FinTech Australia

Safe and responsible AI in Australia discussion paper response

August 2023

fintechaustralia.org.au

About this Submission

FinTech Australia thanks the Australian Government's Department of Industry, Science and Resources for the opportunity to comment on the Discussion Paper entitled “Safe and responsible AI in Australia” (**Discussion Paper**).

This document was created by FinTech Australia in consultation with its members. In developing this Submission, interested members participated in a consultation process to discuss key issues and provided feedback to inform our response to the Discussion Paper.

About FinTech Australia

FinTech Australia is the peak industry body for the Australian fintech sector, representing over 420 fintech companies and startups across Australia. As part of this, we represent a range of businesses in Australia’s fintech ecosystem, including fintechs engaging in payments, consumer and SME lending, wealthtech and neobanking, the consumer data right and the crypto, blockchain and Web3 space.

Our vision is to make Australia 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;
- Cornwalls;
- DLA Piper;
- Gadens;
- Hamilton Locke;
- King & Wood Mallesons; and
- K&L Gates.

Questions and Responses

Definitions

Question 1. Do you agree with the definitions in this discussion paper? If not, what definitions do you prefer and why?

The Discussion Paper proposes to define Artificial Intelligence (AI) as 'an engineered system that generates predictive outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives or parameters without explicit programming. AI systems are designed to operate with varying levels of automation.'

FinTech Australia considers that while this definition of AI may be suitable in the context of ISO/IEC 22989:2022, which formed the basis of the proposal, it is not suited to be adopted in a regulatory context in its current form. Members note that AI, to become relevant in a regulatory and whole of industry context, an element of 'influence' should be included. Our members propose that the effect of influencing the environment or the process an AI application operates in is a critical threshold element for subjecting AI to mandatory regulatory oversight. We note that a similar element forms part of the definition of AI proposed in the EU AI Act

Some of the feedback that we have collected characterises the proposed definition as too narrow. Members consider the following elements of the proposed definition of AI are neither technology-neutral nor future-proof due to the fast changing and ever evolving nature of AI:

- **'Predictability of outputs'** - one member submits that some form of human vetting or interaction should form part of the definition of AI. Another member submits the alternative element of 'usability of outputs', which can include predictable, unpredictable; accurate or inaccurate outputs;
- **'Human-defined objectives or parameters'** - self-learning algorithms are in fact based on objectives or parameters not being human-defined over time (or being 'machine-defined' goals); and
- **'Without explicit programming'** - concerns were raised by certain members that this would risk carving out a number of AI use cases where initial explicit programming was included – removal of this limb is suggested.

Certain members comment that a preferred approach to defining AI could be to focus on what an AI system is designed or intended to achieve, rather than what it currently does, as the latter can be subject to rapid change, particularly in the context of machine learning, generative AI and automated decision making. This could be supplemented by a requirement on AI creators and vendors to monitor the use/functionalities of the AI system to ensure the risk level does not change over time.

FinTech Australia is of the view that any definition of AI should, to the extent possible, be consistent with definitions adopted in other relevant jurisdictions, as challenges experienced with multi-jurisdictional privacy compliance laws, where varying definitions of ‘personal identifiable information’, ‘personal data’ and ‘personal information’ and associated privacy obligations across patchwork legislation have led to legal and operational uncertainty.

Members are unanimous in requesting that definitions used in the context of AI should be no broader than those adopted in other jurisdictions to ensure Australia stays competitive in the international context – both to facilitate innovation within Australia, and to attract international developers to the Australian market.

Regarding other definitions, such as ‘machine learning’ and ‘generative AI’, members are generally accepting of the proposed definitions. However, there is a preference among members to refrain from incorporating any AI technology or applications specific definitions in the main body of any potential mandatory regulation, due to the inflexibility of such an approach. Rather, FinTech Australia considers that supplementary rules, frameworks or existing standards (e.g. ISO) should give meaning to sub-categories of AI to ensure mandatory regulations remain up-to-date in the fast-moving field of AI. Members conclude that a clear focus should be on reaching a widely acceptable, practical, technology-neutral and future-proof definition of AI.

Potential gaps in approaches

Question 2. What potential risks from AI are not covered by Australia’s existing regulatory approaches? Do you have suggestions for possible regulatory action to mitigate these risks?

