Australian Banking Association

ABA Submission

Exposure Draft – Privacy (Children's Online Privacy) Code 2026

Office of the Australian Information Commissioner

5 June 2026

Australian Banking Association

Table of Contents

Policy Lead: **Arad Moradian** (Policy Director) arad.moradian@ausbanking.org.au

About the ABA

The Australian Banking Association advocates for a strong, competitive and innovative banking industry that delivers excellent and equitable outcomes for customers. We promote and encourage policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership.

Australian Banking Association

ABA submission to the OAIC

The ABA welcomes the opportunity to respond to the Office of the Australian Information Commissioner's (**OAIC**) Exposure Draft of the *Privacy (Children's Online Privacy) Code 2026* (the **Code**) and the accompanying Explanatory Statement.

The ABA and its members acknowledge the Government's concerns regarding the handling of children's personal information in an online environment and support the policy objective of the Code to strengthen children's privacy protections. This submission addresses the practical implications of the Code in the banking industry, which uniquely operates within a highly regulated environment and is already subject to substantial consumer protection, privacy, prudential, conduct and financial crime obligations.

For our members, personal information is primarily collected and handled to provide financial products and services, and to comply with regulatory obligations, including know your customer (**KYC**), anti-money laundering and counter-terrorism financing (**AML/CTF**), taxation law, prudential and conduct requirements. That personal information is held in highly secure environments and is not intended for public dissemination. Substantial consumer protection laws already exist within banking, and the privacy risks to children are significantly lower than in sectors where children's personal information may be publicly available or monetised.

While the ABA acknowledges that the Code is intended to apply to a service level rather than an entity level, the ABA recommends that the OAIC should ensure that for the banking sector, the Code's obligations are proportionate, calibrated to operate coherently with existing banking sector regulation, and avoid regulatory duplication. This is of particular significance given that implementation of certain obligations may be operationally challenging and deliver limited additional benefit to children, when considered in the context of the banking sector's core offering to children - namely, facilitating access to and management of their funds.

Further, banking products are generally designed to be age agnostic, and for some ABA members children represent as little as 1% of the accounts they hold. In that context, requiring differentiated, child-specific solutions would be operationally difficult and, in many cases, require disproportionately complex technical changes across products and systems. That burden is difficult to justify where the relevant products and services pose a relatively low child-specific privacy risk, and where it is unclear what additional regulatory benefit would be achieved in the banking context.

While the ABA supports the objective of strengthening children's privacy protections online, the ABA makes the following key recommendations to ensure that the Code's regulatory burden is proportionate, does not undermine existing regulatory obligations, does not pre-empt broader legislative reform and can be implemented by ABA members:

Key recommendations

Recommendation 1: Defer obligations that anticipate Privacy Act reforms that have not yet been legislated. The ABA holds concerns that the Code introduces concepts and obligations ahead of the broader reforms to the *Privacy Act 1988* (Cth) (**Privacy Act**), which are still under consideration by the Attorney-General's Department. Any pending obligations which are being considered as part of the Privacy Act Review – Report 2022 (**PAR**) should be settled by the Parliament before they are imposed through a subordinate legislative instrument to avoid the risk of inconsistency with the broader PAR reforms.

Recommendation 2: If the Code proceeds in its current form ahead of legislative reform, it is recommended that necessary clarifications and amendments are included to ensure the Code is operationally feasible for the banking sector:

Recommendation 2.1: Consider whether aspects of the Code may be inconsistent with the Australian Privacy Principles (APPs), within the meaning of section 26C(3)(a) of the Privacy Act.

Recommendation 2.2: Include an express exclusion from section 7 of the Code for risk management and compliance related activities undertaken by financial institutions. These activities serve a clear public interest and are often necessary to protect children and the integrity of the banking system, even where the relevant legal right or obligation has not yet been enlivened.

Recommendation 2.3: Amend or clarify key provisions so that highly regulated entities can practically comply. This is critical to ensure the Code operates coherently with existing regulatory frameworks in the banking sector.

Recommendation 2.4: The Code should adopt an age of consent of 14. In the banking context, lowering the minimum age of consent would reduce unnecessary friction, better align with the age at which many children begin engaging more independently with work, income and basic banking, and support children's ability to access and manage their money, without undermining their financial autonomy and literacy.

