5 June 2026

[redacted]
General Manager
Regulatory Intelligence and Strategy Division
Office of the Australian Information Commissioner

Via email copc@oaic.gov.au

[redacted]

Draft Children's Online Privacy Code

The Customer Owned Banking Association (COBA) welcomes the opportunity to provide feedback on the Office of the Australian Information Commissioner's (OAIC) consultation on the draft Children's Online Privacy Code (the Code).

COBA is the industry association for Australia's customer-owned banks (mutual banks and credit unions). Collectively, our sector serves over 5.4 million Australians with purpose-led banking, delivering competition, diversity and market-leading levels of customer satisfaction in the retail banking market. Financial inclusion goes to the heart of who we are; customer-owned banks were originally formed as a self-help solution by communities to ensure everyone had access to fair financial services, and this commitment remains a cornerstone of our model today.

Accordingly, the customer-owned banking sector strongly supports the underlying objective of enhancing online privacy and safety protections for children. While we welcome many aspects of the draft Code, we wish to highlight specific rules where the practical application conflicts with banking regulations and practices. Because retail banking is structured around rigorous legal identification and long-term financial security, applying obligations designed for the wider digital environment risks disrupting the very consumers those measures seek to protect.

Our main concern is that certain rules in the Code may inadvertently result in financial exclusion for young people by unintentionally limiting their access to essential banking services. This risk is particularly concerning for our most vulnerable youth, such as those in state care whose parents may be absent or incarcerated. These individuals rely on bank accounts to receive government support payments, and requiring parental consent in these scenarios would be unworkable.

Several of the proposed rules may also directly conflict with existing regulatory frameworks for banks. For example, the proposed right to request an organisation to destroy a child's personal data could contradict the aims of existing anti-money laundering and counter-terrorism financing (AML/CTF) and other crime prevention laws. This could inadvertently expose youth to exploitation by criminals for both financial and other crimes due to their being treated differently from adults.

Furthermore, banks are already subject to extensive regulation, and layering on complex digital compliance frameworks requires significant resource scale and technical capacity to maintain dual privacy and age-assurance systems. This operational burden could disproportionately reduce the ability of smaller banks to compete or invest in adhering to these reforms. Consequently, smaller institutions may choose to withdraw from the youth market entirely, reducing consumer choice and further concentrating the banking market.

Accordingly, as providers of an essential service and highly regulated entities subject to existing consumer protection frameworks, we propose changes to the Code to not contradict existing laws and allow for flexibility for Authorised Deposit-taking Institutions (ADIs) on specific measures.

Key points

Implementing a restrictive age limit and an annual consent-refresh mechanism creates operational barriers that risk excluding young customers and disrupting active accounts. Raising the age threshold to 15 impacts financial inclusion, particularly for vulnerable minors – such as youth in state care or self-sufficient teens – who rely on independent account access to receive employment wages without parental intervention.

The Code proposes that children and their parents/guardians have the legal right to request an organisation destroy personal information held about the child. However, banks are subject to strict recordkeeping obligations, including under new AML/CTF legislation. To resolve this regulatory conflict, the Code should explicitly exclude ADIs from these destruction requirements or provide flexibility to how banks comply with the obligation.

In addition, we note that this proposed advanced deletion mechanism exceeds current Privacy Act frameworks and introduces 'right to be forgotten' concepts slated for future tranches of privacy reform. This would create a fragmented compliance model between minor and adult consumers, as this right would cease to apply once the account holder turns 18.

When it comes to marketing to children, ADIs are already subject to product Design and Distribution Obligations (DDO) and ASIC regulatory expectations in relation to financial services marketing.

Publishing a Privacy Impact Assessment (PIA) register online poses material security and commercial risks for banks and their customers. Even high-level summaries can allow sophisticated actors to infer details about system architecture, identify control gaps, or map out potential vulnerabilities. While we support institutions maintaining an internal register, we propose access should be restricted to production upon request by the OAIC or the Commissioner.

COBA strongly urges the OAIC to provide guidance before the framework takes effect, ensuring institutions have the regulatory certainty needed to comply without disrupting services. Further, as customer-owned banks operate on a smaller scale, implementing these technical changes may take considerable time. Consequently, we request an extended implementation period for customer-owned banks to ensure a smooth, compliant transition.