The Discussion Paper identifies that AI is currently regulated by several existing regulatory regimes, for example under the *Australian Privacy Act 1988* (Cth), *Competition and Consumer Act 2010* (Cth) and the *Online Safety Act 2021* (Cth), which are tailored to mitigate core risks associated with the use of AI, such as privacy, consumer and competition protections, and online safety. Further, sector-specific regulations which address the potential risks arising from the use of AI, including those for therapeutic goods and financial services, exist.

FinTech Australia considers that those regulatory regimes and sector-specific regulations, due to the fact that they are both established and technology neutral, are, subject to ongoing review and improvements, most suited to address the specific risks associated with AI (e.g. privacy). Members suggest that further coordination of existing regimes and frameworks is preferable to the introduction of a separate regulatory AI regime which may detract from those well-regulated and established regulatory approaches. Members are in strong support of the proposal that the identification of any gaps or uncertainties in existing legislative frameworks should be a key focus of regulator co-operation (i.e. a gap analysis).

FinTech Australia acknowledges that none of the existing regimes address high-risk use cases of AI specifically or is equipped to evaluate and, if required, ban AI applications with unacceptable risk levels. Members suggest any review of and coordination efforts amongst existing regimes should consider high-risk AI uses specifically and focus on incorporating appropriate testing and review mechanisms to close this gap.

Question 3. Are there any further non-regulatory initiatives the Australian Government could implement to support responsible AI practices in Australia? Please describe these and their benefits or impacts.

Members acknowledge existing non-regulatory initiatives, such as the DISR's AI Ethics Principles, pilot and Responsible AI adopt program, and the DISR via CSIRO's National AI Centre and Responsible AI Network. We consider that a non-regulatory approach is the preferred mechanism for implementing and supporting responsible AI, as non-regulatory initiatives function both as a best-practice standard and resource for developers and deployers of AI, irrespective of AI maturity. We submit that the ongoing development of these programs and initiatives should form a core pillar of the Australian Government's AI strategy.

To the extent not already covered by existing programs, members see merit in the following additional non-regulatory initiatives:

- **Government supported 'sandbox' environment** to develop and test new AI applications (with priority access for small-to-medium enterprise (**SME**) developers);
- **AI governance testing framework and toolkit** modelled on the "AI Verify" program adopted in Singapore to allow the testing of developed AI applications;
- **Adoption of a government approved AI rating** (e.g. in relation to associated risk levels) **and/or certification** which signifies voluntary compliance with ethical standards, which may encourage businesses to participate in non-regulatory initiatives and build consumer trust; and
- **Voluntary register of AI practitioners** to track businesses working on AI and the growth of the sector. Mandatory registration could also be considered for high-risk use cases (similar to the approach taken in the EU AI Act).

Question 4. Do you have suggestions on coordination of AI governance across government? Please outline the goals that any coordination mechanisms could achieve and how they could influence the development and uptake of AI in Australia.

FinTech Australia considers that the minimisation of patchwork solutions, and the establishment of a central AI body, particularly in the context of a regulatory AI framework, should be a key priority to further achieve across-government solutions and support responsible and safe AI practices in Australia.

Members consider that a designated AI board (AI Board), composed of various organisations involved in the standards regulation and/or administration of AI to date, including tech standards setting (e.g. CSIRO) This AI board also include regulator representation from the OAIC or ACCC and would coordinate a unified cross-Government response in relation to the development, deployment and use of AI.

Potential responsibilities could include the development of AI standards and best practices, issuance of guidance notes and hosting of AI related roundtables and consultations. In particular, much like the guidance offered by the OAIC on privacy and consumer data right related matters, it was proposed that guidance in relation to any voluntary or regulatory AI framework would be an invaluable resource, in particular for SMEs, to implement responsible and safe AI practices.

Other members went further by proposing a designated AI regulator (AI Regulator) which would, much like the proposed AI Board, focus on coordinating and identifying AI specific gaps in existing regulatory regimes, and facilitate guidance on the adoption of responsible AI, however, also be in a position to undertake formal assessments and make executive decisions in relation to specific AI use cases. Members propose that both the OAIC, whose jurisdiction covers the Privacy Act, and the Office of the National Data Commissioner (ONDC), whose functions include overseeing the implementation of the *Data Availability and Transparency Act 2022* concerning the sharing of public sector data, would be well-placed to take this role. One member adds that an involvement of the Australian Prudential Regulation Authority (APRA) in relation to the coordination of APRA regulatory guidelines and the financial services sector would also be helpful.