Recommendation 2.5: The OAIC should publish guidance on key concepts in the Code well in advance of any required commencement date. Highly regulated entities cannot reasonably design, build and implement compliant systems without guidance on scope, key definitions and the operation of core obligations.

Recommendation 3: The OAIC should limit regulatory duplication and confirm whether existing regulatory frameworks and equivalent controls satisfy the Code's operational obligations where they achieve identical or near identical outcomes.

Recommendation 4: The Code should set a commencement date of at least 24 months from the Code registration date to allow the banking sector sufficient time to implement and comply. The scale of technical changes required to existing systems architecture, governance and design means implementation will not be feasible without an appropriate transition period and supported by regulatory guidance published with sufficient lead time.

Australian Banking Association

Recommendation 1: Defer obligations that anticipate Privacy Act reforms the Government has not yet legislated.

The ABA recommends that obligations in the Code which overlap with reforms the Government has agreed in principle to progress in its response to the PAR should not be finalised through the Code ahead of the broader legislative framework. Several provisions introduce concepts that are, in the ABA's view, identical or substantially similar to proposals agreed in principle by the Government in its 2023 response to the PAR, that have not yet been legislated. Settling these proposals through a subordinate instrument before the primary legislation risks inconsistency, duplication, parallel regimes and a potential need for re-implementation following legislative reform.

The ABA has identified the following areas where the Code codifies concepts identical or substantially similar to unlegislated PAR reform proposals agreed in principle:

- **Section 32: Right to destruction of personal information**
  Section 32 introduces a right for a child, or a person with parental responsibility where the child is under 15 or lacks capacity, to request the destruction of personal information held by an entity. This right does not currently exist in the Privacy Act. It is similar in substance to the general right to erasure proposed by the PAR (Proposal 18.3), which the Government agreed to in principle but has not legislated. The ABA further notes that the Productivity Commission has since recommended against introducing a GDPR-style right to erasure in Australia (Productivity Commission, *Harnessing data and digital technology*, Inquiry report no. 111, 2025, p. 180). Codifying this right for children through the Code would pre-empt both an unsettled reform and an express recommendation that it does not proceed for individuals generally.

- **Section 9: Strictly necessary threshold**
  Section 9 introduces a *"strictly necessary"* test for the default collection, use and disclosure of children's personal information. While the Explanatory Statement confirms that entities may continue to collect children's personal information where it is *"reasonably necessary"* under Australian Privacy Principle (**APP**) 3.2 for their functions or activities, the effect of section 9 is to limit default collection. This sits in the same territory as the *"fair and reasonable"* test proposed under the PAR (Proposal 12.1) which the Government agreed to in principle but has not legislated. Practically, this would result in a new collection standard for children ahead of the proposed *"fair and reasonable"* baseline considered under Proposal 12.1. The cumulative effect is multiple overlapping tests governing the same consideration, which is overly duplicative.

- **Section 11: Removal of reasonable expectations exception**
  Section 11 removes the ability for entities to rely on the *"reasonable expectations"* exception under APP 6.2(a) as a basis to use or disclose a child's personal information for a secondary purpose. As noted, proposal 12.1 of the PAR which the Government agreed to in principle is expected to reform the use and disclosure framework, applying the proposed *"fair and reasonable test"*. The Code eliminates this exception for children before Proposal 12.1 has determined how it should operate within the reformed framework.

- **Section 28: Right to request information about handling of personal information**
  Section 28 expands transparency rights for children beyond existing obligations under APP 12, including the ability to request information about the categories of information held, its sources, purposes, recipients, retention periods, and any automated decision-making or profiling. This overlaps the PAR's proposed enhancement of individual rights, including expanded access and transparency (Proposals 18.1 to 18.5 of the PAR), which the Government agreed to in principle but has not legislated.

- **Division 2: Consent framework**
  Division 2 introduces a detailed consent framework for children, which is only valid for 12 months. These requirements mirror the PAR's proposal to codify the definition of consent in those same terms (Proposal 11), which the Government agreed in principle but has not yet legislated. The Code would fix the mechanics of consent for children before the primary legislation has settled them for individuals generally.

