



4 October 2024

Mr Anthony Murfett
Department of Industry, Science and Resources
Industry House
10 Binara Street
CANBERRA ACT 2600
Submitted via email to aiconsultation@industry.gov.au

Dear Mr Murfett,

MANDATORY GUARDRAILS FOR ARTIFICIAL INTELLIGENCE IN HIGH-RISK SETTINGS

The Australian Finance Industry Association (AFIA)¹ is the only peak body representing the entire finance industry in Australia. We appreciate the opportunity to respond to the Australian Government's *Proposals paper for introducing mandatory guardrails for AI in high-risk settings (Mandatory Guardrails)*.²

We represent over 150 members, including bank and non-bank lenders, finance companies, fintechs, providers of vehicle and equipment finance, car rental and fleet providers, and service providers in the finance industry. We are the voice for advancing a world-class finance industry and our members are at the forefront of innovation in consumer and business finance in Australia. Our members finance Australia's future.

We collaborate with our members, governments, regulators and customer representatives to promote competition and innovation, deliver better customer outcomes and create a resilient, inclusive and sustainable future. We provide new policy, data and insights to support our advocacy in building a more prosperous Australia.

INTRODUCTORY COMMENTS

AFIA welcomes the opportunity to respond to the Mandatory Guardrails noting the significance of AI and its ongoing role in transforming Australian industry and society. We also note the concurrent release of

¹ Australian Finance Industry Association (afia.asn.au)

² Australian Government, Department of Industry, Science and Resources, *Safe and responsible AI in Australia, Proposals paper for introducing mandatory guardrails for AI in high-risk settings*, September 2024.

the *Voluntary AI Safety Standard (Safety Standards)*³. As the Mandatory Guardrails mirror 9 out of the 10 Safety Standards, this submission will comment specifically on the former.

It is worth highlighting that the Guardrails distinguish between AI systems and AI models. The Guardrails are intended to apply to AI systems in 'high-risk' settings; and general-purpose AI models (GPAI) including OpenAI's GPT, DALL-E and Sora.⁴

The rapid advances in AI technologies has accelerated transformation in the finance industry, offering opportunities for innovation, efficiency, and enhanced customer experience.⁵ In the financial services industry, AI has long been used for both back- and front-office operations to increase efficiency and productivity. As recently noted by the RBA,⁶ AI is helping to automate processes, improve decision-making and enhance risk management practices in some areas. For example:

- assessing borrower credit worthiness and automating loan approvals
- executing trades based on market data, historical patterns and real-time signals
- monitoring transactions to identify unusual patterns, such as large withdrawals, that may indicate fraud.

Although they are still in the early testing and experimentation stages, our members are also starting to investigate how generative AI can be used to enhance productivity (for example in writing and debugging code, reviewing documents and providing assistance to staff to help them more efficiently support customers).

This transformation is evident in other industries and sectors with CSIRO finding that 68 per cent of organisations were utilising AI in some way, from simple payroll management, to customer service 'bots' on websites. In another report the CSIRO states that, when used well, *'AI allows people to do things faster, cheaper, safer and better.'*⁷ AI has positive applications and immense potential, as noted in the consultation paper:

*'AI can improve wellbeing and quality of life, grow our economy and support a future made in Australia.'*⁸

However, as acknowledged, there is also growing evidence of risks to people, groups and society. AFIA understands the importance of the Government's role in protecting the community and supports the Government's initiative to facilitate safe and responsible AI use.⁹ We note that effective regulation that

³ Australian Government, Department of Industry, Science and Resources, *Voluntary AI Safety Standard, Guiding safe and responsible use of artificial intelligence in Australia*, 5 September 2024.

⁴ Consultation Paper, p 8.

⁵ For the purposes of this submission, AI System & AI Model are defined per consultation paper, p 8.

