immediate. Cancellation, however, may involve hidden settings, multiple steps or repeated retention prompts. The subscription reforms form part of a significant expansion of Australian consumer protection law and reflect growing concern about digital design practices.

The Competition and Consumer Amendment Act responds to growing regulatory concern about the impact of these models on consumers, particularly inadequate disclosures, automatic renewals and complex cancellation processes. It does so through targeted and prescriptive obligations covering disclosure at the point of sign-up, ongoing notifications during the life of the subscription and the method by which subscribers can exit.

For our previous commentary on the Competition and Consumer Amendment Act, refer to our articles here and here.

In this article, we consider which contracts fall within the new subscription contract regime, what suppliers will be required to do and, more importantly, what businesses should be doing now in anticipation of the Competition and Consumer Amendment Act's commencement.

What types of contracts are covered by the Competition and Consumer Amendment Act?

The new subscription contract provisions are being inserted into Part 3-1 of the ACL, alongside the existing unfair practices prohibitions.

Application to consumer and small business subscription contracts

Broadly, the provisions apply to:

- consumer subscriptions for personal, domestic or household use
- standard form subscription contracts with small businesses that employ fewer than 100 employees or have annual turnover below $10m (consistent with the thresholds in the unfair contract terms regime).

What types of subscription contracts are caught by the regime?

The regime applies to four types of subscription contracts, summarised below.

Subscription contract type	Requirements
Indefinite period contracts	A contract that contains terms that have the effect of providing recurring or continuing supply for an indefinite period, where the person automatically incurs liability to pay and has the right to end the contract.
Fixed period contracts	A contract that contains terms that have the effect of providing for the supply of goods or services for a fixed period, where the supply will continue after the fixed period (i.e. automatically renew) unless a party terminates or ceases supply, the person automatically incurs liability to pay and has the right to end the contract.
Initial free period contracts	A contract that contains terms that have the effect of providing for the supply, or recurring or continuing supply, of goods or services for an initial period free of charge, where the person automatically incurs liability to pay after the initial free period and has the right to end the contract before that liability is incurred.
Initial discount contracts	A contract that contains terms that have the effect of providing for the supply, or recurring or continuing supply, of goods or services for an initial period at a discounted rate, where the person automatically incurs liability to pay a higher rate after the initial period and has the right to end the contract before the liability to pay the higher rate is incurred.

Certain arrangements are expressly carved out as 'excluded subscription contracts' under section 48C, including leases and licences of real estate, hire-purchase contracts, contracts for payment in instalments, the supply of childcare, the supply of pre-school or school tuition (only at a pre-school, pre-primary, primary or secondary level) and any other contracts subsequently prescribed by the regulations.

Notably, public utility contracts and contracts for the supply of prescription healthcare products are no longer expressly excluded and may be captured unless excluded by regulation.

What must businesses do?

The subscription contract framework imposes obligations at three stages of the subscription lifecycle: upfront disclosure, ongoing disclosure and cancellation requirements. The Competition and Consumer Amendment Act also establishes a framework for regulations to mandate specific obligations. At the time of writing, those regulations have not been released.

Disclosure at the offer stage

Before a consumer or small business signs up to a subscription contract, the Competition and Consumer Amendment Act requires suppliers to disclose:

- a statement that the contract, if entered into, would be a subscription contract
- any liabilities to pay that the subscriber would or may incur
- the period of the contract
- details of how and when the contract may renew, extend or otherwise continue
- any notice required before the subscriber can end the contract
- how the subscriber can end the contract, including the specific steps they must take to cancel.

This information must be presented in a legible, prominent and unambiguous way, in close proximity to where the contract is available to be entered into (or, where given verbally, in a comprehensible, audible and unambiguous way within a reasonable time before the consumer could agree to the contract). The regulations may also prescribe additional information and specific manners of disclosure for certain goods, services or circumstances.

Ongoing disclosure during the subscription

Disclosure obligations do not end once the consumer has signed up. The Competition and Consumer Amendment Act requires suppliers to notify subscribers of prescribed information at prescribed times during the life of the contract, in a legible, prominent and unambiguous way.

Rather than setting out the exact content and timing in the Competition and Consumer Amendment Act itself, these details will be set by regulation, allowing flexibility by contract type, industry and risk profile. While the regulations have not yet been released, businesses should anticipate obligations such as reminders before a free trial or introductory discount ends, notices ahead of automatic renewals and price increases and periodic reminders for long-running subscriptions.

Cancellation must be easy to find and straightforward

Section 48F requires suppliers to provide a way to end the contract that is 'easy to find' and 'straightforward' and to ensure that each cancellation method requires only steps that are 'reasonably necessary' to end the contract and protect the subscriber's interests.

> In practical terms, cancelling a subscription should not be more difficult than signing up.

Suppliers must also offer an online cancellation option where the subscriber entered into the contract online, or where the supplier provides an online way of entering into a subscription contract for the same kind of goods or services. Retention pop-ups, mandatory exit surveys

and multi-step cancellation journeys will therefore need careful review. While factual explanations about the consequences of cancellation and appropriate security measures may be permissible, unnecessary or extensive feedback requirements are unlikely to be reasonable.

What the reforms do not prohibit

The reforms do not prohibit subscription models, automatic renewal, free trials, introductory discounts or proportionate attempts to retain a customer. They instead require clear disclosure, prescribed lifecycle information and cancellation pathways that do not unreasonably obstruct a subscriber's decision to leave.

Practical implications for businesses

In light of the upcoming changes, businesses should consider the following steps:

- **Map your subscription offerings:** Identify every product or service that auto-renews, rolls over from a free trial or moves from an introductory price to a higher rate, including offerings sold to small businesses on standard form terms.
- **Audit the sign-up journey:** Check that the price after any trial or discount, the renewal date and frequency, and the steps to cancel are displayed prominently next to the 'subscribe' or 'start trial' button, rather than in linked terms and conditions or fine print.
- **Review telephone and in-store sales scripts:** Ensure staff explain the key subscription terms clearly before the customer agrees and keep records of what is said.
- **Build reminder capability:** Ensure billing and CRM systems can send timed notices, for example before a free trial converts to a paid plan, before an annual renewal, or before a price increase takes effect, so that systems are ready when the regulations are finalised.
- **Test the cancellation process:** Count the clicks needed to cancel compared with signing up, place a clearly labelled 'cancel subscription' option in the account settings and remove requirements to call a hotline or use live chat where the customer signed up online.
- **Reconsider retention tactics:** Any retention offers or exit survey should be optional, shown once and easy to skip and should not delay or obstruct the cancellation.
- **Update terms and train staff:** Align customer terms, FAQs and marketing with the new requirements and train customer service teams to process cancellation requests promptly and confirm them in writing.
- **Review complaints data:** Look at complaints, chargebacks and refund requests relating to unexpected renewals or difficulty cancelling, as these are often early warning signs of compliance issues.
- **Review customer journeys, not only contracts:** Assess website and app design, billing processes, renewal communications, account settings and cancellation pathways. In light of the broader reforms with respect to a general prohibition on unfair trading practices, compliance risk is likely to arise from operational design as well as the written terms.