In each case identified above, the concern is that the Code would establish a separate framework for children ahead of any potential amendments to the primary legislation. If the two frameworks diverge, or the reforms adopt a modified approach that must then flow through to children, regulated entities will be required to unnecessarily pivot and re-implement. The ABA recommends that these obligations be deferred until the relevant reforms have been settled by Parliament.

Recommendation 2: If the Code proceeds in its current form ahead of legislative reform, it is recommended that necessary clarifications and amendments are included to ensure the Code is operationally feasible in the banking sector

The ABA has identified a number of regulatory coherence issues that remain paramount to the banking sector as the Code is developed and finalised. These concerns relate to the interplay between the Code and existing regulatory frameworks applicable to banking. If the OAIC proceeds to finalise these obligations, it is essential that the matters below are either amended or clarified to ensure that the Code is operationally feasible.

Recommendation 2.1: Consider whether aspects of the Code are inconsistent with the Australian Privacy Principles, within the meaning of section 26C(3)(a) of the Privacy Act

Section 26C(3)(a) of the Privacy Act requires that an APP code must not be contrary to, or inconsistent with, the APPs. The ABA is concerned that certain requirements of the Code, particularly where they detract, or take away rights, from existing statutory protections (for example, section 11's effect on the APP 6.2 reasonable expectations exception) or apply a different legal test (for example, the *"strictly necessary"* threshold in section 9, as against the *"reasonably necessary"* test in APP 3.2), may be inconsistent with the APPs. The potential consequence is that the Code may be beyond the OAIC's legislative powers, and partially invalid. The ABA requests that the OAIC clarify how these provisions are intended to operate consistently with the APPs and amend the drafting where necessary to ensure compliance with section 26C(3)(a).

Recommendation 2.2: Include an express exclusion from section 7 of the Code for risk management and compliance related activities undertaken by financial institutions

As a threshold matter, the ABA recommends that the Code expressly exclude risk management and compliance related activities from the scope of the Code. For example, this would include activities undertaken to comply with AML/CTF obligations, detect and prevent fraud and scams, identify and respond to financial abuse, and fulfil regulatory reporting requirements.

In our view, these activities are not related to the provision of a designated internet service that is likely to be accessed by children, or primarily concerned with the activities of children. Given the operation of section 7 serves to define which activities the Code's requirements apply to, this exception will better reflect that the Code is not intended to affect or restrict all activities conducted by regulated entities. This will provide greater clarity, certainty and improve the ability to address the privacy risks that may arise in the course of activities that are *'likely to be accessed by children*' or '*primarily concerned with the activities of children*' as contemplated in section 7.

Australian Banking Association

Recommendation 2.3: Amend or clarify key provisions so that highly regulated entities can practically comply

Section 32: Right to destruction of personal information

The ABA notes significant operational concerns with the proposal to introduce a right of destruction. Relevantly, no equivalent right exists for adults, which risks creating a two-tier system that is different for adults and children. In these circumstances, the ABA recommends that it would be more appropriate for a right of destruction to be introduced into the primary legislation, rather than via a Code.

In any case, having regard to the large, complex, highly intricate and protected systems that banks operate, a right of destruction would be technically difficult to operationalise, introduce unnecessary complexity and be disproportionately onerous to comply with relative to the benefit of destruction. Banks are subject to extensive mandatory data retention obligations under AML/CTF legislation, prudential standards, taxation law, and other regulatory frameworks. While section 32(3) of the Code provides an exception where retention is required or authorised by law, it is unclear how that exception is intended to operate in circumstances where the continued handling of information may still be necessary to protect the account or the customer, but an express legal retention obligation is not enlivened. This includes fraud and scam detection, account protection measures, risk protocols and controls, and the detection and management of mule account activity, noting that children's accounts may be targeted for misuse in this way.

Further, the ABA notes that this broadly framed right of destruction may be exploited by bad faith actors to purge information that would otherwise support the detection and investigation of financial crimes involving children's accounts. This provision as drafted risks undermining anti-fraud and AML/CTF controls and may conflict with obligations to maintain secure and resilient systems, including, where applicable, under the *Security of Critical Infrastructure Act 2018* (Cth). It is also unclear how the provision is intended to operate alongside evolving regulatory settings such as the scam prevention frameworks.