⁶ Reserve Bank of Australia, *Financial Stability Review – September 2024* (available online at [4.1 Focus Topic: Financial Stability Implications of Artificial Intelligence | Financial Stability Review – September 2024 | RBA](#)).

⁷ CSIRO, *Australia's artificial intelligence ecosystem*, (December 2023), p 7.

⁸ Op cit, n 2, p 3.

⁹ Ibid.

promotes the responsible use of AI needs to be balanced against innovation, competition, and enhanced consumer outcomes.

As noted in the Mandatory Guardrails paper, the use of AI is currently shaped by a range of existing regulatory and legal obligations in Australia including under ‘consumer, privacy, anti-discrimination, competition, data protection, and copyright law’.¹⁰ In the context of the financial services industry there are an additional array of laws¹¹ which intersect with the development and deployment of AI. As acknowledged by the Mandatory Guardrails paper there is a differing level of maturity in different sectors with ‘...heavily regulated industries like the financial sector already...[having]... a range of obligations that support the safe and responsible use of AI.’¹² In the context of regulated entities in financial services industry, the deployment of AI systems or AI models is therefore not without regulatory oversight. As summarised by Therese McCarthy Hockey in AFIA’s Risk Summit 2024:

*“...[The financial services]... prudential framework already has adequate regulations in place to deal with generative AI for the time being. Our prudential standards may not specifically refer to AI but nor do they need to at the moment. They have intentionally been designed to be high-level, principles-based and technology neutral”.*¹³

For example (and this is by no way exhaustive) ASIC Regulatory Guide 241 addresses automated order processing,¹⁴ ASIC Regulatory Guide 255 provides guidance on automated financial product advice;¹⁵ CPS 234: Information Security addresses cyber security controls,¹⁶ CPG 235: Managing Data Risk provides guidance on protecting data from misuse and theft¹⁷ and CPS 230 introduces enhanced requirements in operational risk management, resilience and tolerance levels for disruption and service provider management.¹⁸

Accordingly, AFIA considers that it is very important that the development of Mandatory Guardrails involves express consideration of how the Mandatory Guardrails interact with existing legal obligations and steps are taken to minimise inconsistencies with existing legal obligations. Consistency of interpretation and application of the Mandatory Guardrails across financial services and other sectors in the economy will also be critical in reducing friction and compliance burdens for all.

AFIA is currently undertaking research on the use of AI within financial services. This is intended to highlight the range of current and potential future use of AI within the industry. We look forward to sharing the outcome of this research when finalised.

¹⁰ Op cit, n 2, p 4.

¹¹ E.g. *Corporations Act 2001* (Cth); *National Consumer Credit Protection Act 2009* (Cth); *ASIC Act 2001* (Cth).

¹² Op cit, n 2, p 43.

¹³ Terese McCarthy Hockey, ‘Remarks to AFIA Risk Summit 2024’ (available online at [Member Therese McCarthy Hockey’s remarks to AFIA Risk Summit 2024](#)) 22 May 2024.

¹⁴ ASIC, RG 241 Electronic trading (available online at [Regulatory Guide RG 241 Electronic trading \(asic.gov.au\)](#)).

¹⁵ ASIC, RG 255 Providing digital financial product advice to retail clients (available online at [Regulatory Guide RG 255 Providing digital financial product advice to retail clients \(asic.gov.au\)](#)).

¹⁶ APRA, *Prudential Standard CPS 234* (available online at [cps_234_july_2019_for_public_release.pdf \(apra.gov.au\)](#)).

¹⁷ APRA, *Prudential Practise Guide CPG 235* (available online at <https://www.apra.gov.au/sites/default/files/CPG-235-Managing-Data-Risk.pdf>).

¹⁸ APRA, *Prudential Standard CPS 230* (available online at [Prudential Standard CPS 230 Operational Risk Management - clean \(apra.gov.au\)](#)).