For many businesses, compliance will require more than updated terms and conditions. It will require coordinated changes to customer journeys, billing systems, renewal processes, cancellation architecture and staff practices. Organisations that begin that work now will be better placed when the reforms commence on 1 July 2027.



Online safety and privacy: Developments to watch

By Lara Cresser, Partner, Sinead Lynch, Partner, Emily Woolmer, Associate and Kalarni Orr, Lawyer

As at 30 October 2026

It has been nearly a year since the *Online Safety Amendment (Social Media Minimum Age) Act 2024* (Cth) (**Online Safety Amendment**) came into force and Australia is now entering its next phase of online regulation, proving it continues to be a global leader in regulating the rapidly evolving online landscape.

The Online Safety Amendment took effect on 10 December 2025, with significant civil penalties for systemic failures by social media platforms to take 'reasonable steps' to prevent children under 16 holding accounts. The reform matters even for businesses that are not 'age restricted social media platforms'. It confirms a trend of online regulation aimed at **preventing** harms to children, by reducing the risk of harm, including through mandated standards for age assurance and online safety controls.

In this article we explore:

- the Children's Online Privacy Code 2026 (**COP Code**) introduced under Australia's *Privacy and Other Legislation Amendment Act 2024* (Cth) (**POLA Act**), with the COP Code to be developed by the OAIC by 10 December 2026
- the Online Safety Amendment (Digital Duty of Care) Bill 2026 (**Digital Duty of Care Bill**), which was recently tabled in Parliament and is now before a Senate committee inquiry (Senate Environment and Communications Legislation Committee) for review and response on or before 20 November 2026.

Children's data, profiling and digital engagement

The COP Code proposes to introduce a number of substantial new obligations applicable to children that extend well beyond the existing requirements of the *Privacy Act 1988* (Cth) and Australian Privacy Principles (**APPs**). The COP Code must be developed, finalised and registered by the Privacy Commissioner on or before 10 December 2026.

The COP Code is intended to apply to any online service that constitutes a social media service, relevant electronic service or designated internet service, as defined in the *Online Safety Act 2021* (Cth) (**OSA**).

Privacy Commissioner Carly Kind commented that, *"it has been estimated that by the time a child turns 13, around 72m pieces of data will have been collected about them, making them vulnerable to harms from data breaches, discrimination, algorithmic bias and targeted advertising of harmful products, amongst other risks."*

The COP Code is intended to complement existing protections for children online, such as the Online Safety Amendment. It also includes new obligations designed to create better online experiences for children and young people.

Regulatory timeline

10 December 2025 social media minimum age reforms took effect	**8 September 2026** Exposure draft released	**15 October 2026** Digital Duty of Care Bill introduced	**20 November 2026** Senate committee reporting date identified in the article	**10 December 2026** Deadline for the Children's Online Privacy Code

Interestingly, on 17 September 2026, the European Commission published its highly anticipated proposal for an EU KIDS Act, 'EU Keeping Internet Digital Spaces Accountable and Trustworthy'. The proposed regulation sets age limits, 'safety-by-design' requirements and mandatory age verification on a wide range of digital services and platforms aimed at children. It proposes a gradual uptake of social media for children, restricting access to social media for children under 13 entirely and setting an EU-wide minimum age of 15 for minors to create their own autonomous accounts. The EU KIDS Act would apply to any provider whose service or system is accessible to minors and falls within one of the following categories: online social networking services, video-sharing platform services, software application stores, online games, operating systems, AI companions and general conversational chatbots.

Assent of children under 15 years must be obtained in certain circumstances

Consent

The COP Code is proposed to set the age at which 'a child' can consent to the collection, use, disclosure or storage of their personal information under the Privacy Act, at **15 years old**. For a child under 15, consent from a person with parental responsibility will be required for the handling of any individual's information under that age (with limited exceptions).

Where consent is obtained from a person with parental responsibility, the APP entity collecting, using or disclosing the information will be required to take reasonable steps to verify that the person who gives consent does, in fact, have parental responsibility for the child.

Additionally, it is proposed that an age-appropriate notice detailing, amongst other prescribed matters, how a child's information would be handled, must be provided. The OAIC 'Extended guide to the Children's Online Privacy Code' states that an age-appropriate notice should be child-friendly, easily accessible and in age-appropriate language. This could include non-text-based, visual or audio content notices and pop-up notices.

When children must give assent

Assent of children under 15 years must be obtained in certain circumstances

The COP Code introduces the concept of 'assent'. Assent is when a child expresses their agreement or approval to something, but that approval is not legally binding. It applies where a child under 15 is an end-user of the entity's service and the child enables the entity to:

- collect sensitive information about the child (such as health information)
- use or disclose personal information about the child for a secondary purpose
- use or disclose personal information about the child for the purpose of direct marketing.

In these cases, the APP entity must seek the child's assent to the collection, use or disclosure, and for the entity to contact a person with parental responsibility to obtain their consent to that collection, use or disclosure.

The COP Code explains that online services must do a two-step permission process in the above specific situations by first getting assent from the child, before then getting consent from the child's parent or carer (the person with 'parental responsibility'). The assent requirement would maintain parental consent as the legal authorisation for the collection, use or disclosure while still involving the child in this process.

The request for assent must be age-appropriate and notify the child of the following:

- the information to which the notice relates
- the purpose of the collection, use or disclosure
- the period for which the entity will rely on the consent provided by the person with parental responsibility for the child for the purposes of handling the information
- the consequences of assenting and not assenting
- the child's right to withdraw the assent at any time and the process for withdrawing consent
- if the assent is for the use and disclosure of the information, how the information will be used and the recipients of the information.

Best interests of the child

The COP Code also proposes to layer a 'best interests of the child' assessment test. If implemented as proposed, this test would materially narrow an entity's flexibility in their handling of personal information.

The COP Code Explanatory Statement indicates that entities would need to consider:

- child exploitation risks
- likely mental or physical impacts on the child
- likely impact on the physical, psychological, emotional, social and cognitive development of the child
- the extent to which the child's ability to develop and express their views and identities may be affected.

In practice, online services collecting, using and / or sharing personal information about a child must consider that child's best interests alongside their reasons for collecting the information. This includes determining why the collection is necessary, what the potential risks of harm associated with the collection might be and ensuring that these reasons are consistent with the best interests of the child. Privacy Impact Assessments (**PIAs**) must include, among other requirements, an assessment of whether the handling of children's personal information is consistent with the best interests of the child and record this assessment, including the reasoning on which the assessment is based.

Additionally, the COP Code is intended to reinforce privacy by design requirements for in-scope online services. When assessing whether measures are accessible and clear, entities will be expected to consider whether such measures are appropriate for children, including whether they can be easily understood, located and used.

The OAIC provides an illustrative example, where a child registers and signs up for an online messaging service, it may be strictly necessary for the entity to collect limited personal information to create an account and enable messages to be sent and received. However, the collection or use of the child's personal information to provide personalised recommendations, targeted advertising or make service improvements would not generally be strictly necessary to deliver the core messaging service.