For these reasons, if the Code retains this provision, per recommendation 2.2 above, the Code should therefore expressly recognise that there will be circumstances in which the continued retention of personal information is in the public interest, such as for account protection, fraud prevention and risk management, even if an express legal retention obligation has not yet been enlivened. This would ensure the provision operates appropriately across services that require ongoing monitoring, risk detection and intervention capabilities, and does not inadvertently prioritise destruction outcomes in a manner that may compromise the safety and protection of children. Alternatively, this right should be limited to specific entities that hold publicly available information about children.

The ABA also notes that the Code mandates destruction as the default response, rather than permitting de-identification. In complex data environments, including legacy systems and backup or archival environments, de-identification may achieve the same privacy outcome while allowing entities to manage legitimate risk, fraud and compliance functions. The ABA recommends that the Code expressly permit de-identification, as an alternative to destruction.

In the current drafting of section 32, there is some ambiguity about whether a child of any age has the right to request destruction. To align with the remainder of the Code, the ABA suggests this right is only extended to children from the minimum age of consent (unless the child lacks capacity) and in other circumstances the right lies with the person with parental or guardian responsibility.

Section 9: Strictly necessary threshold

Banks collect, use and disclose customer personal information about a child for ancillary activities to the delivery of a financial service, including to detect fraud, prevent scams, financial crime compliance, security monitoring, complaint handling and to support vulnerable children. These are not "*optional elements*" to be switched off by default – they are critical activities designed to meet regulatory requirements or address community expectations.

A requirement to implement technical and organisational controls that, by default, only permit banks to collect, use and disclose customer personal information that is "*strictly necessary*" for a banking *"service"* may inadvertently limit critical banking activities. Much depends on the OAIC's confirming it will take an expansive interpretation of an entity's *"service"* to include these critical ancillary activities.

Further, the *"strictly necessary"* standard introduces a threshold that is narrower than the current *"reasonably necessary"* test under APP 3.2 and narrower than the *"fair and reasonable"* test contemplated by the Government's proposed reforms to the Privacy Act. In a banking context, this creates practical difficulty. While the explanatory statement provides that section 9 *"does not narrow or restrict the operation of APP 3.1 or 3.2,"* in effect, the 'default' requirement appears irreconcilable with APP 3.2 under which banks lawfully collect, use and disclose personal information for these ancillary activities that clearly fall within their *"functions and activities."*

The ABA recommends that the Code clarify that information collected, used or disclosed by default to meet regulatory obligations, to protect the security and integrity of the service, or to detect and prevent fraud and scams, is taken to satisfy the *"strictly necessary"* threshold.

Section 11: Removal of reasonable expectations exception

The drafting of Section 11 of the Code suggests that any use or disclosure of a child's personal information, whether in respect to a primary or secondary purpose, must be with the child's consent and in their best interests.

It is not clear whether the drafting of section 11 is intended to limit the use or disclosure of a child's personal information for the primary purpose of collection or it is intended to apply to uses or disclosures for secondary purposes only. If the provision is retained, it is recommended that this is explicitly clarified in the drafting of the Code. In any event, removing the ability for banks to rely on APP 6.1(b) in respect of the use or disclosure of a child's personal information for secondary purposes is significant. It will create extensive operational challenges for banking activities where it is not appropriate to obtain individual consent, and where the *"authorised or required by law"* exception in APP 6.2(b) or the permitted general situation at section 16A Item 2 of the Privacy Act cannot be relied upon.

In facilitating financial products or services, banks undertake complex activities designed to protect, support and assist customers, particularly in respect to fraud and scams detection. In circumstances where the APP Guidelines state that the primary purpose for collection, use or disclosure should be construed narrowly rather than expansively, it is probable these activities will be regarded as uses for secondary purposes where the *"reasonable expectations"* exception would ordinarily be relied on. While the ABA notes that uses required or authorised by law will continue to be permitted under APP 6.2(b), the removal of the *"reasonable expectations"* exception will adversely affect a range of routine, low-risk uses that are not legally mandated but are clearly within the scope of what a reasonable person would expect. An example of this is outlined below.