INTERACTIONS WITH INTERNATIONAL APPROACHES

The current global regulatory environment for AI is fragmented, with the UK, China, Singapore, ASEAN, Europe and US jurisdictions all adopting different approaches. This presents challenges for financial organisations operating in global markets, as many of the AI models used by Australian organisations are developed internationally, with some estimates showing over 50 per cent of large-scale AI models were developed in the United States.¹⁹

Financial organisations rely on AI developed internationally. Members headquartered overseas face the challenge of adhering to different regulatory regimes simultaneously. Dependence on developers raises questions about how Australian organisations can enforce obligations when there is inconsistency between regulatory frameworks.

Most AI developers are not based in Australia. As CSIRO Director of Digital, National Facilities & Collections, Elanor Huntington states:

*'[generative AI (GAI) models] are rarely made in Australia. The vast majority come from the United States and China. Our industry is becoming increasingly dependent on these models.'*²⁰

The Mandatory Guardrails must address how the proposed obligations will work when developers are not subject to Australian laws, as enforcement and compliance may become complex in this context. For example, financial organisations, as deployers, may lack the leverage to enforce compliance or obtain necessary information, raising concerns about responsibilities and liabilities. It may also be challenging to ensure developers adhere to the Mandatory Guardrails or other Australian specific regulations while they are also subjected to the regulations of other jurisdictions. In this regard we think it is important to not rush ahead with the Mandatory Guardrails without further considering interoperability and interaction between major regulatory approaches to AI (including Europe's AI Act).

For example, other jurisdictions grappling with AI regulation include:

- **EU:** The AI Act takes a stringent, ex-ante approach but faces criticism for complexity and potential to stifle innovation.²¹
- **US (Federal) and UK:** Tend to prefer principles-based or sector-specific regulations, focusing on fostering innovation while addressing risks.²²
- **Canada:** Is expected to regulate AI in a centralised manner alongside privacy, taking a harms-based approach.²³

¹⁹ Epoch AI, *Tracking Large-Scale AI Models*, (April 2024).

²⁰ CSIRO, *Artificial Intelligence foundation models report* (March 2024).

²¹ Malgieri, Gianclaudio and Frank Pasquale, 'Licensing high-risk artificial intelligence: Toward ex ante justification for a disruptive technology' (2024) 52 *Computer Law & Security Review*.

²² Jellison, Noah and Samantha Ellwood, 'The evolving landscape on AI regulation' (October 2023).

²³ Innovation, Science and Economic Development Canada, 'New laws to strengthen Canadians' privacy protection and trust in the digital economy', (June 2022).

These differing approaches present challenges to compliance with the proposed Mandatory Guardrails. The global disparity in AI regulations leads to unclear compliance requirements, depending on the jurisdiction in which the developer is located.

PRINCIPLES AND DEFINITIONS GOVERNING AI REGULATION

Definitions and scope

AFIA recommends both clarity and consistency in definitions. With AI having the potential to affect all layers of Australian industry, it is important for organisations to have certainty on its deployment across the supply chain, without hindering productivity or innovation. In considering this, AFIA recommends consideration is given to further clarifying who the Mandatory Guardrails will apply to (and how they will apply those entities). For example:

- it is currently unclear exactly how the Guardrails will apply to Developers and Deployers. Clear parameters as to which obligations apply to Developers and which apply to Deployers is crucial to ensuring the Mandatory Guardrails are effectively implemented throughout the value chain without unnecessary duplication and regulatory burden.
- the current inclusion of “suppliers” within the proposed definition of “Deployers”²⁴ may practically result in multiple organisations being considered as a “Deployer” for the same AI System. In practice, only the entity who is using the AI System will have the relationship with the end user necessary to practically implement many of the Guardrails (as relevant to a Deployer). AFIA notes Europe’s AI Act has narrowly defined “Deployer” to those who use an AI System;²⁵
- there is currently no guidance as to how the Guardrails will apply where there are multiple developers and multiple deployers throughout the AI value chain. For example – it is currently unclear who bears the onus of responsibility where an organisation engages a third party to develop an AI Model or AI System on their behalf. Clear parameters as to who is responsible for compliance where there are multiple developers and deployers is essential for financial firms to assess whether their technologies fall under specific regulatory frameworks. Without examples and guidelines, this could potentially lead to unintentional non-compliance or stifled innovation due to over-cautious approaches. Clarity ensures that all stakeholders have a mutual understanding of AI, which facilitates better communication, compliance, and development within the industry; and
- there is a current presumption in the Guardrails that Deployers will be able to flow obligations upstream via contractual relationships. In many circumstances, Australian Deployers will not have the contractual bargaining power to impose significant obligations on international Developers who are not otherwise subject to the Guardrails. If this presumption is to be retained – there must be explicit regulatory requirements on Developers that Deployers can point to during negotiations. AFIA also recommends consideration is given to providing Deployers with a due diligence defence where they have used reasonable efforts to comply with the Mandatory Guardrails.

²⁴ “Any individual or organisation that supplies or uses an AI system to provide a product or service” [emphasis added].

²⁵ European Union AI Act, Chapter 1, Article 3 (4).

Principles based approach to 'high-risk' AI

AFIA appreciates the government's proactive approach in developing principles to define and understand the risks posed by AI. The principles outlined in the consultation paper represent an important step toward safeguarding individual rights and ensuring AI technologies are deployed responsibly.

However, AFIA is concerned that the principles-based approach to defining 'high-risk' AI settings may introduce some uncertainty.²⁶ For example:

- although AFIA is supportive of the focus on protecting human rights, mental and physical well-being, legal standing, and the broader economic and societal impacts of the irresponsible use of AI – the breadth of the current principles has the potential to give rise to uncertainty around what adverse impacts will actually be captured; and
- the lack of guidance around how to interpret the principles will likely result in Developers and Deployers coming to different conclusions as to whether similar (and in some cases the same) AI System is high-risk or not based on the information available to them and how they approach risk. The risk of 'differences' in approach is increased due to the breadth of Principle 6 ("the severity and extent of those adverse impacts..."). For example – is an adverse impact of an AI System that is of a low severity but will impact a large number of people considered high risk? Similarly – is an AI System that will have an adverse impact that is of a medium to high severity but will only impact a few people considered high risk?

This lack of clarity and guidance may result in Australian companies taking a less-proactive approach to AI due to regulatory uncertainty.

Accordingly, and noting that many AFIA members are cautious with AI use already, and few are using AI in customer-facing systems, AFIA recommends:

- the breadth of the current approach to 'high-risk' be clarified to ensure that low-risk applications are not inadvertently subjected to stringent regulations. This should include, at a minimum, express exclusions for AI systems that are intended to:
 - perform a narrow procedural task;
 - improve the result of a previously completed human activity;
 - detect decision-making patterns or deviations from prior decision-making patterns; and
 - perform a preparatory task to an assessment;
- a more granular approach is adopted to defining high-risk AI systems, considering the specific context in which AI is applied. Ideally, this would involve a list of contextual situations where the use of AI Systems is high-risk. Such a list would be expandable over time by the Government or Regulators (as applicable) and it will ensure that the Mandatory Guardrails are focused on genuinely high-risk systems while allowing financial organisations to leverage AI responsibly without excessive regulatory barriers. It will also assist in cross-sectoral consistency as it will reduce the risk that different sectors and different regulators will reach different conclusions as to which AI systems are (and aren't) high-risk. The broader approach could be retained for voluntary safeguards; and
- (if the current principles-based approach is to be retained) a framework is developed which establishes clearer guidelines for interpreting and applying the principles, including defining

²⁶ Consultation Paper, p. 18.

thresholds for what constitutes a ‘severe’ or ‘broad’ impact. This would be beneficial for financial organisations to make informed risk assessments and ensure compliance without unnecessary hurdles.