These additional elements of the service may still be offered if they are reasonably necessary for the entity's functions or activities, but they should not involve the collection, use or disclosure of the child's personal information by default. Instead, they should be subject to clear and meaningful choice, such as through privacy settings which are set to 'off' by default.

Digital duty of care

On 8 September 2026, the Department of Infrastructure, Transport, Regional Development, Communications, Sports and the Arts (the **Department**) released an exposure draft of the Online Safety (Digital Duty of Care) Bill 2026 (**Exposure Draft**) for public consultation. Prime Minister Anthony Albanese announced the Exposure Draft as the next step following the social media minimum age (**SMMA**) requirement. He said it would *"ensure Australians have more choice online,"* including through a 'My Feed, My Way' initiative.

Following consultation on the Exposure Draft, the Online Safety Amendment (Digital Duty of Care) Bill 2026 (**Digital Duty of Care Bill**) was introduced into Parliament on 15 October 2026.

The Digital Duty of Care Bill creates an overarching obligation for a person responsible for an online service to take **appropriate** action to ensure a safe online environment. 'Online service' is defined broadly to include, for example, social media platforms, websites, online games and messaging apps. The duty includes taking **effective** measures to mitigate risks identified in risk assessments conducted in accordance with risk assessment requirements outlined in the Digital Duty of Care Bill.

The Digital Duty of Care Bill proposes a 'safety-by-design' model which aims to ensure platforms provide a **safe online environment** by protecting:

- persons in Australia from seriously harmful material and conduct
- children in Australia from material or conduct that is harmful to children and harms associated with design features of an online service.

In determining whether action or measures are **appropriate** or **effective** for the purposes of complying with the Digital Duty of Care Bill, relevant matters include:

- the extent to which the action or measures achieve, or would achieve, a safe online environment
- whether the action or measures are, or would be, proportionate to the level of risk.

The Digital Duty of Care Bill expressly excludes cost consideration when determining whether an action is appropriate and a measure is effective.

A person responsible for an online service also has several additional obligations that sit alongside the Digital Duty of Care. These include:

- conducting written risk assessments which, among other things, must identify reasonably foreseeable risks
- providing accessible and easy-to-use, user empowerment tools on the online service
- complying with any additional requirements for user empowerment tools specified in the legislative instrument in relation to user empowerment tools, while one is in force
- implementing appropriate age assurance measures and access control measures if there is a reasonably foreseeable risk that a child (under 18) could access or be exposed to specific types of material, such as pornography.

Among other things, the Duty of Care Bill also:

- repeals the Basic Online Safety Expectations (**BOSE**) and the Online Safety Codes and Standards, replacing them with the Digital Duty of Care
- expands the eSafety Commissioner's information gathering powers to include the production of documents (not limited to information only), similar to the power in the recent amendments to the SMMA provisions of the OSA
- increases civil penalties broadly throughout the OSA
- gives the eSafety Commissioner broad powers to access an online service's features, systems and processes, by written notice and via a nominated person
- establishes a research and data access scheme
- authorises the eSafety Commissioner and approved Australian researchers to use sock puppet (fictitious) accounts for prescribed activities.

The Government has said that individual instances of harmful material or conduct on a service will not necessarily breach the Digital Duty of Care. However, the presence of such material or conduct may form part of the evidence of a systemic breach.

What organisations should be considering ahead of December 2026

Together, these reforms will require many providers to fundamentally redesign their service to either comply with each regime as though all users are children, offer a differentiated service for adult and child users or restrict children's access altogether.

Recommendations ahead of December 2026:

The COP Code

- **Map your exposure.** Assess whether any product is likely to be accessed by children, including services not aimed at them. The COP Code could likely capture consumer-facing website, app or online services.
- **Test age assurance in practice.** Decide whether to differentiate between child and adult users or apply the COP Code's protections to everyone. Stress-test the mechanisms you choose. Contracts with age

assurance vendors should limit processing, prohibit retention of raw inputs and require attestations that data has been destroyed.

- **Refresh notices, consents and defaults**. Develop age-appropriate consent forms and privacy policies. Audit your default settings against the 'strictly necessary' standard.
- **Stress-testing controls**: Assess current safety and age assurance measures against the 'reasonably practicable' standard, not just against existing terms of service.
- **Embed governance**. Update or undertake PIAs to reflect the COP Code's factors. The COP Code mandates PIAs, training and regular reviews and requires privacy practices to be reviewed at least once a year.
- **Engage relevant stakeholders**. Best-interests assessments, design defaults and marketing practices cut across product, technology, marketing, compliance and legal teams. The COP Code will require changes to technical, operational, organisational and consent processes.

The Digital Duty of Care Bill

- **Map your exposure.** The Digital Duty of Care Bill obligations are broad and the potential for exposure is far-reaching. Key trigger points are harms associated with specific categories of conduct or material on online services, and access to specific design features by children under 16.
- **Identify persons responsible.** For each online service, identify any individuals that may be responsible and have individual obligations under the Digital Duty of Care Bill.
- **Analyse the risk assessment process.** Critically analyse the Digital Duty of Care Bill's risk assessment requirements to determine whether they necessitate any changes to current practice.
- **Check whether current processes are out of date.** The Digital Duty of Care Bill proposes to repeal the BOSE and the Online Safety Codes and Standards. If it passes, some measures already in place by online services may be able to be changed or removed.

Security, pixels and consent: Preparing consumer and retail businesses for Tranche 2 Privacy Reforms



By Sinead Lynch, Partner and Shania Amolik, Associate

To date, Australian privacy law has largely been focused on transparency. If you tell customers what you are doing with their personal information and why, the bar was met. This is set to change. Under the proposed Tranche 2 Reforms, transparency alone will no longer be sufficient. If the reforms are enacted as proposed, many consumer-facing organisations will need to review, and in some cases substantially update, how they collect, use, secure and manage personal information.

On 31 August 2026, the Government released the exposure draft Privacy Amendment (Personal Data Protection) Bill 2026 (the **Draft Personal Data Protection Bill**) for public consultation, which closed on 18 September 2026. We now await the next step – presentation before Parliament – which is currently expected before the end of December 2026. As we outlined in our recent insight, Tranche 2 Privacy Act Reforms: What you need to know, if enacted in its current form, the Draft Personal Data Protection Bill will be the most significant overhaul of the *Privacy Act 1988* (Cth) since the Australian Privacy Principles (**APPs**) commenced in 2014.

For consumer and retail businesses that operate loyalty programs, customer accounts and digital advertising technology, this article focuses on two key areas that warrant immediate attention.

Security and incident preparedness

Balancing customer experience and security

Many consumer-facing businesses are built for scale, and reducing friction at sign-up and checkout is a legitimate commercial priority. In practice, this can sometimes result in certain security settings being calibrated in favour of convenience, for example, making multi-factor authentication optional, adopting less stringent password requirements or defaulting to 'guest' checkout lanes. Each decision may be reasonable in isolation, but together they can increase vulnerability and exposure to account takeover and credential-based attacks. Under the Draft Personal Data Protection Bill, businesses should expect these practices to attract closer scrutiny.