Some banks currently employ models that use the personal information of customers, including children, to identify patterns of transactions which may indicate technology facilitated abuse of a customer, irrespective of age. The purpose of these models is to identify individuals using online banking transfers to send abusive messages in the description of transfers to another person.

The output of the model is used by relevant support teams to respond to and action. While these models evidently operate in the best interests of customers, it is not practicable or appropriate to obtain consent for its application at an individual level, particularly when it is applied at scale. If the Code were applied to this activity under APP 6.1, this would result in the exclusion of customers under 18 from the model which will:

(a) adversely affect how banks can detect and assist customers who are minors experiencing abuse;

(b) limit the extent to which banks can identify harm to children and may make them more vulnerable to financial abuse, coercion, grooming or exploitation; and

(c) reduce recall and distort risk signals in the training and monitoring population.

In lieu of a blanket removal of the exceptions for secondary uses or disclosures in APP 6.1(b), the ABA recommends that the OAIC consider retaining the *"reasonable expectations"* exception in APP 6.2(a). Alternatively, the ABA recommends that a new exception to section 11(1) of the Code is introduced for secondary uses or disclosures that provide a public benefit, are directed to the prevention of fraud, scams or financial crime, or are undertaken for risk and compliance purposes under another legislative or regulatory framework (for example, AML/CTF Act 2006 (Cth)).

Section 28: Right to request information about handling of personal information

The ABA does not oppose transparency in principle. However, the introduction of this right duplicates transparency requirements proposed under other provisions within the Code including section 20 (assent to particular purpose), section 23 (APP Privacy Policy) and section 24 (Notice of Collection).

Further, section 28 introduces a level of detail that goes significantly beyond existing obligations in APP 12 and APP 1.3, including the requirement to disclose categories of information held, sources, recipients, retention periods, and the application of automated decision-making or profiling at an individual level that is not contemplated in the upcoming introduction of APPs 1.7-1.9. Additionally, it is not made clear by the Code or Explanatory Statement the specific gap that section 28 seeks to address that is not already covered by the above APP requirements.

Additional clarification is required as to how this right applies where personal information relating to a child is held only indirectly, including where it is linked to another customer or third party. The ABA recommends that the obligation be aligned with existing APP 12 requirements, with any additional transparency requirements deferred to the Government's proposed further reforms to the Privacy Act, where they can be considered as part of a coherent individual rights framework.

Division 2: Consent framework

The ABA holds the following concerns regarding the application of Division 2 to banking products and services:

- Section 15(4)(b) specifies that consent in respect to the collection and handling of children's personal information is only valid for 12 months. This consent model does not reflect the ongoing nature of banking relationships. A customer who opens a bank account at age 14 should not be required to re-consent annually to the handling of their personal information for the same ongoing service. Strict application of the 12-month consent period may require entities to restrict a child's access to their funds, or to essential banking services, where consent is not renewed in time. This gives rise to a real risk of financial exclusion for children who do not, or cannot, renew their consent, including an inability to access their own funds. Such an outcome would disproportionately disadvantage children and may place them in a worse position than adult customers, particularly where the child handles their funds autonomously and may not be able to easily seek a parent or guardian to re-consent.

  The Code also assumes that where a child is under the age of 15, consent will be provided by a person with parental responsibility. In banking, products for minors may be opened, administered or operated by signatories or other persons who do not hold parental responsibility. The ABA recommends that the Code clarify how the consent framework applies in these scenarios, including where parental responsibility is shared or where the person managing the account is not the child's parent, legal guardian or legally responsible for the child's day-to-day care, welfare and development.

  This risks service disruption where consent lapses and creates an administrative burden for both the entity and the customer with little tangible benefit.

  For the reasons outlined above, the ABA recommends that consent provided for a collection, use or disclosure in connection with an ongoing banking product or service ought to remain valid for the duration of that product or service, subject to an individual withdrawing their consent.