Responses suitable for Australia

Question 5. Are there any governance measures being taken or considered by other countries (including any not discussed in this paper) that are relevant, adaptable and desirable for Australia?

FinTech Australia considers the following two governance measures as particularly desirable for adoption in Australia:

- **AI Verify** (Singapore) – AI Verify is a governance testing framework and toolkit developed by the Infocomm Media Development Authority and the Singapore Personal Data Protection Commission. The testing framework allows AI developers to verify AI applications against eleven internationally accepted AI ethics and governance principles through a combination of technical tests and process checks. The AI Verify toolkit is a 'one-stop' tool library for organisations to conduct technical tests, for example with a view to verify explainability, robustness or fairness of an AI application. While the program is still considered to be in its infancy, benefits, such as accessibility, technical specificity, and visibility, are reasons why members propose the adoption of this governance measure. One member considered that the intersection of technical and ethical issues is a particular concern for the AI developer community and that a tool to assist with the resolution of this issue would be well-received by AI developers;
- **AI Watch** (EU) – AI Watch is a knowledge service established by the European Commission to monitor AI development, uptake and impact of AI in the EU, as well as provide public access to resources on AI systems and development. Members consider that existing governance measures, such as the DISR's Responsible AI adopt program and the DISR via CSIRO's National AI Centre and Responsible AI Network offer some of the resources available through AI Watch, however, proposed that AI Watch, as an open-to-all knowledge and resource service, has greater potential to impact public trust and AI uptake. Members suggest that a separate, designated AI resource service would complement the industry focussed approach of existing initiatives.

Target areas

Question 6. Should different approaches apply to public and private sector use of AI technologies? If so, how should the approaches differ?

FinTech Australia submits that the public sector plays an important role in building public trust through the use of AI applications. As such, members expect that higher standards, whether voluntary or regulatory, should be met by the public sector. Members further consider that valuable insights could be gained from mandatory compliance frameworks, such as the NSW AI Assurance and Ethics frameworks.

The private sector, due to being exposed to market demands and trends resulting in a need to stay competitive, should benefit from a less prescriptive approach. To the extent not considered unacceptable/high-risk or banned applications (please see our answers to Question 12 below), members are in strong support of industry specific codes of conduct and voluntary technical and ethical standards to further innovation and limit intervention to contexts that require it.

We consider that the potential benefits obtained from entrepreneurial and innovative uses of AI outweighed the residual risks associated with following a voluntary regulatory approach in relation to low to medium risk AI applications. One member submits that this approach would allow private sector developers and deployers to focus resources on resolving the technical issues which are still prevalent in many AI applications, rather than pre-occupying resources with mandatory compliance requirements.

Question 7. How can the Australian Government further support responsible AI practices in its own agencies?

FinTech Australia recognises the current Australian Government initiatives relevant to AI outlined in Attachment A of the Discussion Paper. Members propose that that the following measures may assist the Australian Government in supporting responsible AI practices in its own agencies:

- **Establishment of an AI Board or AI Regulator** (please refer to our answer to question 4) who may coordinate existing regimes, and conduct risk-assessments;
- **Adaptation of a consolidated AI strategy for government agencies**;
- **Best practice guides for the most popular use cases;**
- **Implementation of a government-wide AI assurance and ethics framework** (similar to the NSW AI Assurance Framework and Ethics principles); and
- **A central or agency specific AI register** which identifies AI applications implemented by relevant agencies (other than low risk applications), supplemented by risk assessments in relation to relevant use cases.

Question 8. In what circumstances are generic solutions to the risks of AI most valuable? And in what circumstances are technology-specific solutions better? Please provide some examples.

Members consider generic solutions lend themselves to low risk and high-volume AI applications where generic solutions enable large audiences to benefit from AI applications. While we consider that technology specific solutions require longer development and implementation timeframes and are, due to being at risk of becoming out of date very quickly, generally undesirable, members suggest that a combination of any one of the following factors may necessitate a departure from generic solutions:

- **Fast-evolving use case of an AI application**;
- **Human oversight issues**;
- **High-risk impact of an AI application**; and/or
- **Degree of regulation prevalent in the sector in which the AI application is predominantly deployed** (e.g. the medical sector).

Question 9. Given the importance of transparency across the AI lifecycle, please share your thoughts on:

Where and when transparency will be most critical and valuable to mitigate potential AI risks and to improve public trust and confidence in AI?