The *Privacy and Other Legislation Amendment Act 2024* (Cth) (the **POLA Act**) clarified that the 'reasonable steps' required to secure personal information under APP 11 include technical and organisational measures. In practice, however, approaches to these measures continue to vary across organisations and can be costly to implement. The Draft Personal Data Protection Bill would build on this position by replacing APP 11 with a new principle covering both security and destruction of personal information.

The Draft Personal Data Protection Bill would expressly require entities to:

- regularly evaluate the effectiveness of their compliance with the proposed security and destruction obligations
- take active consideration of whether to destroy personal information they no longer need (and, if so, to take reasonable steps to destroy or de-identify it)
- take any steps needed to identify the personal information to which those obligations apply.

The last requirement signals for the first time an implied statutory obligation to audit or carry out data mapping of personal information holdings.

A business that does not have appropriate security and access controls (for example, multi-factor authentication on accounts holding years of purchase history, addresses and payment tokens) may find it difficult to demonstrate that its steps were reasonable in the circumstances.

The 72-hour clock

Under the Notifiable Data Breaches scheme, APP entities have up to 30 days to assess a suspected eligible data

Suspected breach: assess and take steps to prevent or reduce harm	**Reasonable grounds to believe an eligible breach occurred:** 72-hour clock begins	**Within 72 hours:** notify the OAIC	**At the same time, if practicable:** notify affected individuals	**After initial notification:** provide missing information and correct material errors

breach. That window would remain, but once an entity becomes aware of reasonable grounds to believe that an eligible data breach has occurred, it would have 72 hours to notify the Office of the Australian Information Commissioner (**OAIC**) with a statement of the breach. The entity would also need to notify affected individuals (or those at risk) of the content of that statement at the same time, if practicable, or otherwise as soon as practicable afterwards. Incomplete initial statements may be permitted, but omissions must be explained[1]. This change is not unexpected. It would bring the Privacy Act more closely into line with the 72-hour regulator notification timeframe under the UK / EU GDPR, as well as existing sector-specific timeframes for certain regulated entities in Australia, such as APRA-regulated financial services businesses.

However, the Draft Personal Data Protection Bill also proposes two further obligations that go beyond a notification timeframe and set the law apart from international neighbours:

- a statutory obligation to take reasonable steps to implement practices, procedures and systems that will ensure the entity complies with the data breach provisions
- a separate obligation to take reasonable steps to **prevent** or **reduce** harm as soon as practicable after becoming aware of reasonable grounds to believe or suspect that there has been a data breach.

Failing to comply with either would be a standalone interference with privacy, even if no eligible data breach ultimately occurs.

What your business should consider now – at minimum

- **Revisit the friction debate and the balance between security and convenience.** Document why each customer-facing security control is enabled. Consider requiring mandatory multi-factor authentication for accounts holding stored value, payment details or sensitive data. Regularly test and evaluate the effectiveness of those controls, consistent with the proposed APP 11.
- **Map, then minimise, your data.** It will be difficult to give the OAIC a statement within 72 hours, or to identify the personal information to which APP 11 applies without knowing which systems hold which customers' information. Consider whether legacy loyalty and marketing data is still needed and, if not, take reasonable steps to destroy or de-identify it.
- **Revisit incident playbooks and response plans.** Distinguish the point at which a data breach is suspected. This would trigger the assessment and harm-reduction obligations from the point at which there are reasonable grounds to believe an eligible data breach has occurred the 72-hour period would start. Build in harm-reduction steps from the moment a breach is suspected, pre-delegate authority to notify, prepare template statements and notifications (including for incomplete initial statements) and rehearse the plan regularly.

Marketing, pixels and the return to consent

The pixel determinations

In June 2026, the Privacy Commissioner published determinations that each of Medmate Australia2 and Monash IVF[3] had interfered with the privacy of individuals by: (i) collecting sensitive (health) information through third-party tracking pixels without consent (APP 3.3), (ii) failing to take reasonable steps to notify individuals of the APP 5.2 matters (APP 5.1) and (iii) using or disclosing that sensitive information for direct marketing, including retargeted advertising on social media platforms, without consent (APP 7.1).

While both decisions turned on the handling of sensitive health information, the Commissioner's reasoning on collection, identifiability and direct marketing is relevant across many sectors. For retailers, the key points to bear in mind are:

- **You may be the collector of what your website or other pixel collects.** The Commissioner found that an organisation that commissions, deploys and configures a tracking pixel collects the information it transmits, even where the data is sent directly to, and stored on, the platform's servers.
- **Individuation can make data personal information:** If data allows you to single out or distinguish an individual from others (for example, to retarget them with advertising), the Commissioner's view is that the individual is likely to be 'reasonably identifiable' and that information is personal information, even if you never know their name.
- **Retargeting can be direct marketing.** Using or disclosing personal information to serve ads to individuals based on their behaviour on your site engages APP 7.
- **A generic cookie banner or privacy policy may not be sufficient.** Where sensitive information is involved, consent is required to collect it and to use or disclose it for direct marketing and reasonable steps must be taken to notify individuals of the collection by pixels of such data.

Tranche 2: Identifiability, consent and trading

The Draft Personal Data Protection Bill would also provide statutory clarification that an individual can be 'reasonably

1 An incomplete initial statement would be permitted where it is impossible or impracticable to provide all required details within 72 hours, provided the entity explains which matters are missing and why, supplies them as soon as practicable, and notifies any material changes or errors (Draft Bill, s26WK(5), Schedule 3 (Data Security))
2 *Commissioner Initiated Investigation into Medmate Australia Pty Ltd (Privacy)* [2026] AICmr 41).
3 (*Commissioner Initiated Investigation into Monash IVF Pty Ltd (Privacy)* [2026] AICmr 40

identifiable' even if their name or legal identity is not known, for example, where information allows them to be recognised, singled out or otherwise dealt with as a distinct individual in practice. This reflects the concept of 'individuation' applied by the Commissioner in the pixel determinations. In the marketing context, if cookie, pixel or device data lets your organisation single out a shopper across visits to serve a tailored ad or offer, it is likely to be personal information, however anonymous it may appear.

Where it is, the Privacy Act obligations, including any applicable consent requirements, will apply. The Draft Personal Data Protection Bill also provides that, where required, consent must be voluntary, informed, current, specific and unambiguous. Practices such as pre-ticked boxes, bundled consents and dark patterns are likely to be difficult to reconcile with that standard.

Importantly, under the Draft Bill, disclosing personal information for money or other consideration, or for the purposes of direct marketing, would be a 'trade' of that information and trading would require the individual's consent. This may capture disclosures made through cookies and pixels in programmatic advertising.

Sharing loyalty data with retail media networks, brand partners or ad platforms would therefore generally require opt-in consent, unless an exception applies (for example, disclosures to a processor acting on the organisation's behalf, or disclosures needed to provide a product or service the individual requested). Direct marketing itself would not generally need consent. However, the Draft Personal Data Protection Bill would redefine it to cover the communication, by any means, of advertising or marketing material to an individual who is selected or targeted (individually or as a member of a class, such as an audience segment) using their personal information.