- In the ABA's view, the requirement for a child's assent, in addition to the consent of a person with parental responsibility, appears to operate as a double consent model. In this context, it is not clear whether assent is tied to consent – that is, where a person with parental responsibility provides consent for a child under the age of 15 and the child's assent is also obtained, it is unclear whether that assent must be refreshed in the same manner, and on the same 12-month cycle, as consent. The ABA further notes that the Explanatory Statement indicates that a child's assent is not required where a person with parental responsibility has already provided consent to the handling of the child's personal information for a specific purpose. This position is not explicitly reflected in the drafting of the Code and should be clarified to ensure consistency between the Code and the Explanatory Statement.

Section 38: Privacy Impact Assessments (PIA)

Section 38 of the Code requires entities to conduct a PIA for new services or activities that are likely to be accessed by children, or where an entity proposes to adopt any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of children.

The ABA seeks clarification on the scope of this obligation. Banks offer a wide range of products and services, many of which may be accessed by children. A requirement to conduct PIAs for each of those services or activities represents a significant compliance burden. To this end, it is recommended that the requirement to conduct PIAs is limited to high-risk services and activities

involving children's personal information. Additionally, the ABA requests that the OAIC provide further guidance on the following:

(a) clarifying how '*significant impact on the privacy of children*' is intended to be interpreted and applied in practice; and

(b) assurance that the obligation does not apply retrospectively. That is, it applies to new or updated activities from the commencement date.

The Code requires entities to publish a register of PIAs online (section 39(2)) and to provide copies of PIAs that are listed on the register to the Commissioner on request (section 39(3)). During the roundtable, the OAIC indicated this obligation would require entities to maintain a public register that states the name and date a PIA was conducted, in a similar manner to what is required for agencies under the *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Cth). That is, entities would not be required to publish the PIA or include information that could expose sensitive internal controls, compliance arrangements or security settings. The ABA requests that this position is explicitly confirmed by the OAIC in guidance.

Recommendation 2.4: For banking products and services, the Code should adopt an age of consent of 14

The Code proposes to introduce a minimum age of consent of 15 years old. If a child is below the age of 15, consent to the collection, use or disclosure of a child's personal information must be from a person with parental responsibility for the child, subject to limited exceptions.

In a banking context, the establishment of a minimum age of consent of 15 creates significant complexity for how banks offer products and services to children. This is because it is common for children under the age of 15 to independently own and operate bank accounts without parental or guardian consent. Although the minimum age to open an account independently varies across financial institutions in Australia, it is generally 14 years old.

A proposed consent age of 15 is particularly problematic in circumstances where the minimum age to work in many states or territories is below 15. The practical implication is that children can work and earn an income, while being unable to operate a bank account and manage their money without parental or guardian consent. This may adversely affect a child's financial autonomy and inclusion, and the development of their financial literacy. These concerns are reinforced by research into children's financial engagement: ASIC has found that children aged 5 to 12 are learning about money at school, while teenagers aged 13 to 17 are making independent financial decisions (ASIC, *Young people and money*, December 2021). More broadly, financial literacy is developed through the gradual introduction of children to financial transactions and banking services. Limiting access to these services through higher consent thresholds may therefore be counterproductive, and adopting an age of consent of 15 would negatively impact children in the banking sector.

Having regard to the above circumstances, the ABA recommends that the minimum age of consent is amended to 14 years of age for banking products and services.

Recommendation 2.5: The OAIC should publish guidance on key concepts in the Code well in advance of any required commencement date

On the 11 May 2026, the OAIC indicated in the roundtable that it intends to publish guidance on key concepts in the Code and to develop an implementation roadmap. The ABA welcomes this commitment. However, the scope, content and timing of that guidance have not been confirmed. The ABA considers it essential that guidance on key concepts is finalised and made available to regulated entities, with sufficient lead time before the required commencement date. In the absence of guidance,

entities cannot reasonably design, build and implement compliant systems. The ABA has identified the following concepts that require regulatory guidance as a priority.

Scope, including *"likely to be accessed by children"* and the application of *"designated internet service"* to banking services

The Explanatory Statement indicates that the Code is intended to apply to specific services that are *"likely to be accessed by children"*, rather than all services provided by an entity. However, the threshold for when a service is considered *"likely to be accessed by children"* is unclear.