FinTech Australia considers transparency is most critical and valuable in the development and risk-assessment phase of an AI application, in particular for AI deployers who need to base subsequent risk-assessments and AI application use cases on such assessments.

One member emphasised the particular importance of human involvement throughout the AI lifecycle - from the AI model build including data identification and use (by the AI model owner), to the actual interaction / execution to be aware of its use (by the AI model executor if not also model owner), and lastly, to the model and outcome monitoring (by the AI model executor if not also model owner), to ensure explainability and contestability of an AI model.

While members acknowledge transparency is important at the point where interaction with AI takes place and decisions are being made (e.g. consumer interaction), they note the benefit that consumers may derive from the knowledge that AI is being used in a particular circumstance might be limited. Many consumer products are already entirely built on the use of AI and consumers are, to a large degree, unaware of this. To the extent applications are low-medium risk, disclosure of additional information relating to the AI application used, beyond the mere fact that AI is being involved in the supply of the product or services, may overwhelm consumers and exacerbate existing trust issues.

Further, members note that potential consequences flowing from the disclosure of information in relation to deployed AI applications, for example similar to the opt-out mechanism for non-essential cookies, is not feasible in the context of AI. Many products and services are built on and not merely supplemented by AI, and AI deployers would largely not be in a position to provide products and services without the use of relevant AI applications. However, a lack of transparency or disclosure to inform consumer choices may also frustrate consumers and create public trust issues in relation to its use.

FinTech Australia supports the idea that potential disclosure requirements in relation to the use of AI applications be regulated under the existing and proposed privacy regime (in particular for automated decision-making processes). Members are generally open to the idea that separate requirements may apply for high-risk applications.

Mandating transparency requirements across the private and public sectors, including how these requirements could be implemented.

FinTech Australia proposes that public sector transparency requirements could entail a high level outline of risk assessments conducted for AI applications, preferably in a centralised or agency specific register.

Private sector transparency disclosure requirements should, to the extent not regulated under existing legislation (e.g. the Privacy Act), be limited to high-risk applications. One member considers that the publication of a high-level 'risk-rating', to the extent such categorisation is adopted, may reassure consumers of the nature of application used.

Question 10. Do you have suggestions for:

Whether any high-risk AI applications or technologies should be banned completely?

FinTech Australia is open to the idea that very high-risk applications or technologies may be subject to banning to improve public trust, boost industry confidence and increase viability of low to medium risk applications and technologies. However, members note that banning high-risk AI applications and technologies should be driven by a regulatory framework which, developed under industry consultation, considers the particular detriment which bans may have on the innovation of AI technology, and is based on a well-defined and well-known set of risk assessment criteria.

Descriptive assessment criteria, such as ‘practices that have a significant potential to manipulate persons through subliminal techniques’ as proposed by the EU AI Act, should be narrowly defined and their meaning supplemented by relevant examples. In addition to established assessment criteria, members suggest that any bans should be frequently reviewed and take into account newly developed safety controls and mechanisms.

We further note that an alignment of applicable bans with decisions reached in other jurisdictions, for example AI applications and technologies banned under the EU AI Act, may facilitate both cross-jurisdictional AI harm prevention and trade and benefit the Australian AI industry long term. However, members consider bans which go beyond the consensus reached in other jurisdictions in relation to very high-risk applications may, unless such bans would account for risks that are specific to Australia, stifle AI innovation and disproportionately affect local AI developers and deployers (please also refer to our answer to Question 12).

Criteria or requirements to identify AI applications or technologies that should be banned, and in which contexts?

FinTech Australia considers a combination of any one of the following criteria or requirements, following a comprehensive risk assessment, may warrant the ban of an AI application or use case (but only if banning is proportionate to the likely harms that may result from the AI):

- **large scale and/or high complexity AI applications**;
- **very high risk/impact expected** (e.g. decisions that are threatening to life, welfare, financial well-being, freedom, particularly affecting vulnerable groups, creation of fake news by AI, or compromise of national secrets resulting in a threat to national security);
- **irreversible/perpetual material decisions**;
- **applications with human oversight issues/high level of automation**; and
- **immoral** (social scoring for certain purposes) **or illegal** (facial recognition for tracking of broader public without cause) **purposes**.

Question 11. What initiatives or government action can increase public trust in AI deployment to encourage more people to use AI?

