New Zealand Banking Association
Te Rangapū Pēke

Submission

to the

Office of the Privacy Commissioner – Te Mana Mātāpono Matatapu

on the

Consultation Paper: *Biometric Processing Privacy Code*

14 March 2025

NEW ZEALAND BANKING ASSOCIATION – TE RANGAPŪ PĒKE
PO Box 3043, Wellington 6140, New Zealand
www.nzba.org.nz

About NZBA

1. The New Zealand Banking Association – Te Rangapū Pēke (**NZBA**) is the voice of the banking industry. We work with our member banks on non-competitive issues to tell the industry's story and develop and promote policy outcomes that deliver for New Zealanders.

2. The following eighteen registered banks in New Zealand are members of NZBA:

- ANZ Bank New Zealand Limited
- ASB Bank Limited
- Bank of China (NZ) Limited
- Bank of New Zealand
- China Construction Bank (New Zealand) Limited
- Citibank N.A.
- The Co-operative Bank Limited
- Heartland Bank Limited
- The Hongkong and Shanghai Banking Corporation Limited
- Industrial and Commercial Bank of China (New Zealand) Limited
- JPMorgan Chase Bank N.A.
- KB Kookmin Bank Auckland Branch
- Kiwibank Limited
- MUFG Bank Ltd
- Rabobank New Zealand Limited
- SBS Bank
- TSB Bank Limited
- Westpac New Zealand Limited

Contact details

3. If you would like to discuss any aspect of this submission, please contact:

Antony Buick-Constable
Deputy Chief Executive & General Counsel
antony.buick-constable@nzba.org.nz

Sam Schuyt
Associate Director, Policy & Legal Counsel
sam.schuyt@nzba.org.nz

Introduction

4. NZBA welcomes the opportunity to provide feedback to the Office of the Privacy Commissioner – Te Mana Mātāpono Matatapu (**OPC**) on Consultation Paper: Biometric Processing Privacy Code (**Consultation**). NZBA commends the work that has gone into developing the Consultation, alongside the draft Biometric Processing Privacy Code (**Code**) and Biometric Processing Privacy Code – draft guide (**Guidance**).

5. As fraud and scam attacks become larger and more sophisticated, some organisations are implementing new fraud detection processes (including ones based on biometric information) to manage these risks. Increased pressure is being placed on banks by the Government, regulators, the Banking Ombudsman and consumer bodies, such as Consumer NZ, to take heightened measures to help mitigate the problem. [1]

6. Therefore, the banking industry favours a risk-based approach to biometrics. For example, there are strong use cases (particularly in the fraud and scams area) which biometric processing could assist with. Overregulation in this area may impact the effectiveness of such initiatives.

7. We consider that the Code would benefit from refinement to better enable a risk-based approach to be taken, as set out in more detail in this submission below.

Scope

Who the Code applies to

8. NZBA agrees that the Code should apply to any organisation using biometric processing in relation to individuals. This aligns with the application of the Privacy Act, which applies to all agencies that collect personal information. We agree with the application of Sections 8 and 12 of the Privacy Act.

9. We do consider that organisations that only have corporate clients (for example, banks that only operate in New Zealand on a wholesale basis) should be expressly excluded from the Code.

10. It would be helpful to clarify, in the Guidance, that the Privacy Act (and related guidance such as the OPC's "Working with Sensitive Information"[2]) would apply to the collection and use of biometric information where the Code does not apply.

    10.1. For example, it could be specified that the scenarios included on the right-hand column of the table at page 6 of the Guidance would still be subject to

[1] See: Strengthening bank processes and consumer protections against scams – an open letter to the New Zealand banking industry
[2] See: https://www.privacy.org.nz/publications/guidance-resources/working-with-sensitive-information/

other privacy requirements. We note that page 20 of the Consultation does state that OPC guidance on sensitive information would continue to apply.

11. We also consider paragraph 4(1) of the Code is confusing. It states the code applies to 'the activity of biometric processing; and biometric information as a class of information'.

12. However, the definition of 'biometric information' appears to require that the information is subject to biometric processing. This is circular, and we are not clear as to why paragraph 4(1) has been drafted in this way or why paragraph 4(1)(b) is required – is it intended to clarify that it applies to the collection of biometric information for biometric processing, separate to the actual processing?

When the Code applies

13. As a general note on the proposed timelines for implementation, we refer to paragraphs 37 – 42 of our submission of 22 May 2024 on the exposure draft of the Code (**Previous Submission**)[3].

14. In principle, NZBA does not support any retrospective application of the Code.

15. In the event that the OPC does apply the Code to pre-existing activities, we agree with a longer compliance period, to ensure existing arrangements that use biometrics and associated activities are brought into compliance with the Code.

16. However, we consider that 9 months is too short a timeframe, and that a commencement period of 12 months would be more appropriate. This would also be consistent with other jurisdictions.

    16.1. We expect there will be a significant compliance burden, cost and technical complexity in applying any potential roll-back in the banking sector. Many banks who use biometric information and processing would have relied on third party service providers and taken steps to ensure they have met their existing privacy obligations (including notice requirements).

    16.2. Projects to conform existing processes to new regulation are complicated and will take time to develop and deliver. New processes will need to be created as well as new documentation provided to comply with the Code.

    16.3. We consider it should be possible for an agency to obtain an extension (via an authorised exemption mechanism) without penalty to this 12-month timeframe if they are unable to comply with this transitional period due to making necessary and complex adjustments to processes and systems.

[3] See NZBA's submission on the exposure draft of a biometric processing code of practice (22 May 2024).

17. It is also unclear how this would work in practice given pre-existing arrangements addressing earlier customer fraud and scam losses. We are concerned that it could result in confusion and frustration for a significant number of banking customers.