While the Explanatory Statement provides a banking specific example, it is insufficient to address the range of issues that arise in practice. A bank's website, mobile application, online banking platform, educational content, disclosure documents and public webpages may all be accessed by children in some manner, even where those services are not designed for them. Further, it is common for general products such as everyday transactions and savings accounts to be offered to both adults and children, while not specifically targeting children.

While the OAIC has referred to its intent to develop guidance that is broadly aligned with the United Kingdom Information Commissioner's Office guidance on *"likely to be accessed by children"*, until equivalent guidance is provided in the Australian jurisdiction, it will not be possible for regulated entities to meaningfully assess with certainty whether its products or services fall within the scope of the Code. To this end, clarification is required on how the *"likely to be accessed by children"* threshold applies to mixed-audience and general-purpose banking services, and how terms such as *"designated internet service"* are intended to apply in the financial services context. This should include whether publicly accessible pages, product disclosure materials and online educational content are captured. The threshold should be directed at services designed for, directed to, or with a material proportion of child users, rather than services that a child could theoretically access.

The ABA recommends OAIC guidance confirm that entities may evidence material proportion using a combination of:

- **Observed usage data** (e.g., authenticated user age/KYC-held age for logged-in services, and analytics for unauthenticated services);
- **Intended audience and design signals** (product positioning, onboarding eligibility rules, youth-specific journeys);
- **Feature-based risk indicators** (whether the service enables account creation, messaging, sharing, profiling, geolocation, or other higher-risk functionality); and
- **Reasonable sampling and proxy measures** where age is not known (noting the Code's requirement to take steps reasonable in the circumstances to ascertain age, having regard to risk).

The ABA further recommends OAIC guidance clarify that where a service is not designed for or directed to children and available evidence indicates no material proportion of child users, the service should not be treated as *"likely to be accessed by children"* solely because it is technically accessible.

Strictly necessary

The Explanatory Statement confirms that the *"strictly necessary"* threshold under section 9 applies to default settings and does not displace APP 3.2. However, this clarification is contained only in the Explanatory Statement and is not reflected in the drafting of the Code

itself. The ABA recommends that this position be expressly incorporated into the Code to provide legal certainty, rather than relying on the Explanatory Statement alone. Further, the practical distinction between what is *"strictly necessary"* to provide the service, what is *"reasonably necessary"* for the entity's functions, and what may be required under other regulatory frameworks (including KYC, AML/CTF, fraud and scam prevention) is unclear. The OAIC should provide guidance on how *"strictly necessary"* is to be interpreted in the context of the banking sector, including whether information collected to meet regulatory obligations or to protect the security and integrity of the service satisfies this threshold.

Best interests of the child

The ABA supports the principle that the *"best interests of the child"* should be a primary consideration. However, the Code does not provide sufficient guidance on how this standard is to be operationalised in practice. While the Explanatory Statement broadly refers to certain factors' entities should have regard to when assessing the best interests of the child, it would be more appropriate for these factors to be specified directly in the Code. Further, applying this standard to the design and operation of financial services at scale requires practical examples relevant to banking products, mixed-audience services, safety and fraud controls, and online account management tools. The OAIC should develop sector-specific guidance to assist ABA members in applying the *"best interests of the child"* standard in a consistent and proportionate manner so as to avoid generalised assumptions being made about children across various age brackets.

Consent, assent, and age-appropriate notice

The Code introduces distinct concepts of consent and assent, with different requirements depending on the age of the child. The OAIC should provide guidance on how assent differs from consent in practice, how each is to be obtained and evidenced in digital journeys, what constitutes an age-appropriate notice, and whether such notices can sit within existing APP 5 collection notices or require standalone mechanisms.

Commencement and transitional arrangements

The ABA recommends that the OAIC clarify whether the Code applies only to new collections, uses and disclosures of children's personal information occurring after commencement, or whether it will also apply to the ongoing processing of children's personal information that was collected before commencement. The ABA further recommends that the OAIC confirm that the Code will not retroactively invalidate processing that was lawful prior to commencement.