The following initiatives and government actions may increase public trust in AI deployment:

- **consolidation and/or harmonisation of existing regulatory regimes** e.g. through a designated AI board or body, supported by educational resources highlighting laws already applicable to the development and deployment of AI to the public and thus increase public trust (please see our answer to Questions 4 and 7);
- **Government leading by example**, e.g. by adopting a mandatory government AI assurance and ethics framework (please refer to our answers above for detail);
- **Government supported 'sandbox' environment** to develop and test new AI applications (please see our answer to Question 3); and
- **consolidated AI education platform/centre tailored to the general public**, e.g. modelled on the AI Watch platform operated by the European Commission (please see our answer to Question 5).

Implications and infrastructure

Question 12. How would banning high-risk activities (like social scoring or facial recognition technology in certain circumstances) impact Australia's tech sector and our trade and exports with other countries?

FinTech Australia supports the proposal to ban certain very high-risk applications of AI like social scoring or facial recognition in certain circumstances. We anticipate that an approach consistent with that taken by the EU AI Act regarding high-risk activities will result in a positive impact on the trade and export of AI applications by ensuring cross-jurisdictional acceptance. However, some members propose that banning AI activities should only be reserved for such very high-risk applications with unacceptable, and to the extent possible, proven consequences associated with their use. A publicly available risk register and list of banned applications, supplemented with reasons for banning respective AI applications, is regarded as useful by some members.

FinTech Australia further submits that banning certain very high-risk activities which are not banned in other jurisdictions will have a substantial negative effect on Australia's technology sector and trade/export relationships. Unless a ban of such activities accounts for factors that are uniquely present in Australia, we consider that Australia's technology sector will likely be disadvantaged and innovation stifled as a consequence of risk-assessments which go beyond the conclusions reached in relation to high-risk AI applications and technologies in other jurisdictions.

Members prefer the body responsible for risk assessments to work with AI developers to achieve compliance with regulatory requirements, rather than banning controversial AI applications and technologies outright.

Question 13. What changes (if any) to Australian conformity infrastructure might be required to support assurance processes to mitigate against potential AI risks?

FinTech Australia submits that any changes made to the Australian conformity infrastructure should be informed by an in-depth infrastructure gap analysis prior to any changes being made. Further, members consider it preferable to focus on changes which are necessary to protect against substantial AI risks (e.g. other than low level risks), as an overly prescriptive approach may not be technology-neutral and thus not future-proof, and stifle AI innovation.

Risk-based approaches

Question 14. Do you support a risk-based approach for addressing potential AI risks? If not, is there a better approach?

Members largely support a risk-based approach to address the potential risk of AI. There is consensus among members that a more prescriptive and technology focused approach (such as that taken by China) is too onerous and, unless carefully monitored and revised frequently, would stifle innovation. In particular, members note prescriptive approaches may challenge SME AI developers and deployers by imposing artificial compliance hurdles. A risk-based approach, whether voluntary or mandatory, on the other hand would allow for the allocation of resources where the greatest benefit can be expected (e.g. prevention of harm), and encourage industry-led innovation and development of AI technologies through both technical and ethical guidance. We further note that a risk-based approach was also recently proposed in the Attorney General's Privacy Act Review Report[1] for high-risk privacy activities, and as such, a risk-based approach in the context of AI would be consistent with current regulatory proposals in related areas.

Question 15. What do you see as the main benefits or limitations of a risk-based approach? How can any limitations be overcome?

FinTech Australia considers a risk-based approach is commonly applied by organisations in relation to managing business risks and that larger members are well familiar with it. Further, applicable regulatory regimes, such as under the *Privacy Act 1988* (Cth) or the *Anti-Money*

[1] Privacy Act Review Report | Attorney-General's Department (ag.gov.au).

Laundering and Counter-Terrorism Financing Act 2006 (Cth), require risk-based assessments. As such, a risk-based approach would be consistent with existing regimes and members suggest that they would, to a degree, have the benefit of relying on existing compliance practices.

We note the evolving nature of AI applications may warrant more frequent and recurring assessments than those known from existing regimes, in particular in relation to high-risk AI applications. An underpinning and frequently updated regulatory guidance, e.g. for when re-assessments should take place and how post-market monitoring should occur is proposed by one member.

Question 16. Is a risk-based approach better suited to some sectors, AI applications or organisations than others based on organisation size, AI maturity and resources?

