

18 September 2026

To: Attorney-General's Department
Via online consultation portal



Dear Sir/Madam

Submission on the Privacy Reform Consultation Paper and exposure draft of the *Privacy Amendment (Personal Data Protection) Bill 2026*

The Australian Financial Markets Association (**AFMA**) represents over 140 leading financial market participants, including banks, international banks, brokers, government treasury corporations, super funds, asset managers, energy firms and market infrastructure providers. AFMA's core objective is to promote efficiency, integrity and professionalism in Australia's financial markets.

AFMA makes this submission in response to the Exposure Draft of the *Privacy Amendment (Personal Data Protection) Bill 2026 (Exposure Draft)* and the accompanying Consultation Paper released on 31 August 2026. AFMA is broadly supportive of modernising Australia's privacy framework but considers that further refinement is needed to ensure the reforms operate effectively. This submission consolidates members feedback and outlines our key observations and recommendations.

1. Information sharing for fraud prevention and market integrity

AFMA members strongly support the broader move towards facilitating information sharing where necessary to prevent fraud and other forms of investor or financial harm. Members are particularly supportive of the expansion of the existing exception from "misconduct" to "wrongdoing", the clarification that wrongdoing can involve both internal and external actors, and the enhanced ability to undertake proactive monitoring and information sharing.

The financial markets have established a Share Fraud Working Group, which coordinates cross-firm efforts to identify and disrupt share fraud. Members consider the proposed reforms, including the expanded permitted general situation (PGS) 2 and the new fair and reasonable test, would provide a clearer legal basis for such sharing.

Recommendation 1: AFMA recommends that the OAIC confirm, through published guidance, that the "connection to the entity's functions or activities" factor under proposed APP 3.2 supports the collection, use and disclosure of personal information for fraud prevention, market integrity and investor protection purposes, recognising that these are core regulatory functions of financial market participants. The guidance should also confirm that the expanded PGS 2 provides a clear legal basis for proactive monitoring and cross-firm information sharing to detect and disrupt wrongdoing, and that the consequences of not sharing information (including potential ongoing fraud and investor harm) are a relevant contextual consideration in assessing whether disclosure is reasonable in the circumstances. Further, the inclusion of "precise geolocation tracking data" in the definition of sensitive information will impose significant limitations on fraud and scam prevention activities that rely on location data to detect suspicious activity. PGS 2 should be updated to permit the collection,

use and disclosure of personal information, including sensitive information such as geolocation data, for pre-emptive security measures without requiring the consent of the relevant individual.

Definitional and scope concerns

(a) Trading of personal information

The proposed definition of "trading" personal information may inadvertently capture a range of ordinary business activities common in wholesale financial markets, including referrals between business units, information sharing between affiliated entities and within global financial groups, cross-selling and servicing arrangements, and data-sharing arrangements that support client servicing or business operations.

Recommendation 2: The trading provisions should expressly exclude legitimate operational information flows. In particular: (i) an exception should be included for intra-group and multinational group transfers occurring pursuant to appropriate contractual protections; the existing carve-out in proposed section 6FC(2)(a) should be expanded to include marketing-related information that the individual has requested from the recipient; and (iii) the limitation in section 6FC(3)(a)(i) and (ii) restricting the unlawful activity and serious wrongdoing exceptions to fraud should be removed, as information sharing to address other forms of serious wrongdoing (such as scams, money laundering and sanctions evasion) should not be characterised as "trading" personal information.

(b) AI-generated inferences and the expanded definition of personal information

The proposed reforms expand the concept of personal information to include certain AI-generated inferences. This raises significant operational questions, including whether inferences constitute personal information in their own right, how consent requirements operate where an inference has not yet been generated, and whether privacy obligations extend to model outputs and conclusions. More broadly, it is unclear how organisations should manage compliance obligations where information previously outside scope is subsequently drawn in by technological developments, or how traditional consent mechanisms can operate where AI-generated outputs are not foreseeable at the point of collection.