Recommendation 3: The OAIC should limit regulatory duplication and confirm whether existing regulatory frameworks and equivalent controls satisfy the Code's operational obligations where they achieve identical or near identical outcomes

Age assurance (section 8)

Section 8 requires entities to take steps that are reasonable in the circumstances to ascertain the age of end-users, having regard to the risk of harm that may arise from the collection, use or disclosure of personal information. The ABA notes that banks already hold verified identity information on their customers through KYC processes and are well placed to determine the age of an account holder. The ABA recommends that the OAIC confirm that existing KYC and identity verification processes satisfy the requirements of section 8 for regulated financial services entities. Clarification is also required as to whether any age assurance expectations apply to publicly accessible webpages or services that do not involve an authenticated customer relationship.

Complaints handling (sections 34 to 36)

Division 7 of the Code (sections 34 to 36) requires entities to provide children with information about their privacy rights and to embed child-friendly inquiry and complaints processes into their services. Banks are already subject to detailed complaints handling requirements under the Australian Securities and Investments Commission's Regulatory Guide 271 pertaining to Internal Dispute Resolution and are members of the Australian Financial Complaints Authority. The ABA recommends that guidance is provided which recognises that existing internal and external dispute resolution frameworks which are updated (such as to include child friendly language), are sufficient to satisfy the obligations under Division 7, rather than requiring the establishment of parallel mechanisms.

Notification of control or monitoring mechanisms (section 33)

Section 33 requires entities to notify a child where a mechanism is provided that enables a person with parental responsibility to control or monitor the child's use of the service, or monitor the child's geolocation data. 'Geolocation data' is not defined in the Code and there is little guidance on how this provision is intended to practically apply.

Many banks offer youth accounts for children under a certain age (e.g. 14 years of age), where a parent or guardian is required to open the account. For these accounts, certain parental oversight features are generally available, which enables persons with parental responsibility to access and/or have control of spending limits, transaction notifications, and account monitoring functionality. This data, particularly in-person purchases may reveal a child's location. Under the current drafting of section 33, it is not clear whether this would be classified as 'monitoring geolocation activity' that would require constant notice to the child.

The ABA seeks clarification on how section 33 applies to standard parental controls offered as part of banking products for minors, and whether existing disclosure and notification practices are sufficient to meet this obligation.

Recommendation 4: The Code should set a commencement date of at least 24 months from the Code registration date to allow the banking sector sufficient time to implement and comply

The ABA recommends that the OAIC adopt a longer implementation period of 24 months, or a phased commencement model supported by timely guidance and a roadmap that allows entities to design, build and test compliant systems in an orderly way.

While the Code must be registered by 10 December 2026, its commencement date has not yet been determined. If the Code were to commence the day after registration on 11 December 2026, it would not be possible to practically implement the scale and complexity of the changes required across systems, consent mechanisms, governance frameworks, customer communications and digital service design to achieve compliance. Specifically, the proposed obligations relating to privacy-by-default settings, consent and assent, destruction requests and service redesign are likely to require substantial system changes across multiple products and channels. Additionally, both digital and non-digital origination channels will be affected, requiring not only technical design changes but also a review of existing mandatory disclosures (such as Target Market Determinations and Product Disclosure Statements) that are already in place.

To support the case for a phased commencement, ABA members are willing to contribute further detail to the OAIC on how a phased implementation plan could be structured in practice. At a high level, subject to confirmation around scope, a number of obligations could be addressed by leveraging existing regulatory processes and frameworks already identified above in Recommendation 3.

However, other obligations will not be feasible to design or implement without the OAIC first publishing guidance on key concepts and the intended scope of certain provisions, including those identified in this submission. Further still, a number of obligations will require significant system and process changes across multiple products and channels, including the design, testing and deployment of new consent and notification mechanisms, which will require substantial additional time. The ABA would welcome the opportunity to provide further information to the OAIC on the practical sequencing of these requirements to assist in the development of an implementation roadmap.

In the absence of sufficient time and guidance on how certain provisions are intended to be interpreted and applied, there is a real risk that ambiguity and a lack of clarity around compliance requirements may result in poorer outcomes for children. That outcome would be contrary to the OAIC's stated objective of protecting children within the digital world, not preventing them from engaging in it.