As outlined in our answer to Question 15, FinTech Australia notes some members may be able to rely on their risk-assessment and management expertise derived from compliance practices under existing regulatory frameworks. Smaller organisations which do not fall under such regimes may not necessarily have the benefit of such experience and may lack the resources to conduct risk assessments, in particular in relation to high-risk activities which require in-depth and frequent reviews. Members consider that in addition to government guidance around risk assessments and assessment criteria in the context of high and very high-risk AI applications, threshold requirements, such as related to an organisation's turnover, AI maturity or AI application reach, would allow SME AI developers and deployers to overcome potential risk compliance hurdles outside of a mandatory compliance framework.

Question 17. What elements should be in a risk-based approach for addressing potential AI risks? Do you support the elements presented in Attachment C?

Members are generally in support of the elements proposed in Attachment C in relation to internal risk-assessment and monitoring, such as conducting impact assessments for potential risks, human in the loop/oversight assessments and internal training requirements. It is suggested that human in the loop/oversight assessments should be limited to high-risk use cases where the benefit of human oversight outweighs the detrimental effect human intervention has on the efficiency of the application.

One member comments that consumer-facing elements, such as notices and explanations, may increase organisational accountability for AI developers and users, but may not result in increased trust by consumers. Rather, the member considers that, given the fact that an increasing amount of consumer products and applications is powered by AI, recurring notices, pop-up windows or possible consent requirements may overwhelm consumers and further distrust. The proposal made under the ongoing Privacy Act Reforms to inform consumers about automated decision-making processes is considered sufficient.

Question 18. How can an AI risk-based approach be incorporated into existing assessment frameworks (like privacy) or risk management processes to streamline and reduce potential duplication?

FinTech Australia considers existing and proposed frameworks, such as privacy impact assessments for high-risk processing activities as proposed under the Privacy Act reforms, should be leveraged to streamline approval or AI applications. Members propose that, except for banning very high-risk applications, existing and currently proposed frameworks sufficiently addressed the risks posed by AI applications for end-users. To the extent that existing frameworks are not considered sufficient, members note that risk assessments should be modelled in a way that allows for mutual recognition amongst both national and international regimes concerned with the regulation of AI.

Question 19. How might a risk-based approach apply to general purpose AI systems, such as large language models (LLMs) or multimodal foundation models (MFMs)?

FinTech Australia considers that the control elements proposed in Attachment C will need to be evaluated in an application-specific context. While not all elements may lend itself to the evaluation of LLMs or MFMs, we consider that a risk-based approach, driven by frequently reviewed, organisation-internal risk frameworks, will enable risk-based assessments of emerging AI uses.

Question 20. Should a risk-based approach for responsible AI be a voluntary or self-regulation tool or be mandated through regulation? And should it apply to:

Public or private organisations or both?

A risk-based approach should apply to public and private organisations alike. There was support among members for the proposal that development, deployment and post-market obligations should be mandated through regulation for very high-risk AI applications for both private and public organisations.

A risk-based approach in relation to low to medium risk AI applications should only be mandated through regulation for public organisations to facilitate public trust, and that a voluntary industry led approach based on best-practice standards may be followed by private organisations. Members propose that existing and upcoming regulatory compliance obligations, e.g. in relation to privacy impact assessments or disclosure of automated-decision making as proposed by the Privacy Act Reforms, sufficiently addressed the specific risks associated with the use of AI in relation to low to medium risk uses.

Developers or deployers or both?

To the extent that AI activities are regulated (e.g. in high to very high-risk contexts), members are of the view that developers and deployers should both be regulated, considering their interrelationship in relation to AI risk management. FinTech Australia notes that developers, who are responsible for conducting initial quality and risk assessments, rely on deployers to notify possible risks and to report any incidents and malfunctions to meet post-market monitoring. Deployers on the other hand, due to the volume of AI applications frequently implemented in a commercial context, rely on developer’s initial risk assessments and up-to-date technical documentation to decide whether an AI application is right for their business. Further, deployers as the initial point of contact for all consumer enquiries, should be enabled to explain and justify the use of respective AI applications.

Conclusion

FinTech Australia thanks the Department for the opportunity to provide views on such an important suite of issues, and greatly appreciates the work put into developing the Discussion Paper. We look forward to engaging in future consultations on ensuring safe and responsible use of artificial intelligence in Australia.