



FinTech Australia

Consultation on Guidance for Transparency in Automated Decision Making

June 2026

About this Submission

This document was created by FinTech Australia in consultation with its members.

In developing this submission, interested members of the industry participated in meetings to discuss key issues and provided feedback to inform our response to the [Office of the Australian Information Commissioner \(OAIC\)'s Automated Decision-Making \(ADM\) Transparency Obligation \(APP 1\) Issues Paper](#) (**ADM Issues Paper**).

FinTech Australia and its members particularly acknowledge the support and contribution of our policy partner, DLA Piper, to the topics explored and developed in this submission.

About FinTech Australia

FinTech Australia is the peak industry body representing the Australian financial technology sector, with a membership of more than 400 companies and startups nationwide. Our members span the full breadth of the fintech ecosystem, including payments, consumer and business lending, artificial intelligence, wealthtech, regtech, neobanking, open banking, digital assets, distributed ledger technologies, DeFi, and Web3. The fintech industry delivers a wide range of business-to-business and business-to-consumer financial products and services that support the smooth operation of the Australian economy.

Our vision is to position Australia as one of the world's leading markets for fintech innovation and investment. This submission has been compiled by FinTech Australia and its members in an effort to advance public debate and drive cultural, policy and regulatory change toward realising this vision, for the benefit of the Australian public.

FinTech Australia would like to recognise the support of our policy partners, who assist in the development of our submissions:

- Allens;
- Ashurst
- DLA Piper;
- Gagens;
- Mallesons; and
- K&L Gates.

Summary and Key Recommendations

Introduction

FinTech Australia welcomes the opportunity to make a submission to the OAIC regarding its proposed regulatory guidance for the purpose of Australian Privacy Principles (**APPs**) 1.7 – 1.9 (**ADM Guidance**). We set out below our comments on the ADM Issues Paper.

Executive Summary

FinTech Australia and its members support the ongoing development of a technology neutral and fit for purpose privacy regime in Australia. This includes ensuring that individuals are transparently informed of the use of automated decision-making processes that may significantly affect their rights and interests, so that they can make informed choices about the use of relevant products and services.

FinTech Australia recognises the importance of building and maintaining public trust in digital services and its members are committed to responsible and transparent deployment of technology in their operations. At the same time, FinTech Australia is keen to ensure that the OAIC's ADM Guidance is clear, proportionate, and allows fintech businesses to apply APPs 1.7 – 1.9 in a practical, consistent and operationally efficient manner.

Some of the specific issues raised in the ADM Issues Paper are discussed below, in the Detailed Response. By way of summary, the following key themes emerged from the consultation with our members.

Clarity and consistency: As a sector with high usage of artificial intelligence (**AI**) and ADM tools, our members want clear guardrails to be imposed regarding the extent of the disclosure requirements. ADM tools are deployed by and on behalf of fintechs for a broad range of functions across complex digital ecosystems, including customer-facing, internal operational and decision-support use cases, and, as drafted, the requirements under APP 1.7 to 1.9 may capture a wide spectrum of use cases. Without clear guidance, the extent of the required disclosures may be difficult to assess and could lead to inconsistent practices across or within sectors. This could have the unintended consequence

of penalising APP entities which choose to make more expansive disclosures than their competitors, by making their data processing practices appear to be more intrusive.

Alignment with global frameworks: Equivalent requirements for ADM disclosures exist in other data protection regimes which many of our members are subject to. This includes Articles 13 and 14 of the General Data Protection Regulations (**GDPR**), which requires meaningful information to be provided about the logic involved in ADM, as well as the significance and the envisaged consequences of such processing for the data subject. Relevantly, amendments to the California Consumer Protection Act (**CCPA**) which took effect on 1 January 2026 introduce various rights and obligations with respect to use of Automated Decision-Making Technology (**ADMT**) which are referred to throughout this submission. The ADM Guidance should, to the extent possible within the confines of APPs 1.7 – 1.9, allow businesses operating across multiple jurisdictions to develop consistent disclosures regarding the use of ADM/ADMT.