With regards to general-purpose AI (GPAI), we note the government is currently considering whether all GPAI models should be treated as high risk due to ‘unforeseen risks’.²⁷ The definition presented in the consultation paper for GPAI is broad: *‘an AI model that is capable of being used, or capable of being adapted for use, for a variety of purposes, both for direct use as well as for integration in other systems.’*²⁸

AFIA agrees with the importance of protecting users from the harm lack of human intervention may cause, but also recommends that consideration is given to ensuring that:

- only the truly high risk GPAI Models are subject to the Mandatory Guardrails. While risks may be ‘unforeseen’, it is not clear why some models, especially smaller models, should be automatically considered high risk particularly in circumstances where the variety of purposes is known and/or suitably constrained by design; and
- GPAI Models that are open source (which could include situations where the Developer releases the weights of the model and has limited control over how they are subsequently deployed) are subject to special treatment to acknowledge the reduced control Developers have in this situation.

The application of the Guardrails as they stand to all GPAI Models also gives rise to questions about how they will be practically implemented as between Developers and Deployers. This question is amplified for GPAI given the variety of purposes for which it may be used by Deployers and End Users.

Specific exclusions – fraud detection and prevention

As noted above, many members of the financial services industry in Australia utilise narrow AI for operations optimisation.²⁹ This reflects the position internationally where, as recently summarised by the OECD, international financial services industry participants commonly use AI for “automated fraud detection, detection and prevention of financial crime and/or market abuses, cyber-security threat detection and monitoring, AML/CFT monitoring (e.g., reducing the rate of false positives and false negatives), stress testing and capital optimisation, trading and portfolio management optimisation and support functions for financial advice, risk management (e.g. loss forecasting) and credit portfolio monitoring.”³⁰

In line with global best practices and to ensure that AI continues to enhance the security and efficiency of financial services without unintended consequences, AFIA recommends that the definition of ‘high-risk’ AI explicitly excludes AI systems used for fraud detection, prevention, and other compliance-related functions.

²⁷ Ibid p. 29.

²⁸ Ibid p. 9.

²⁹ Consultation Paper p. 9.

³⁰ OECD, Regulatory Approaches to AI in Finance, Page 15 (available online at https://www.oecd.org/en/publications/regulatory-approaches-to-artificial-intelligence-in-finance_f1498c02-en.html) 5 September 2024.

A similar exclusion has already been approved in Europe's AI Act with Annex III (5)(b) explicitly excluding AI systems used for the purpose of detecting financial fraud from the scope of the high-risk AI Systems:

“(b) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems used for the purpose of detecting financial fraud”³¹ [Emphasis added]

This exclusion is of particular importance given the criticality of systems for fraud detection and prevention to protect consumers and maintain system integrity. The ability to utilise AI to detect financial crime or scam activity may also have significant impacts for financial organisations to meet their obligations under existing legislation including *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.

MANDATORY GUARDRAILS

The ten Mandatory Guardrails are designed to ensure accountability, risk management, data protection, testing, human oversight, transparency, contestability, supply chain transparency, record-keeping, and conformity assessments. While these objectives are important for responsible AI use, there are practical challenges that financial organisations will face in their implementation. A key one being, as flagged earlier, financial services is already a heavily regulated industry, there are a range of competing regulatory obligations. It will be challenging to determine how to apply the guardrails in the event of inconsistency with existing legal obligations.

The Mandatory Guardrails paper identifies the assessment of credit worthiness or credit scoring as an example of a high-risk use of AI which has been regulated in other jurisdictions. The finance industry has been using automated data analytics and machine learning systems for many years to assess a customer's credit worthiness for the purpose of fulfilling legal obligations to lend responsibly.