Rather than introducing measures that might inadvertently discourage ADIs from serving younger demographics, we welcome the opportunity to work collaboratively with the OAIC on some aspects of the Code. More detailed consideration of specific elements of the Code can be found at **Appendix A** of our submission. By ensuring the final framework balances robust privacy safeguards with the practical realities of a highly regulated financial ecosystem, we can protect young people while preserving their access to safe, modern banking services.

We thank the OAIC for taking our views into account. Please do not hesitate to contact [redacted] if you have any questions about our submission.

Yours sincerely

[redacted]

Chief Executive Officer

Appendix A – COBA comments on draft Children's Online Privacy Code

No.	Proposal	COBA comment

1	S15 - Consent must be informed	• Increasing the minimum age would require significant changes to onboarding, systems, and Terms & Conditions.
		• Many customer-owned banks allow customers under the age of 15 to operate deposit accounts (not credit products). In Australia, a Tax File Number may be obtained without a parent or guardian from the age of 13, which is typically the age many begin casual employment and require accounts for salary deposits.
		• Increasing the age threshold to 15 risks compromising financial inclusion, particularly for vulnerable minors such as those in state care or self-sufficient youth who require independent bank account access to receive employment wages without parental intervention.
		• A COBA member has shared its direct operational experience, which highlights that setting the minimum age requirement at 15 years of age would have negative impacts on vulnerable people under that age who need a bank account. The member also stressed how restricting account opening for minors to situations where parental or guardian consent is available would result in financial exclusion:
		  ○ The customer-owned bank is periodically approached by caseworkers from a state government Youth Justice agency seeking to open bank accounts for young people in their care.
		  ○ These young people are often not attending school, do not have a parent available or willing to be involved, and may be under legal guardianship arrangements where the guardian is effectively the state. In several cases, the young person needed a bank account urgently to receive Centrelink payments - without an account, they simply could not access their entitlements.
		  ○ In the mutual bank's experience, these young people frequently lack standard identification documents. They may possess only a birth certificate and no Medicare card, no school ID, and no driver's licence. A parent is either absent, unknown, incarcerated, or the subject of a child protection order. Requiring parental consent in these circumstances is not workable.
		  ○ The customer-owned bank has managed these cases through its AML/CTF Program's special circumstances provisions, accepting referee letters from government caseworkers as alternative identification (consistent with AUSTRAC guidance on assisting customers without standard ID). However, if the regulatory framework were to mandate parental consent for under-15s as a threshold requirement, it may affect our ability to exercise this flexibility for younger children in these circumstances.
		• There would also be potential impacts for existing customers under 15, including the question of whether access to existing accounts and digital banking services would need to be restricted.
		• COBA notes that under Australian law, a child is generally defined as anyone under 18 years of age, and banking industry guidelines explicitly recognise minors as a class of customers inherently vulnerable to specific risks. Introducing a requirement where consent must be "informed" for a specific sub-class of children – namely those under 15 years of age – creates an additional layer of operational and compliance complexity in how banks interact with under-18s generally.

		• COBA believes the OAIC should reflect on this position, and we suggest that the Code needs to address our concerns around financial exclusion for vulnerable youth. We ask that the role of essential banking products be considered carefully when finalising the Code.
2	S16 - Consent must be current	• An annual consent-refresh requirement may be an appropriate requirement for certain products used by children, for example, communication apps and social media. However, we do not think it is appropriate for it to be applied to basic banking products. • We are concerned that implementing an annual consent-refresh mechanism could lead to the forced termination of active banking relationships. This is because, in our members' experience, many customers have minimal to no touchpoints with their bank during the year and due to a lack of engagement from customers there is a high risk that the customer does not act on notices to re-provide consent. • Requiring an annual consent refresh poses significant operation challenges, as institutions standardly provide privacy disclosures at initial collection or during major re-engagement milestones, meaning regular customer touchpoints often occur far less frequently than every 12 months. • We believe that for banks this obligation is onerous both to the institution and to their customers, especially as bank accounts are low risk, relatively simple and well understood products that are essential to interact with the economy. • COBA suggests that the Code be modified to ensure that it does not create barriers or contribute to the financial exclusion of young people. As such we believe that ADIs should be excluded from the requirement to obtain annual consents.
3	S17 – Consent can be withdrawn	• Providing minors with an unconditional right to withdraw consent creates a direct conflict with mandatory legal and regulatory collection requirements under other regulatory frameworks, such as anti-money laundering and counter-terrorism financing (AML/CTF), meaning a withdrawal request would likely force institutions to terminate products or services rather than allow for consent to be withdrawn. • To address this, the framework must allow entities to refuse a withdrawal if ongoing data collection is necessary to deliver the service or meet statutory obligations.
4	S21 - Consent must not be obtained by coercion and S23 - APP privacy policy requirements	• Customer-owned banks are already subject to product Design and Distribution Obligations (DDO) and ASIC regulatory expectations in relation to financial services marketing. • Consequently, banks treat minors as inherently vulnerable and account for ASIC's position that children are more susceptible to persuasive and implicit marketing tactics and have reduced ability to interpret marketing intent. Given this, customer-owned banks existing approach is to ensure marketing to minors is clear, straightforward and not overly persuasive. • In line with OAIC guidance, banks' privacy policy and collection notices are already designed to be understandable at age 14.