Balancing transparency with granularity: Members are conscious that a high degree of granularity could result in the disclosure of operationally or commercially sensitive information, or be disproportionately resource intensive. Excessive transparency about a fintech's use of ADM may:

- expose the existence of ADM used for anti-fraud, compliance or investigative processes, undermining tools which are covert by design;
- disclose proprietary methodologies (for example, credit assessment models) that are not intended to be public and would jeopardise commercial-in-confidence classifications; and
- create ongoing administrative overheads, given the dynamic nature of AI/ADM systems and the need for frequent updates to ensure continued accuracy.

The ADM Guidance should confirm that APP entities are not required to disclose information about fraud detection, scams prevention, AML/CTF controls, cybersecurity controls or credit risk decisioning where doing so would compromise system integrity, enable reverse engineering, increase fraud or scam risk, or disclose commercially sensitive or proprietary information. The guidance should also confirm that entities may describe categories of automated decisions, such as credit assessment, transaction monitoring, identity verification or fraud detection, rather than disclosing details of specific models, tools, rules or thresholds.

Proportionality: The effort involved in identifying and documenting all relevant ADM use cases across an organisation, particularly within global businesses with complex supply chains, should not

be underestimated. Whilst some visibility is necessary as part of a mature AI governance framework, some businesses may find this process challenging and resource-intensive, particularly given the scale and dynamism of AI/ADM implementation. The ADM Guidance should acknowledge this reality and provide clear guidance on the level of effort which should be expended to identify additional ADM use cases.

Risk-based and practical implementation: Members would also welcome guidance that recognises the different risk profiles of ADM use cases. Customer-facing ADM that directly affects access to financial products or services may warrant more specific disclosure than internal operational uses, such as transaction monitoring, fraud controls, AML/CTF screening, cybersecurity, complaints triage or back-office workflow tools. The ADM Guidance should make clear how entities can adopt risk-based, category-level disclosures that provide meaningful information to individuals without requiring technical detail that could undermine consumer protection, system integrity or operational security.

The following recommendations summarise the key areas where FinTech Australia considers the ADM Guidance would benefit from further clarity.

List of recommendations

As the OAIC develops the ADM Guidance, FinTech Australia recommends that the OAIC consider the following:

1. **Guidance on key statutory concepts**, specifically:
 - A non-exhaustive list of the types of "decisions that may affect the rights or interests of an individual";
 - A non-exhaustive list of "things done" by a computer program which are considered "substantially and directly related to making a decision";
 - Clarification that assessment of whether a decision "significantly affects an individuals' rights and interests" should be conducted objectively, based on knowledge reasonably available to the entity at the time the decision is made; and
 - Clarification of when a decision is considered to be "substantially" automated, including the degree of human involvement required to fall below this threshold;
 - guidance on how "substantially and directly related" applies where automated tools are used at multiple points in a broader decision-making process;

- guidance on whether automated reminders, tips, prompts, nudges or in-product messages fall within scope where they influence, but do not determine, a decision ultimately made by the individual affected; and
- more worked examples showing how APPs 1.7 to 1.9 apply in common financial services and fintech contexts, including onboarding, identity verification, credit assessment, transaction monitoring, fraud and scams detection, AML/CTF controls, customer eligibility assessments and hardship processes.

2. Clear boundaries on transparency obligations, specifically:

- a clear statement that entities are not required to disclose commercially sensitive, proprietary or security-related information, including details of ADM processes used in connection with AML/CTF obligations, fraud and scams detection, credit risk decisioning, cybersecurity controls or proprietary algorithmic models, where disclosure could reasonably prejudice the entity's commercial interests, compromise system integrity, enable reverse engineering, increase fraud or scam risk, or undermine the effectiveness of such systems;
- confirmation that APP entities may use category-level disclosures, rather than model-by-model or tool-by-tool disclosures, where this provides meaningful information about the kinds of personal information used and the kinds of decisions made or materially assisted by ADM;
- explicit treatment of risk-based disclosures, including how the level of disclosure may vary depending on the nature of the decision, the likely impact on individuals, the sensitivity of the information used, and whether the ADM use is customer-facing or internal and operational; and
- Acknowledgement of the practical difficulties associated with documenting ADM use cases, to allow for flexibility in the manner and level of aggregation across disclosures.