Organisations would need to provide a simple means to opt out and each communication would need to explain how to do so. Each collection, use and disclosure would also need to be lawful and satisfy the new 'fair and reasonable' test, so consent alone may not support a practice customers would not reasonably expect.

Other: POLA Act obligations arriving in December, 2026

As many will be aware, two POLA Act milestones also fall on or before 10 December 2026.

1. **Automated decision-making (ADM) transparency.** From 10 December 2026, privacy policies must disclose the kinds of personal information used, and the kinds of decisions made, where an entity has arranged for a computer program to make, or do something substantially and directly related to making, a decision that could reasonably be expected to significantly affect an individual's rights or interests.
   - Where those conditions are met, the privacy policy must set out prescribed information on the kinds of personal information used and the kinds of decisions made (solely or substantially) by the operation of such programs (or processes). The OAIC's recent guidance and fact sheets on this obligation confirm that this transparency obligation is not confined to AI or fully automated decisions, and may extend to a broad range of software, decision-support tools and embedded technologies. Privacy policies may group kinds of decisions and personal information, but they should not identify any use of sensitive information separately.
   - For consumer and retail businesses, systems that may warrant review include automated pricing and offer engines, credit or buy now pay later eligibility tools, fraud detection and account suspension tools and loyalty tier or personalisation engines, including tools supplied by third parties. Businesses should map these systems, assess each against the OAIC guidance and flowchart and update their privacy policies before 10 December 2026.

     Read our insight on ADM here for more detailed information on the scope of this transparency obligation for your business.
2. **Children's Code** - The OAIC must also register its Children's Online Privacy Code by 10 December 2026. Businesses whose apps, online services or promotions are likely to be accessed by minors, or individuals under the age of 18, should monitor its final form and scope. For more information on these changes, see our article on Children's Online Safety and Privacy Children's Code.

What marketing teams should consider

- **Audit every pixel and tag.** Identify what fires, on which pages, with which parameters (URLs, hashed emails, advanced matching) and to whom.
- **Restrict sensitive journeys.** Consider removing or restricting pixels on sensitive or higher-risk journeys, including health, pharmacy, politics, financial hardship and age-gated pages.
- **Strengthen consent notices.** Replace generic cookie banners with layered notices that name the pixels and platforms used, backed by consent records you can produce.
- **Map outbound data flows.** Inventory every outbound data flow from loyalty and CRM systems and identify which would need opt-in consent as 'trading' under the Draft Personal Data Protection Bill.
- **Build in privacy sign-off.** Make privacy sign-off a standard step before any new tag, audience or data partnership goes live.

Final note

The Draft Bill is an exposure draft and has not yet been introduced into Parliament. Its commencement date and any transition period remain unsettled. However, given the extended period of consultation that preceded it, the short exposure draft consultation period and broader community concern about privacy and the use of AI, there appears to be momentum behind the reforms.

Many of the POLA Act changes, including the new penalty provisions, took effect the day after Royal Assent, and that Act passed within three months of its introduction. It is therefore possible that parts of Tranche 2 could also commence relatively quickly once passed. As the Draft Personal Data Protection Bill's new handling and security obligations would apply to personal information already held, businesses should start preparing now rather than waiting for the final gavel to drop.



Product safety reform is back on the agenda

By Adam Walker, Partner

The Australian Government has commenced a significant review of Australia's consumer product safety framework, releasing a consultation paper on strengthening the post-market regulation of unsafe products under the Australian Consumer Law (**ACL**).

Other developments also indicate that product safety reform is a major consumer law and regulatory priority. These include:

- the Australian Competition and Consumer Commission's (**ACCC**) response to CHOICE's designated complaint regarding unsafe products sold online
- renewed discussion of general safety protections
- a review of mandatory product safety standards.

For manufacturers, importers, distributors, retailers and online marketplaces, the current reform agenda is notable not only because of the breadth of the issues under consideration, but because policymakers are increasingly questioning whether Australia's existing product safety framework remains fit for purpose in an era of global e-commerce, digital marketplaces and complex supply chains.

A framework built largely around responding to harm

Australia's product safety regime under Part 3-3 of the ACL has traditionally relied on a combination of pre-market and post-market tools. Pre-market measures include mandatory safety standards, mandatory information standards and product bans. Post-market measures include mandatory reporting, voluntary and compulsory recalls, safety warning notices and enforcement activity.

Treasury's September 2026 Consultation Regulation Impact Statement identified three key concerns with the current post-market framework:

1. unsafe products continue to impose significant costs on consumers, businesses and the economy
2. product safety information may be incomplete, inaccurate or delayed
3. existing regulatory tools may not provide sufficient incentives or powers to support timely and effective risk management.

A recurring theme throughout the consultation is that Australia's framework still depends heavily on identifying and addressing risks after products have entered the market.

The reform options currently under consideration include:

Improving recall and information processes

Treasury is considering reforms to improve recall effectiveness and information flows, including:

- clarifying what constitutes a recall action
- improving recall terminology
- strengthening compulsory recall processes
- introducing targeted intervention powers
- expanding mandatory reporting requirements
- potentially requiring the reporting of serious 'near misses'.

Expanding regulatory intervention tools

Treasury is also examining whether regulators should have additional powers to:

- publish safety warning notices directly
- exercise certain approval and administrative functions that Ministers currently exercise
- vary compulsory recall requirements in specified circumstances
- improve the administration of mandatory reporting and recall systems.

Strengthening enforcement

Additional proposals include increased penalties, expanded administrative powers and technical amendments to the product safety framework designed to improve consistency and regulatory effectiveness.

Importantly, Treasury has emphasised that it has not identified a preferred option. Stakeholder feedback will inform whether reform is warranted, which options should proceed and how they should ultimately be designed.

Online marketplaces have become the central policy issue

The consultation formally focuses on post-market regulation. However, concerns about products sold through online marketplaces are driving much of the current policy momentum. CHOICE's designated complaint to the ACCC concerning allegedly unsafe, banned and prohibited products sold online has accelerated this focus. CHOICE argues that Australia's product safety framework has two fundamental weaknesses:

- there is no overarching law preventing unsafe products from being sold
- online marketplaces can facilitate the supply of unsafe products while avoiding meaningful accountability.

In September 2026, the ACCC released its response. The ACCC recognised that there are 'gaps in the current product safety framework relating to online marketplaces' and expressly supported reform directed at those platforms.

The ACCC observed that current product safety laws are often difficult to apply to online marketplaces because:

- product safety obligations generally apply to suppliers
- online marketplaces often position themselves as intermediaries rather than suppliers
- many sellers using those platforms are located overseas, making enforcement challenging.

The ACCC stated that 'reforms are needed to ensure product safety regulators have effective enforcement powers irrespective of the method of purchase'.