Recommendation 3: AFMA recommends that the reforms be accompanied by comprehensive guidance on how privacy obligations are intended to operate across the AI lifecycle, including on the application of the fair and reasonable test, notice and transparency obligations, and consent requirements in technology-enabled environments.

(c) Scope of the right to erasure

The proposed definition of "large digital platform" in section 6EB(1) is likely to extend well beyond the major consumer-facing online platforms the reform appears to target. The definition draws on broad categories of digital services (including designated internet services) and applies a \$500 million group-revenue threshold on a disjunctive basis, meaning many financial institutions with an ordinary online presence will be captured regardless of whether they operate a consumer-facing platform.

Recommendation 4: The definition of "large digital platform" should be amended so that an organisation must satisfy *both* the gross revenue test and the end user threshold test in proposed section 6EB, and the right to erasure should exclude platforms that are predominantly business-to-business.

AFMA further recommends that regulated financial services entities be excluded from the scope of the proposed right to erasure. Financial institutions appear capable of being captured as an unintended consequence of the large digital platform definition, despite being subject to extensive sector-specific regulation and record-keeping obligations.

If financial services entities remain in scope, the legislation and accompanying guidance should make clear that the right to erasure does not override obligations to retain information under other legal, regulatory, court-ordered or investigative requirements, and should permit additional industry-specific exceptions where appropriate.

2. Overseas data transfers and permitted general situations

The proposed amendments to PGS 4, 5 and 10, which restrict disclosures to non-overseas recipients, create a significant practical gap for multinational financial institutions. Financial institutions routinely need to disclose personal information to overseas recipients for purposes including legal claims, alternative dispute resolution and intra-group legal functions. These restrictions could undermine the ability of Australian entities to effectively manage cross-border legal and operational risks.

Recommendation 5: PGS 4, 5 and 10 should be expanded to permit overseas disclosures where the other requirements of those PGS items are met. The Government should also exercise its existing power to prescribe whitelisted countries providing substantially similar privacy protections, and consideration should be given to introducing an Australian equivalent to the GDPR's Standard Contractual Clauses.

3. 72-hour data breach notification

While AFMA supports alignment with international standards, the hard 72-hour notification deadline raises practical concerns for financial institutions managing complex incidents where forensic investigations remain ongoing. In particular, the requirement under proposed subsection 26WK(5) to explain why a statement is incomplete within the 72-hour window imposes an unnecessary additional burden during the critical early stages of an incident response, when resources should be focussed on containment.

Recommendation 6: Proposed subsection 26WK(5)(b)(iii), requiring entities to set out the reasons why it is impossible or impracticable to provide a complete statement, should be removed. The threshold for incomplete reporting in subsection 26WK(5)(a) should be aligned with the GDPR standard of "not reasonably possible", and the period for notifying the OAIC should be decoupled from the period for notifying affected individuals.

4. Implementation regulatory interaction and transition

Given the scale and complexity of the proposed reforms, including the retrospective application of the expanded personal information definition to existing datasets, implementation will require considerable time and investment. Organisations will need to re-assess existing data holdings, renegotiate contractual arrangements with third parties, review outsourcing and technology service arrangements under the new controller/processor framework, and uplift internal processes and governance frameworks.

AFMA also recommends that the OAIC publish comprehensive guidance on the interaction between the Privacy Act and other regulatory frameworks applicable to financial institutions, particularly where

obligations arise from regulatory guidance or industry standards rather than statute. While proposed APP 3.3(a) exempts conduct required or authorised by Australian law from the fair and reasonable test, many financial sector obligations arise from “soft law”, such as APRA or ASIC guidance, and the interaction between these and the proposed reforms requires clarification.

Recommendation 7: The implementation period should be no less than 24 months, and the OAIC should issue practical guidance on the interaction between the reformed Privacy Act and existing regulatory obligations, including those arising from regulatory guidance and industry standards.

Next steps

AFMA and its members would welcome further discussion on the content, observations or recommendations made in this submission. Please contact Jodie Maurer (jmaurer@afma.com.au)

Yours sincerely,

Jodie Maurer

Jodie Maurer

Australian Financial Markets Association