3. Guidance on operational and technical use cases, specifically:

- distinction between customer-facing ADM and internal operational ADM, with guidance recognising the importance of internal systems used for fraud detection, scams prevention, AML/CTF compliance, cybersecurity, transaction monitoring, risk controls, complaints triage and other operational processes;
- clarification of how the ADM obligation applies to continuously-learning AI systems, including the level of detail required in privacy policies where models, rules, weights, thresholds or outputs may change over time; and

- guidance confirming that privacy policy disclosures may describe the relevant categories of ADM and personal information at an appropriate level of generality, rather than requiring entities to update privacy policies for every model refinement, system update or operational change.

4. **Guidance on third-party and supply chain arrangements:**

- Clarification of the circumstances in which an entity which obtains the benefit of a third-party ADM tool is considered to have "arranged for" the decision, distinguishing between scenarios where: (i) the entity instructs or commissions a vendor to use ADM on its behalf, and (ii) the entity procures a service which the vendor uses ADM to deliver;
- A non-exhaustive list of reasonable steps entities should take to obtain visibility into the use of ADM within their supply chain and, where full information is not available, what level of assumption is acceptable;
- guidance confirming that an APP entity should be taken to have taken reasonable steps where it undertakes reasonable enquiries of suppliers and relies in good faith on information provided by those suppliers; and
- Targeted guidance directed at providers of ADM tools, encouraging provision of sufficient information to enable their customers to meet the transparency obligations.

Detailed Response

1. **Meaning of 'computer program'**

Members do not have specific views on the meaning of "computer program" and do not consider that detailed consideration of this topic is necessary in the ADM Guidance. Members acknowledge that the concept of "computer program" is intended to be defined broadly in order to capture a wide range of technologies, as well as the diverse ways in which such technologies can and will be used (as noted in the various examples relating to Microsoft Excel functionality in the ADM Issues Paper).

It is worth noting that the CCPA approaches the threshold question differently. Rather than focusing on whether a "decision" has been made (or how that decision should be characterised), the CCPA focuses on the nature of the technology – namely, whether it amounts to ADMT. ADMT is defined as technology which processes personal information and uses computation to replace, or substantially replace, human decision-making (and the concept of a replacement or substantial replacement of

human decision-making is separately defined in the CCPA). If the technology is classed as ADMT, its outputs are prima facie captured by the disclosure requirements in the CCPA. The CCPA also expressly excludes certain functions, such as spellchecking, calculators, databases and spreadsheets where they do not replace human decision-making, from the scope of ADMT.

FinTech Australia requests that the ADM Guidance ought to take a similar approach and expressly exclude basic software tools that are unlikely to be used for ADM.

2. 'Substantially and directly related to making a decision'

FinTech Australia seeks further clarity from the OAIC on interpretation of the phrase "substantially and directly related to making a decision", noting that this represents one of the key threshold tests in APP 1.7.

Members raised a particular concern as to the classification of ADM tools used at multiple points within a single decision-making process. In some operations, a computer program may contribute at several stages, with each individual usage not necessarily meeting the "substantial and direct" threshold in isolation. When viewed in totality, however, the aggregate contribution of the ADM tool to the ultimate decision may be direct and substantial. Accordingly, FinTech Australia seeks guidance on whether the "substantially and directly related" test should be assessed on an aggregate basis across the entirety of a decision-making process, or whether each discrete use of the tool must independently satisfy the threshold.

Members also seek guidance on whether APPs 1.7 to 1.9 apply where a computer program contributes to decision-making, but the ultimate decision is made by the individual affected. For example, fintech products may use automated reminders, tips, prompts, nudges or in-product messages to support a customer's own decision-making, such as whether to make a repayment, review spending, change a product setting or take up an optional feature. In these cases, the individual retains final control over the decision. The ADM Guidance should clarify when these types of automated prompts are merely informational or supportive, and when they may become sufficiently substantial and direct to fall within the ADM transparency obligation.

Members also seek clarity on how "directly" applies in multi-stage decision-making processes. In particular, guidance should address whether "directly" refers only to an automated output that immediately precedes a human decision, or whether it may also capture earlier automated steps

that are causally connected to the final outcome because they constrain, filter or shape the decision pathway available to the human decision-maker.

Separately, members further queried the threshold at which the level of human involvement in a process before an ADM tool to fall below the "substantially related" threshold. For example, where a computer program informs or is used throughout a decision-making process, but a human makes the final determination, clarity is needed as to whether the use of the tool at various stages should be aggregated and assessed holistically.