It indicated that many of the issues raised by CHOICE would be best addressed through legislative reforms placing clear product safety obligations on online marketplaces. The ACCC's response further noted that:

- Consumer Affairs Ministers have identified a holistic review of the product safety framework, including general safety protections, as a reform priority
- the ACCC supports consideration of general safety protections as part of broader product safety reform.

This represents a significant policy development. Historically, product safety obligations have focused primarily on manufacturers, importers and suppliers. Increasingly, policymakers are examining whether marketplace operators themselves should bear direct responsibility for products offered through their platforms.

The ACCC's product safety agenda is expanding

The consultation should also be viewed in the context of the ACCC's broader product safety strategy.

Unsafe consumer goods in digital markets remain an ACCC compliance and enforcement priority for 2026-27. The regulator has identified increasing concern regarding the sale of unsafe products through digital channels and has emphasised product safety as an enduring enforcement priority.

The ACCC is also:

- engaging in the Government's marketplace reform process
- strengthening the voluntary Product Safety Pledge
- expanding its use of data and intelligence-led approaches to detect emerging risks
- advocating for better product safety data systems
- pursuing targeted product safety enforcement activity where appropriate.

A notable theme emerging from both the ACCC's complaint response and its broader regulatory reform agenda is the desire to create a more level competitive playing field. The ACCC has expressly observed that stronger product safety frameworks can prevent businesses supplying cheap but unsafe products from gaining an unfair competitive advantage over compliant businesses.

Mandatory standards are also evolving

At the same time, the product safety debate is not limited to enforcement powers.

The ACCC has separately identified opportunities to modernise mandatory product safety standards. These include recognising a wider range of overseas standards and improving flexibility for businesses while maintaining safety outcomes. The regulator has stated that adopting appropriate international standards may reduce compliance costs while preserving consumer protection.

This reflects a broader regulatory objective of ensuring that product safety requirements remain responsive to technological developments, changing products and evolving global supply chains.

Practical implications for businesses

Together, the Treasury consultation, the ACCC's response to the CHOICE complaint, the review of mandatory standards and renewed discussion of general safety protections signal a new phase of regulatory scrutiny for Australia's product safety framework.

Organisations should consider:

- assessing product safety governance and escalation processes
- reviewing systems for capturing incidents, complaints and emerging hazards
- evaluating recall readiness and consumer communication procedures
- reassessing contractual allocation of product safety responsibilities across supply chains
- reviewing online marketplace participation and platform governance arrangements
- monitoring compliance with mandatory standards and product bans
- whether current product safety systems would withstand scrutiny under a more interventionist regulatory framework.

For businesses operating in digital markets, particular attention should be given to marketplace arrangements, cross-border sales models and products sourced from overseas suppliers, all of which are attracting increasing regulatory attention.

While the ultimate shape of any reforms remains uncertain, businesses should expect product safety, online marketplace accountability, recall effectiveness and regulatory intervention powers to remain key areas of policy and enforcement focus in the near term.



Wage compliance landscape: The growing cost of non-compliance for employers and franchisors

By Kiri Jervis, Partner Jonathon Hadley, Partner, Bailey Joffe, Graduate and Isabella O'Gorman, Graduate

In 2025-26, the Fair Work Ombudsman recovered $453m in unpaid wages and entitlements for more than 181,000 workers. The message is clear: wage compliance failures carry serious financial, legal and reputational consequences. Complex modern awards, large casual workforces, variable rostering arrangements and decentralised franchise networks can allow payroll errors to arise and continue undetected. With the criminalisation of intentional wage theft now in effect and regulators stepping up enforcement, employers and franchisors in the consumer sector face heightened scrutiny.

We unpack the key developments and practical steps organisations can take to strengthen compliance and manage their risk exposure.

What has changed?

The wage compliance landscape has evolved significantly in recent years, resulting in a number of important changes of which franchisors and employers must be aware. Employers are required to navigate a complex framework of obligations under the *Fair Work Act 2009* (Cth) (**FW Act**), applicable modern awards or enterprise agreements, annual wage review increases and other minimum employment standards.

Since 1 January 2025, intentional wage theft is a criminal offence. Employers face criminal liability for deliberate underpayments occurring on or after 1 January 2025, as well as conduct occurring before that date where it forms part of a broader pattern of intentional underpayment.

The Fair Work Ombudsman (**FWO**) now has the power to investigate and prosecute both companies and individuals for criminal wage theft offences, with penalties including significant monetary fines, imprisonment or both. Further, under the new provisions, companies (excluding small business employers) will be liable for significant civil penalties for underpayments. The amendments have substantially increased the consequences of non-compliance and heightened the level of vigilance employers must take in their wage reviews.

These risks are particularly acute for retailers, hospitality operators and franchised businesses, where multiple awards, penalty rates, allowances, junior rates, casual loadings, meal and rest breaks and frequently changing rosters can create significant payroll complexity.

Lessons from recent enforcement action

Australia has experienced several high-profile wage underpayment scandals, including more recently, Coles and Woolworths. Since the introduction of the new criminal offence, no prosecutions have been commenced but the FWO's enforcement activity makes clear that non-compliance remains a top regulatory priority.

In September 2023, The Royal Society for the Prevention of Cruelty to Animals (Queensland) Limited (**RSPCA Queensland**) self-reported wage underpayments and non-compliance to the FWO. On 18 June 2026, the FWO announced that RSPCA Queensland had entered into an enforceable undertaking to rectify the approximately $4.3m in underpayments owed to 1,008 staff, including interest and superannuation.

Fair Work Ombudsman, Anna Booth, said, *"The matter serves as a warning of the significant long-running problems that can result from an employer failing to have appropriate checks and balances to ensure workplace compliance. We expect employers to meet their legal obligations under their own enterprise agreements and any applicable awards."*

RSPCA Queensland's underpayments affected employees across a range of occupations, including administrative,

veterinary and retail roles, and involved both current and former employees working on a casual, part-time and full-time basis. The root causes were the misapplication of enterprise agreement provisions, the incorrect application of relevant award provisions and failures in annual leave calculations.

Wage compliance issues rarely resolve themselves. They must be proactively monitored and regularly reviewed, as waiting for a complaint or audit to surface problems is not a viable strategy.

Underpayment class actions: the ALDI settlement

On 23 October 2026, the Federal Court approved the settlement of an underpayment class action against ALDI Foods Pty Ltd (**ALDI**) in *Boi v Aldi Foods Pty Ltd* [2026] FCA 1576. The claims, brought on behalf of 32,308 current and former store and warehouse employees, alleged that ALDI failed to pay for work performed before rostered shifts and, for store employees, after them, including time that ALDI's time-keeping system automatically adjusted back to rostered start and finish times.

ALDI had already made voluntary payments of approximately $28.9m, but 16,378 group members had received no payment. ALDI's total liability, including those payments and interest, is estimated at approximately $55.2m, and ALDI settled without admitting liability. This illustrates that small, systemic payroll settings can create underpayment exposure across thousands of employees and a voluntary remediation program will not necessarily close out your risk.