Guardrail 5: the black box problem and human oversight

Guardrail 5 outlines that organisations must ensure that humans can effectively understand a high-risk AI system, oversee its operation and intervene when necessary across the AI supply chain and throughout the AI lifecycle. AFIA supports the necessity of human oversight over high-risk AI, to ensure decisions made which affect individual rights and privacy are governed appropriately. Achieving meaningful human oversight per Guardrail 5 will be challenging, especially with complex AI systems that operate as 'black boxes'.³² The proposal is an important safeguard, but further clarity is needed on Guardrail 5.

³¹ Annex III, cl 5(b), Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act). See also Recital 58 that states “...AI systems provided for by Union law for the purpose of detecting fraud in the offering of financial services and for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements should not be considered to be high-risk under this Regulation.”.

³² Consultation Paper, p. 11.

Guardrail 7: Contestability

Guardrail 7 states that “Organisations will be required to establish processes for people who are negatively impacted by high-risk AI systems to contest AI-enabled decisions or make complaints about their experience or treatment.” Although AFIA supports the importance of ensuring that there are suitable internal compliant handling functions and sufficient information provided to those who are impacted by high-risk AI Systems, it is important that any new requirement of contestability is considered in light of the purpose for which AI Systems are used and existing legislation.

In the financial services industry, there are many situations where contestability of decisions that are made using AI Systems should be encouraged as the decision will have a legal or similarly significant effect on an individual. For example, decisions that go to the creditworthiness of individuals and the eligibility of individuals for banking products e.g., credit cards, loans, insurance and the identification of customers experiencing vulnerability. However, Guardrail 7 goes far beyond this to capture contestability for any “negative impact” by a “high-risk AI system”. This breadth is even broader than the approach taken in Europe where Article 22 of the GDPR applies contestability to “*decisions based solely on automated processing including profiling which produces legal effects concerning him or her or similarly significantly affects him or her*”.

Guardrail 8: Be transparent with other organisations across the AI supply chain about data, models and systems to help them effectively address risks

AFIA supports in principle the government’s intention in **Guardrail 8** to promote transparency across the AI supply chain, however requests further clarity on how this can operate across lengthy and global supply chains. There may be challenges enforcing this guardrail, particularly when dealing with overseas developers who are not subject to Australian law.

The proposal’s emphasis on transparency is a welcome step, but financial institutions need clearer guidance on how to enforce compliance or access critical information from foreign developers. Without this, organisations could face difficulties in meeting the transparency requirements, raising questions about liability. For instance, if a financial institution cannot obtain essential data from a foreign developer, can they still be held responsible for non-compliance? As noted above, AFIA considers it very important to ensure that Deployers have a due diligence defence where they have used reasonable efforts to comply with the Mandatory Guardrails.

Further, AFIA recommends the scope of the definition of the AI supply chain be narrowed or be considered with more flexibility noting the diversity of actors and industries involved.³³ Under the current proposal, requiring AI compliance along the length of the supply chain may be difficult. By focusing on the most critical suppliers, this ensures the framework is not overly burdensome for organisations dealing with global technology vendors.

³³ Ibid. pp 8, 34.

Guardrail 9: Keep and maintain records to allow third parties to assess compliance with guardrails

Transparency and record-keeping, as outlined in Guardrail 9, are crucial for ensuring accountability and enabling third parties to assess compliance.³⁴ However, practical challenges arise in implementing comprehensive record-keeping for complex AI systems, especially when dealing with proprietary or third-party models.

Organisations may face difficulties in auditing automated decision-making processes, particularly when using AI models developed externally. Questions arise about the extent to which financial institutions can request developers to provide audit records or whether they are permitted or obligated to audit service providers. Additionally, concerns exist about whether external parties can audit an organisation's automated decision-making, especially when these external parties are located in different jurisdictions. AFIA is also concerned about the potential breadth of this Guardrail noting the Proposal' states it *"could include the power for regulators to access documents on enforcement and compliance in their regulatory remit"*.