Comparable frameworks may provide useful guidance. Under the amended CCPA regulations, "substantially replace human decision-making" is defined by reference to whether a business uses the technology's output to make a decision without human involvement. Human involvement, in turn, requires the reviewer to:

- know how to interpret and use the technology's output;
- review and analyse the output and other relevant information; and
- have authority to make or change the decision based on their analysis.

FinTech Australia members consider that the level of CCPA's clarity regarding the scope of "human involvement" provides greater certainty. The ADM Guidance would benefit from similarly practical guidance on when human involvement is sufficient to mean that a computer program is not substantially and directly related to making the relevant decision.

3. Meaning of 'significantly affect rights or interests'

FinTech Australia supports a prescriptive approach to interpreting which decisions "significantly affect rights or interests" of data subjects. This aspect of the ADM Guidance should provide clear, categorical guidance to businesses, removing the need to rely on case-by-case assessments and reducing the potential for inconsistent interpretation of this limb.

The ADM Guidance should list the types of decisions considered to "significantly affect rights or interests", such that decisions falling into these categories would de facto be presumed to fall within the threshold for disclosure. It would be appropriate to base this list on the examples listed within question 6 of the ADM Issues Paper (e.g. "access to essential utilities, telecommunications, educational services, and essential banking and credit services"). This approach would enable

businesses to focus resources on use cases that clearly have a significant effect on the rights and interests of individuals, rather than expending effort assessing marginal or "edge" cases.

This is similar to the approach taken under the CCPA, which defines a "significant decision" as a decision which *"provision or denial of financial or lending services, housing, education enrolment or opportunities, employment or independent contracting opportunities or compensation, or healthcare services"*.

Of course, the ADM Guidance can note that these examples are non-exhaustive, and that other types of decisions may be captured by exception.

Whilst formation of a contract may have an impact on the rights and interests of the counterparties, it would be excessive if disclosure is required for every automated decision associated with a commercial transaction. The ADM Guidance should assist APP entities in distinguishing between decisions which genuinely affect a person's substantive rights and interests, and those that are merely incidental to ordinary commercial activity.

Members also queried the factors listed in question 4 of the ADM Issues Paper. The ADM Guidance should clarify that "vulnerability" must be assessed objectively, based on the knowledge reasonably available to the entity at the time of the decision. Unless a fintech routinely interacts with "vulnerable" cohorts (such as children or individuals with disability), an entity cannot reasonably be expected to know the circumstances affecting an individual such that certain decisions (for example, denial of a pricing credit) would have a disproportionate impact on them relative to others.

4. Meaning of 'making a decision'

FinTech Australia generally considers the concept of "making a decision" to be relatively straightforward. In most instances, it ought to be clear that a certain decision has been made (for example, the decision to display a job advertisement to a particular candidate, per Fictional Edge Case: Discriminatory Targeted Job Ad in the ADM Issues Paper). The less certain aspect tends to be whether that decision meets the other thresholds for disclosure (i.e., those discussed in sections 2 and 3 of this submission).

5. Meaning of 'arranged for'

FinTech Australia considers the concept of "arranged for" as being one of the more challenging aspects of the new APP 1.7-1.9 obligations, depending upon the extent to which this requires examination of the ADM "supply chain". Members are concerned about the level of visibility they are expected to have into the use of ADM tools by vendors and technology service providers.

By way of example, credit reporting agencies may use ADM to generate credit scores, and fintech lenders rely upon those scores to approve or deny credit. This use case would seemingly meet the threshold for disclosure under APPs 1.7 – 1.9 and thus the lender would be required to disclose information relating to the ADM tools, even though the ADM itself was used by the credit reporting agency and not the lender.

In practice, credit reporting agencies and other technology vendors are unlikely to share necessary information to customers, as this may result in disclosure of proprietary and commercially sensitive information. Fintechs may therefore bear disclosure obligations in respect of third-party tools of which they have limited visibility. If assumptions are made in order to meet disclosure requirements, this may have the effect of somewhat undermining the purpose of the transparency requirements.

The ADM Guidance should therefore address what reasonable steps APP entities should take to obtain visibility into the ADM practices of their supply chain, and what level of assumption is acceptable where full information is not available.