5	S32 - Request to destroy personal information about a child	• Existing statutory retention requirements prevent the immediate destruction of customer data, compounding the regulatory conflict. For example, banks are subject to record-keeping obligations under AML/CTF which means that our members are not able to delete personal information on request under existing law. • This creates a clear tension with strict interpretations of the proposed "strictly necessary" and "best interests of the child" requirements and introduces uncertainty regarding how competing regulatory obligations are intended to be reconciled. This highlights the need for the OAIC to prepare essential guidance for industry on the operation of the Code **before** it commences. • In addition, the inclusion of an advanced deletion mechanism exceeds current Privacy Act frameworks and prematurely introduces "right to be forgotten" concepts slated for future tranches of privacy reform, creating an inequitable and fragmented compliance model between minor and adult consumers. • COBA recommends the removal of these concepts from the Code until such time that the primary legislation is amended and there is a consistent "right to be forgotten" for both adults and minors.
6	S39 - Register of privacy impact assessments	• The requirement to publish a Privacy Impact Assessment (PIA) register online may involve the disclosure of commercially sensitive information. Even where limited information is published, this may enable sophisticated actors to infer details about system architecture, identify control gaps, or assess potential vulnerabilities. • The high frequency of internal operational updates would likely generate an overly dense public register, risking unnecessary consumer confusion and anxiety without delivering meaningful transparency. • This requirement does not appropriately balance the policy objective of transparency with the need to protect sensitive operational and security information. • COBA believes that ADIs should be exempt from public disclosure requirements; but supports our members developing a register that is maintained internally for regulatory oversight. Access to this register should be restricted to being made available on request by the OAIC.
7	Impact on banking competition	• Smaller, customer-owned institutions may lack the scale, resources, and technical infrastructure needed to implement and maintain dual privacy and age-assurance systems as would need be required under the existing draft Code. Facing prohibitive compliance costs, many smaller banks may be forced to completely exit the youth market or eliminate online onboarding pathways for minors. • The proposed compliance frameworks risk inadvertently worsening market concentration in Australia's already highly oligopolistic banking sector, where the major banks control over 70% of banking assets. • This concentration is heavily reinforced by consumer behaviour; historical data and industry research consistently show that the vast majority of consumers rarely switch institutions once an account is established. Consequently, whichever bank captures a customer in their youth often retains that relationship. This outcome would structurally entrench the dominance of the major banks.

		• Customer-owned banks serve a diverse range of communities, offering tailored solutions that recognise the unique circumstances of the individuals they serve. The potential of forcing smaller institutions out of the youth market removes the very community-first alternatives that drive true financial inclusion and competitive diversity.
8	Regulatory guidance required before code commencement	• COBA strongly urges the OAIC to provide guidance before the framework takes effect, ensuring institutions have the regulatory certainty needed to comply without disrupting services. • A significant regulatory gap between the implementation date and the eventual publication of guidance creates profound compliance uncertainty for financial institutions. • Smaller providers require comprehensive, definitive guidance to be finalised and released well ahead of the proposed December commencement date to allow adequate lead time for systems engineering and risk framework updates. • Enforcing compliance with highly subjective requirements without concurrent or prior guidance undermines regulatory certainty and exposes well-meaning institutions to unintended non-compliance. • Because customer-owned banks operate on a smaller scale than their listed peers, they rely heavily on third-party vendors to maintain and manage their core systems. As highly regulated financial institutions, these banks face the complex task of aligning their existing compliance frameworks with the new Code requirements. Updating third-party supplier agreements and implementing these technical changes takes considerable time. Consequently, we request an extended implementation period for customer-owned banks beyond the current December 2026 deadline to ensure a smooth, compliant transition.