# Australian regulators tackle misleading claims, conflicted remuneration and emerging cybersecurity risks



The Australian securities and consumer regulatory landscape has recently seen several significant enforcement actions and judicial interventions addressing misleading conduct, conflicted remuneration, corporate governance disputes, and emerging cybersecurity risks in the corporate sector.

On 17 April 2025, the Australian Securities and Investments Commission (ASIC) issued infringement notices totalling $37,560 to Chapter Two Holdings Pty Ltd, a debt management company. ASIC alleged that Chapter Two made misleading claims on its website stating it had wiped $80 million in debt and saved consumers $30 million in interest. These figures were found to be either false or lacking substantiation. The move demonstrates ASIC’s ongoing commitment to ensuring financial services firms provide accurate representations to consumers regarding their services.

A more substantial penalty was imposed by the Federal Court of Australia on 24 April 2025, when DOD Bookkeeping Pty Ltd was ordered to pay $11 million for breaching conflicted remuneration rules. The Court found that DOD’s financial advisers repeatedly engaged in "cookie-cutter" advice, encouraging clients to roll over their superannuation funds into self-managed superannuation funds (SMSFs) and purchase property through an entity related to DOD Bookkeeping. Significantly, the advisers’ recommendations were influenced by bonuses paid contingent on clients settling on properties from the related entity, constituting a clear breach of conflicted remuneration laws. ASIC Deputy Chair Sarah Court highlighted to media that misconduct exploiting superannuation funds is a key enforcement priority and noted that “the size of the penalty demonstrates the seriousness of the misconduct,” which the Court described as “plainly deliberate and extended over a period of several years”.

In parallel, the Australian Competition and Consumer Commission (ACCC) commenced proceedings on 23 April 2025 against Ateco Automotive Pty Ltd, trading as LDV Automotive Australia (LDV), for alleged misleading advertising under the Australian Consumer Law. The ACCC alleges LDV made unsubstantiated claims about the durability and suitability of certain vehicle models, asserting these vehicles were notably tough and appropriate for off-road conditions despite having a tendency to rust or corrode within five years of manufacture. Of particular concern were claims associated with a 10-year anti-corrosion warranty, which LDV purportedly used to reassure consumers that the vehicles did not have material corrosion risks during the warranty period. The ACCC contends that LDV had no reasonable basis for these representations. The ACCC emphasised the importance of truthful marketing to enable consumers to make informed decisions and underscored the role non-executive directors must play in ensuring marketing accuracy to avoid regulatory scrutiny and uphold consumer trust.

Turning to corporate governance, the Supreme Court of New South Wales intervened on 17 April 2025 in a board deadlock involving Heartland Group Pty Ltd. The deadlock arose when Bernley Corporation Pty Ltd, the majority shareholder, resolved—with one director dissenting—to hold a general meeting proposing to remove the dissenting director, Mr Turner, from Heartland’s board and appoint a replacement. The minority shareholder, Boyded Industries Pty Ltd, which had two directors including Mr Turner, experienced its board become deadlocked and unable to appoint a corporate representative to attend the meeting. Since the Heartland constitution required two members to constitute a quorum and Boyded failed to send a representative, the meeting was effectively stalled. The Court, invoking sections 249G and 1319 of the Corporations Act 2001 (Cth), ordered that a corporate representative of Bernley be considered a quorum member, thus enabling the general meeting to proceed even without Boyded’s representative. This ruling confirms the Court’s readiness to step in when procedural hurdles are employed to frustrate majority shareholder rights and demonstrates judicial support to resolve corporate impasses where deadlocks threaten governance processes.

On the frontier of corporate control, the Takeovers Panel declined on 17 April 2025 to initiate proceedings on an application by Emu NL regarding alleged shareholder associations aiming for board control during a requisitioned spill meeting. The Panel found insufficient evidence to warrant further inquiry. Subsequently, on 23 April 2025, Emu lodged an application seeking review of the Panel’s decision, with the Panel President consenting to the review application; however, a review Panel had yet to be constituted and no determination made on whether proceedings would proceed.

The issue of emerging cyber threats also featured prominently in regulatory comments. On 22 April 2025, ASIC’s corporate finance update highlighted the increasing use of deepfake technology in sophisticated corporate fraud, emphasising the vulnerabilities presented by artificial intelligence-generated audio and video impersonations. ASIC cited two notable examples: a UK energy firm lost $243,000 in 2019 after a finance director was deceived by a deepfake audio of the CEO’s voice; and in 2024, a Hong Kong company incurred a $25 million loss after a senior executive was targeted through a combination of deepfake audio and compromised emails. ASIC’s update warned directors about the instinctive trust in familiar voices and the pressing need to implement robust cyber resilience frameworks that can adapt to these evolving threats. The regulator stressed that, given the increasing sophistication of deepfake technology, “robust verification processes – not assumptions – are key to mitigating risk.”

These recent enforcement and judicial developments underscore the multifaceted challenges currently confronting Australian businesses—from ensuring truthful disclosures and compliance with remuneration laws, to maintaining effective corporate governance and addressing high-tech cyber fraud risks within an increasingly digital business environment.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://asic.gov.au/about-asic/news-centre/> - This URL provides access to ASIC's news centre, which includes updates on enforcement actions and priorities that align with the article’s focus on consumer protection and financial service regulation.
2. <https://www.accc.gov.au/contact-us> - Although not specific to the ACCC’s proceedings against LDV, this URL links to the ACCC’s main contact page, where information on consumer protection and misleading advertising actions can be found.
3. <https://piperalderman.com.au/insight/2025-asic-enforcement-priorities/> - This URL supports the aspect of ASIC’s enforcement priorities, particularly highlighting the focus on superannuation misconduct, which aligns with the discussion of DOD Bookkeeping’s breach of conflicted remuneration rules.
4. <https://asic.gov.au/about-asic/asic-investigations-and-enforcement/asic-enforcement-priorities/> - This page lists ASIC’s enforcement priorities for 2025, which include misconduct exploiting superannuation savings and other areas relevant to the article’s discussion on consumer financial protection.
5. <https://www.bund_chan.vicbar.com.au/corporate-governance> - This URL is not directly related to the specific case mentioned but generally relates to corporate governance issues, such as board deadlocks, which are relevant to the Heartland Group discussion.
6. <https://www.takeovers-panel.gov.au> - This is the main website for the Takeovers Panel, where information on decisions regarding shareholder associations and board control issues can be found, aligning with the article’s mention of the Emu NL case.
7. <https://news.google.com/rss/articles/CBMihgFBVV95cUxOaS1ESGZHMFgzZERVNHJnM0pRZkJQRDVuY2pZbFdkYk5hZXlDeHVKOC1qUW9KYjl0eDZjNnJMODI4M3lfTFdpZmR3Y1Fvbl9YTlIzQVdDNDdPa2JCOWlnQkF3Vk91dVc0Tmp0Y2N6cjYxc3pkaWFNMDdrU09GU2Q0MFNoc3YtQQ?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data