Franchisors under the microscope

The Full Court of the Federal Court's decision in *Bakers Delight Holdings Ltd v Fair Work Ombudsman* [2025] FCAFC 144 has reinforced the heightened scrutiny and regulatory expectations that franchisors play an active role in the prevention of wage theft and workplace contraventions within their franchise networks.

The decision emphasises that compliance obligations cannot simply be delegated to franchisees. Franchisors are expected to maintain active oversight of workplace practices within their franchise networks and take proactive steps to identify, mitigate and respond to risks of non-compliance.

The decision

The FWO commenced proceedings against Bakers Delight Holdings Ltd (**Bakers Delight**) in relation to underpayments between July 2017 and October 2020 that arose from contraventions committed by the franchisee operating the stores.

The FWO sought to attribute accessorial liability to Bakers Delight as the 'responsible franchisor'. Under the FW Act, a franchisor may be liable for contraventions committed by a franchisee where the franchisor knew, or could reasonably have been expected to know, that contraventions were likely to occur.

A franchisor will not be liable if it can demonstrate that it took reasonable steps to prevent the contraventions or contraventions of a similar character.

The FWO argued that Bakers Delight became aware of wage underpayment issues through an audit process that had identified non-compliance within the franchisee's operations. Despite this, Bakers Delight failed to take adequate steps to prevent further contraventions from occurring.

The decision expands the practical compliance obligations expected of franchisors. Once a franchisor becomes aware of a risk of workplace non-compliance, passive oversight will be insufficient to adequately comply with the statutory scheme. Franchisors must actively monitor compliance, investigate potential breaches and take meaningful steps to address any issues identified.

Six steps to strengthen wage compliance

1. **Test payroll settings:** Regularly check classifications, rates, penalties, allowances, overtime, loadings, breaks and leave against applicable awards and enterprise agreements, particularly after annual wage or award changes.
2. **Conduct risk-based audits:** Compare payroll data and records with actual work practices, focusing on higher-risk roles, sites and workforce groups.
3. **Maintain records and reporting channels:** Keep accurate time, pay and entitlement records and provide a clear, confidential process for employees to raise concerns.
4. **Build capability and accountability:** Train payroll, HR, operational teams and franchisees, assign clear responsibility for compliance and escalate material issues appropriately.
5. **Strengthen franchise oversight:** Ensure franchise agreements support access to records, audits, remediation and escalation, backed by active, risk-based monitoring.
6. **Act promptly on issues:** Investigate suspected breaches, quantify and repay underpayments, address root causes and document the steps taken to prevent recurrence.

The regulatory environment is only tightening. Businesses that invest in proactive compliance frameworks, effective monitoring and early intervention will be best positioned to manage both legal exposure and reputational risk.



Retailers under pressure: Why tenant distress is increasing

By Alexandra Walker, Partner, Jasmina Bradonjic, Partner, Rob Hinton, Partner, William Doble, Associate, and Sebastien Butler, Graduate

Australian shopping centres, department stores and retail strips are feeling the strain. Retail insolvencies are now running about 50% above pre-COVID levels, with 871 in FY2024-25 and 1,006 in FY2025–26.[1]

Well-known names have not been spared. In 2026, long-standing retailers including Betts, Lincraft, A.H. Beard, Aussie Disposals and Barbeques Galore have faced administration, closure or wind-up.[2] Discretionary categories such as clothing, footwear, department stores and furniture are under the most pressure. Food and pharmacy retail have held up comparatively well.[3]

The stress is also showing up beyond companies. The Australian Financial Security Authority (**AFSA**) reported that personal insolvencies rose 13.1% in the June quarter 2026 compared with the June quarter 2025.[4] The AFSA reported 30.4% of personal insolvencies in the last five years were business-related.[5]

What is driving this? Inflation, higher cash rates and cost-of-living pressures have squeezed household spending.[6] Retailers are also paying more for wages, rent and energy, which is eroding their margins.[7] On top of these cyclical pressures, spending continues to shift online. Australians spent a record $21.9bn online in the June quarter 2026, up 14% year-on-year, with online now making up 25% of retail spending.[8]

For landlords, the warning signs are there. Business-to-business payment defaults are one of the clearest signs of tenant distress, including in retail trade.[9] CreditorWatch indicators suggest the pressure on retail tenants is unlikely to ease soon. Invoice payment defaults and ATO tax defaults, both leading indicators of future insolvency risk, are rising in the retail space.[10]

Spotting the warning signs before a default occurs

Rent arrears and concession requests

Rent is usually the first thing to change. Payments start arriving late or short. Some tenants fall into a cycle of clearing arrears, only for them to quickly build up again. That cycle can look reassuring, but it often signals an upcoming default.

The risk grows when a tenant pairs arrears with requests for rent relief, deferrals or a lease surrender. A liquidator may later point to these requests as reasonable grounds for suspecting the tenant was, or was about to become, insolvent.

Landlords should record each request and the reason for their response. That record will matter for the commercial decision and for any later unfair preference claim by a liquidator.

Trading and operational indicators of distress

Distress often shows up on the shop floor before it shows up in the rent ledger. Look out for:

- shorter trading hours or unexplained closures
- falling stock levels

1 ASIC Corporate Insolvency Update – Issue 40 – June 2026 | ASIC
2 Retail Bankruptcies, Administrations & Store Closures 2026 – A Running Market Watch by RetailOasis — RetailOasis
3 Retail insolvencies exceed preCovid levels, tipped to rise further this year - Inside Retail Australia
4 AFSA reports personal insolvencies up 13.1% in June quarter 2026 | Australian Financial Security Authority
5 Ibid.
6 Household spending stalls as cost pressures squeeze consumers
7 Rate hike hits retailers at worst possible time | Australian Retail Council
8 Colliers | AU | Online Spending Reaches New High as E-Commerce Fuels Growing Demand for Industrial Space
9 Australia's commercial property splits on office stress
10 Retail insolvencies exceed preCovid levels, tipped to rise further this year - Inside Retail Australia

- high staff turnover
- reduced or paused marketing activity
- complaints from suppliers or contractors
- failure to provide turnover statements when they are due.

If a tenant shares financial information, which the lease may require, read it closely. Profit and loss statements showing substantial losses are a major red flag.

Tenants with several sites need a wider view. A tenant may keep up under one lease while falling behind under another. Landlords should look across the tenant's whole portfolio, not just one premise for an accurate understanding.

Why does this matter? Spotting these signs early gives both parties the best chance of a negotiated outcome. It also lets landlords manage their own insolvency exposure, rather than scramble after an appointment has been made.

Enforcement considerations and commercial strategies

If a tenant enters liquidation, the liquidator can claw back earlier transactions that are considered unfair preference payments.[11] How a landlord responds to a distressed tenant can determine whether it later faces an unfair preference claim. Landlords should weigh that risk against other commercial factors, such as the length and value of their relationship with the tenant.

The High Court in the case of *Bryant v Badenoch Integrated Logging Pty Ltd*[12] found that, in circumstances where a landlord allows a tenant to keep trading while arrears build, it may have no unfair preference exposure at all. This is because allowing the company to keep trading could be considered a benefit for all creditors. This is colloquially known as the 'landlord's defence'. It is not a complete defence and should be considered on a case-by-case basis.