Balancing transparency with security and proprietary concerns is essential. Financial organisations must protect sensitive information; full transparency may expose proprietary algorithms or create security vulnerabilities. A balance must be struck to provide necessary information without compromising security or competitive advantage.

Guardrail 10: Undertake conformity assessments to demonstrate and certify compliance with the guardrails

While the government's goal of ensuring conformity assessments is an important step to align the guardrails, practical issues arise regarding the cost, responsibilities, and logistics of these assessments. Mandatory conformity assessments and certifications may be resource intensive (a situation that will be amplified in Australia where we have a critical AI skills shortage). Organisations may face difficulties conducting assessments, particularly when using AI models developed externally. It is unclear where the responsibility for conducting these assessments lies—whether with the AI deployer or the developer.

Moreover, the application of this guardrail to AI systems developed overseas adds further complexity. AFIA recommends clarity on whether these conformity assessments have extraterritorial implications and how to approach international AI vendors. Financial organisations need guidance on managing these requirements in a global context, ensuring that obligations are clearly defined for both developers and deployers.

³⁴ Ibid. p. 42.

PROPOSED REGULATORY OPTIONS

AFIA supports Option 2—the framework approach— in principle but further details and consultations are necessary to fully assess its implications.³⁵ Option 2 may be preferable as it introduces framework legislation with associated amendments to existing legislation rather than applying a singular legislation across diverse industries and sectors. This option provides a common language and consistent guardrails across the economy while allowing for sector-specific considerations. It aligns with the need for clarity and operational certainty without overhauling the entire regulatory landscape.

However, if Option 2 is taken, AFIA emphasises the importance of ensuring that the framework approach does not result in regulatory overlap or complexity that could hinder innovation and competitiveness in the financial sector. Clear guidance and a coordinated implementation strategy which looks to the specific needs of the finance industry are crucial to address these concerns and to ensure that the new regulations support both compliance and technological advancement.

Interaction with existing legislation

The proposed guardrails should harmonise with existing legislation to avoid duplication and conflict. For example, data governance measures should align or at the least not conflict with the *Privacy Act 1988*, and cybersecurity requirements should consider the *Security of Critical Infrastructure Act 2018*.

Overlapping regulations can create confusion and increase compliance costs. Clear guidance on how the guardrails interact with current laws is necessary to ensure organisations can comply effectively without unnecessary complexity.

CLOSING COMMENTS

AFIA and its members are committed to using AI responsibly, enhancing customer experiences, and maintaining trust. Collaboration between industry and government is vital to develop regulations that protect consumers while fostering innovation and competitiveness.

Financial organisations support the intent to regulate AI responsibly but have concerns regarding practical implementation, potential overregulation, and the need for clarity. Specific issues include the definition of high-risk AI, applicability to overseas developers, and the feasibility of certain guardrails.

Overly restrictive regulations may deter investment and innovation in AI within the finance industry. Careful consideration is needed to avoid unnecessary hurdles that do not proportionately enhance safety or trust. A balanced framework that fosters innovation while ensuring safety and responsibility is essential.

³⁵ Ibid, p. 43.

We consider the government should provide detailed guidance, consider explicit exclusions for essential financial functions like fraud detection, and consider how the approach aligns with international standards.

AFIA appreciates the government's proactive approach to AI regulation and its willingness to engage with industry stakeholders. By working collaboratively, we can develop a regulatory framework that safeguards consumers, promotes innovation, and maintains Australia's competitiveness in the global market.

I would appreciate the opportunity to discuss our recommendations and provide the Inquiry with further information about the specialised products, services and technologies offered by smaller lenders.

Should you wish to discuss our submission or require additional information, please contact me at roza.lozusic@afia.asn.au or 0431261201.

Yours sincerely

A handwritten signature in black ink, appearing to read 'Roza Lozusic', with a stylized flourish extending to the right.

Roza Lozusic
Executive Director, Policy and Public Affairs