The ADM Guidance should additionally clarify the circumstances in which an entity which benefits from the output of a third-party ADM tool is considered to have "arranged for" the decision, and should distinguish between scenarios where: (i) the entity directly instructs or commissions a vendor to use ADM on its behalf, and (ii) the entity procures a service which the vendor delivers using ADM.

The CCPA addresses this supply chain challenge through a distinct mechanism that is absent from the Australian framework. Under the CCPA, a business that makes ADMT available to another business (a "recipient-business") to make a significant decision must provide to the recipient-business all facts available to the business that are necessary for the recipient-business to conduct its own risk assessment. Service providers and contractors are also contractually required to assist the recipient-business in complying with its ADMT obligations, including cooperating in the risk assessment process.

Adopting an analogous approach, specific sections of the ADM Guidance could be addressed towards providers of ADM tools, encouraging disclosure of necessary information to customers. This would support improved information sharing and uplift transparency around ADM more broadly. Over time, the requirement to provide relevant information could also be factored into contractual terms between ADM providers and customers, where commercially feasible to do so.

6. Extent of disclosure

Members are also conscious of the level of granularity which they may be expected to include in their privacy policies regarding the use of ADM. Fintechs often use multiple ADM tools across different functions, so the ADM Guidance should confirm that APP entities may include consolidated or aggregated or category-level disclosures rather than requiring a use-by-use, model-by-model or tool-by-tool breakdown. For example, entities should be able to describe categories of automated decisions, such as credit assessment, transaction monitoring, identity verification, fraud detection, scams prevention or customer eligibility assessments, without disclosing the details of specific models, tools, rules, thresholds or vendor systems.

Detailed disclosures may, in some cases, undermine processes that necessarily operate with a degree of opacity to maintain their integrity and effectiveness. For example, disclosures relating to fraud detection, scams prevention, Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) processes, cybersecurity controls, transaction monitoring, credit risk decision and investigative processes may enable bad actors to reverse-engineer processes, evade detection or exploit vulnerabilities. On this basis, disclosure should not be required where transparency would compromise system integrity or result in an increased risk of serious harm to individuals. Similarly, APP entities should not be required to disclose proprietary or commercially sensitive information. Express carve-outs of this nature in the ADM Guidance would be consistent with the CCPA and the Explanatory Memorandum for the *Privacy and Other Legislation Amendment Act 2024* (Cth). The ADM Guidance should also confirm that APP entities may describe categories of automated decisions, such as credit assessment, transaction monitoring, identity verification, fraud detection or scams prevention, rather than disclosing details of specific models, tools, rules, thresholds or vendor systems.

Practically, ADM models are frequently updated, meaning highly specific disclosures could require constant updates to privacy policies, which may require a disproportionate effort and ultimately prove unhelpful for consumers.

The impact of the ADM Guidance should also be considered in light of the draft Privacy (Children's Online Privacy) Code 2026. Those FinTech Australia members offering financial products to children will be required to make uplifts under the Privacy (Children's Online Privacy) Code 2026 in terms of the level of transparency offered, and the two regimes must be consistent and proportionate when viewed together.

Conclusion

FinTech Australia welcomes the OAIC's consultation on the ADM Guidance and appreciates the opportunity to contribute to its development. As set out in this submission, our members are committed to responsible and transparent deployment of technology, whilst seeking clarity and proportionality in the regulatory framework.

The key themes emerging from our consultation with members include the need for clear and consistent guidance on threshold concepts such as "substantially and directly related" and "significantly affect rights or interests", alignment with established international frameworks, practical guidance on supply chain transparency obligations, and recognition of the justifiable limits on disclosure where proprietary, commercially sensitive or security information is involved.

We encourage the OAIC to adopt a prescriptive approach where possible, providing categorical guidance that enables businesses to focus resources on use cases that overwhelmingly have a significant impact on individuals' rights and interests, rather than expending effort on marginal assessments.

A clear and proportionate approach will better support consumers by improving the usefulness of ADM disclosures, while allowing fintechs to continue deploying technology responsibly to improve safety, access, efficiency and innovation in financial services.

FinTech Australia and its members look forward to continuing engagement with the OAIC as the ADM Guidance is finalised, and remain committed to supporting the development of a transparency framework that protects consumers while enabling responsible innovation in the Australian fintech sector.