In practice, landlords should:

- document the commercial reasons for any concession provided to tenants
- avoid demanding lump-sum payments of arrears shortly before a likely appointment
- watch the tenant's position across all of its leases in the centre
- take advice before accepting a surrender or a payment plan.

Tenants also have a role to play. A tenant that wants to preserve its relationship with the landlord during a period of financial hardship should start negotiations early. The tenant should also provide full financial information and consider formal restructuring options before arrears become unmanageable. A negotiated outcome often preserves more value for both parties than enforcement or liquidation.

What happens when a tenant enters formal insolvency?

Once a tenant enters a formal insolvency process under the *Corporations Act 2001* (Cth) (**Corporations Act**), the appointment can curtail the landlord's usual remedies.

Landlords who understand how each process works are best placed to protect their position.

Receivership

A secured creditor, usually the tenant's financier, may appoint a receiver to realise its security. The receiver will often aim to sell the business as a going concern. Landlords generally retain their right to enforce. However, a landlord may be unable to terminate the lease solely because of the appointment (**ipso facto stay**).

A receiver who uses or occupies leased premises becomes personally liable for rent accruing from seven days after appointment. The receiver can avoid this by giving notice within that period that they do not intend to use or occupy the premises. The landlord would then usually take possession.

A receiver acts primarily in the secured creditor's interests. Landlords should engage early on whether any sale includes the premises and whether the buyer will take an assignment of the lease.

Voluntary administration

Voluntary administration (**VA**) gives a company breathing space. A statutory moratorium prevents landlords from re-entering premises or recovering property used by the tenant without the administrator's consent or the Court's leave (**Moratorium**).

The Ipso Facto Stay also applies and generally prevents a landlord from terminating the lease solely because the tenant has entered administration.

Administrators become personally liable for rent accruing from five business days after their appointment. They can avoid this by giving notice within that period that they do not propose to exercise rights in the premises.

Where a company has multiple stores, administrators will often decide early which stores to keep trading and which to vacate. David Jones is a timely example. After 188 years of trading, the department store entered voluntary administration in November 2026. The administrators have said the business will keep trading while it is restructured, but they are expected to close some unprofitable stores while they look for a buyer. For David Jones' landlords, the five-business-day window and the administrators' review of the store network will largely decide what happens next for each store.

A VA can end with a deed of company arrangement (**DOCA**), which may bind landlords in respect of unsecured claims, including rent arrears and may compromise those claims for a fraction of their value.

Liquidation

A liquidator may disclaim the lease as 'onerous property'. The landlord can then prove in the winding up for its loss, but as an unsecured creditor it may recover little. If a liquidator continues to occupy the premises for liquidation, rent for that period may be payable as a liquidation expense.

11 Note that a liquidator could seek to claw back payments made by a tenant during the relation back period as an unfair preference under section 588FA of the *Corporations Act 2001* (Cth). The relation-back period is the six month period from which a liquidator or bankruptcy trustee measures for examining, and potentially recovering, voidable transactions entered into before a company went into external administration.

12 *Bryant v Badenoch Integrated Logging Pty Ltd* [2023] HCA 2 at [70].

Process	Control	Landlord enforcement	Rent liability	Immediate action
Receivership	Receiver	Generally retained, subject to the ipso facto stay	Usually from seven days after appointment if occupying	Confirm whether the premises are required for a sale
Voluntary administration	Administrator	Moratorium and ipso facto restrictions apply	Usually from five business days after appointment	Engage early and review any notice concerning occupation
Liquidation	Liquidator	Lease may be disclaimed	Occupation rent may be an expense	Lodge proof of debt and assess security

Key implications for landlords

Security is critical. The Moratorium generally does not affect bank guarantees and landlords can usually call them on promptly, provided the right to call is based on an existing default, such as unpaid rent, rather than solely on the tenant entering administration. If the only trigger is the appointment, the Ipso Facto Stay may prevent the call. This makes bank guarantees the most reliable protection. Landlords may also apply security deposits they hold in line with the lease. By contrast, a landlord generally cannot enforce a director's personal guarantee during a VA.

Landlords should act quickly upon the occurrence of any of the above formal appointments and complete the following:

- review the lease and security (including the location of any bank guarantee)
- engage early with the administrator, receiver or liquidator about its intentions for the premises
- keep accurate records of rent accruing after appointment
- lodge proofs of debt on time.

Early engagement often puts landlords in the best position to negotiate a lease assignment, a surrender or new terms with a buyer of the business.

Experts



Adam Walker
Partner
+61 3 9252 2515
+61 419 132 932
adam.walker@gadens.com



Alexandra Walker
Partner
+61 3 9252 2507
+61 417 120 414
alexandra.walker@gadens.com



Breanna Davies
Partner
+61 2 9163 3017
+61 414 581 209
breanna.davies@gadens.com



David Fleming
Partner
+61 2 8349 3684
+61 419 347 740
david.fleming@gadens.com



Jasmina Bradonjic
Partner
+61 3 9612 8205
+61 458 072 658
jasmina.bradonjic@gadens.com



Jonathon Hadley
Partner
+61 7 3231 1653
+61 411 465 515
jonathon.hadley@gadens.com



Kiri Jervis
Partner
+61 2 8349 3613
+61 414 883 719
kiri.jervis@gadens.com



Lara Cresser
Partner
+61 7 3231 1549
+61 491 052 933
lara.cresser@gadens.com



Marina Olsen
Partner
+61 2 8349 3608
+61 420 939 339
marina.olsen@gadens.com



Rob Hinton
Partner
+61 3 9252 2531
+61 416 044 822
rob.hinton@gadens.com



Sinead Lynch
Partner
+61 2 9163 3064
+61 499 700 603
sinead.lynch@gadens.com



Lisa Haywood
Special Counsel
+61 3 9612 8455
lisa.haywood@gadens.com

With special thanks to our other contributors

Senior Associates: Annika Dunlop, Brittany Dorney

Associates: Emily Woolmer, Shania Amolik, William Doble

Lawyers: Kalarni Orr

Graduates: Bailey Joffe, Eva Zofrea, Isabella O'Gorman, Phoebe Ralston, Sebastien Butler, Tess Nossal

Editorial:
Ailsa Pender, Senior Manager – Brand and Communications
Claus Huttenrauch, Graphic Designer
Heather Homan, Marketing and Communications Advisor
Lucia Sheridan, Marketing and Communications Manager
Melanie Tapper, Business Development Advisor

Office Locations

Adelaide
Level 1
333 King William Street
Adelaide SA 5000
+61 8 8456 2433

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

Canberra
Level 1
55 Wentworth Avenue
Kingston ACT 2604
+61 2 6163 5050

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

Perth
Level 27, Palace Tower
108 St Georges Terrace
Perth WA 6000
+61 8 6317 6500

Sydney
Level 29
8 Chifley Square
Sydney NSW 2000
+61 2 9231 4996

gadens.com