18. As set out a paragraph 39 of our Previous Submission, we submit that the OPC should consider the following additional transitional arrangements:

    18.1. Grandfather existing arrangements of biometric information.

    18.2. Allow existing uses of biometric information that were collected before the implementation of any new Code to continue under the current Privacy Act regime.

    18.3. Establish a clear cutoff date after which new practices under any new Code will apply to all biometric information processing activities.

    18.4. Consider phased implementation such as introducing the new Code in phases, prioritising high-risk or high-impact uses of biometric information first, providing a timeline for different sectors or use cases to come into compliance with a Code gradually.

What the Code applies to

Biometric information

19. NZBA agrees with the definition of biometric information and appreciate the OPC providing examples of each definition in the Guidance. We also consider the OPC has done well in streamlining the definitions, although note that it is still difficult to fully comprehend some terms without having to refer to several other defined terms. We do consider that:

    19.1. It would be helpful to clarify in the Guidance whether the inclusion of biometric information in AI processes is considered biometric processing. The definition, in its current state, is broad.

    19.2. The Code and Guidance should expressly acknowledge that biometric information used purely for authentication, and not transmitted, is excluded from the definition (for example, where biometric verification to log in to an app only creates a positive / negative authentication from a device, and no data is transmitted or exchanged).

    19.3. Further, the Code and Guidance should explicitly state that it does not apply to images / photos (for example, where ID is taken on file for anti-money laundering purposes).

20. We also agree with the incorporation of the concept of biometric processing such that the Code only applies to biometric information that is subject to biometric processing, given:

    20.1. the heightened risk profile tied to automated processing; and

    20.2. the possibility this could take place without the individual's knowledge.

21. However, we consider it would be useful to clarify in the Guidance that a 'result' is excluded from the definition of 'biometric information'. This is clear from page 22 of the Consultation, but lacks clarity in the definition of biometric information. The biometric definitions also appear to be out of order on pages 3 and 4 ('biometric features' is not in alphabetical order).

22. We note the example provided for 'biometric feature' on page 6 of the Guidance is broader than the concept of a 'biometric feature' under the Code. We understand 'biometric feature' to mean a number or an algorithm that is put in place to represent a particular attribute within the biometric sample, as opposed to how an algorithm recognises the information. This is important as biometric features are commonly employed by third party service providers.

23. The definition of 'result' is very broad, although we consider this acceptable as the term is appropriately used in the Code.

Biometric processing and verification

24. NZBA agrees with the definition of biometric processing. We appreciate the OPC providing further explanation and examples in the Guidance to assist with the interpretation of the term, and calling out that fraud prevention tools fall under the definition of biometric verification.

25. However, we do consider that the definition of 'biometric verification' is contradictory, as it means the '*automated* one-to-one verification' before extending the application to information that is not held in a biometric system. For this reason, NZBA seeks clarity for when OPC would consider a use case is automated, and verification can occur without a biometric system.

26. In our view, the definition also limits the term to comparison of information with information that has previously been provided by the individual. It may also be more beneficial to include a reference to information about the individual that has previously been *collected* by the biometric system, as some information may be collected from individuals indirectly or via continuous collection.

27. We submit the definition of biometric verification should clearly capture this – i.e., "biometric verification means … with biometric information that has previously been captured by a biometric system, or been provided by the individual …".

Biometric categorisation

28. In principle, we agree with the exclusions of readily apparent expression. We also agree with the exception for an analytical process that is integrated in a commercial service. We appreciate the OPC clarifying the latter exclusion covers analytical processes in devices, such as smartwatches.

29. However, paragraph (c) of the carve-out for the definition (i.e. what is meant by a 'readily apparent expression') will be difficult to apply. The extent to which something is a readily apparent expression and could be determined conclusively without biometric processing is too vague to be determinative. For this limb to be satisfied, we question whether it will have to be readily apparent to the agency deploying the technology at the time of collection, or something that would ordinarily be considered readily apparent.

30. We therefore seek clarification on this issue in the Guidance – i.e., whether the exception applies if the expression is unclear to the agency deploying the technology, for example because they cannot see the individual. We also ask that the Guidance provides some examples of what the exception does not cover.

Additional rules

Rule 1: Purpose of collection of biometric information

Alternatives and effectiveness

31. NZBA agrees that organisations should examine the effectiveness of using biometrics. We appreciate the OPC providing examples of the types of evidence which can form part of the assessment of effectiveness.

32. We disagree with the 'available alternative' explanation in the Guidance and its inclusion in rule 1, paragraph (1)(b)(ii) of the Code. In our view, there will always be alternatives with less privacy risk available to solve a problem, and therefore the overriding consideration should be that it is:

> *[N]ecessary for a lawful purpose (in that it achieves the stated aim, whether there are alternatives or not), and that the biometric processing is proportionate to any privacy risks.*

33. The very nature of technological development is that it creates more efficient, effective and reliable ways of doing manual tasks. For example, if an organisation seeks to enable TouchID to log on to a digital banking channel, the organisation would only be able to achieve this if there was no alternative that had less privacy risk. If the current definition of 'alternative' is relied on as explained in the Guidance, this would not be achievable as there are alternatives with less privacy risk (i.e. entering a PIN). The

statement that it is not necessary to deploy biometrics if there is an alternative available that creates less privacy risk is therefore not satisfactory.

34. As noted in our previous submission, the main use case for collecting biometric information in the banking sector is currently fraud and criminal activity prevention and detection. While biometric fraud prevention tools are effective to keep up to date with fraud and scams, there will always be alternative fraud prevention tools that do not involve using biometrics. We submit that OPC should narrow the Guidance to clarify this definition – for example, from:

> *[T]he alternative does not need to achieve the exact same outcome as the biometric processing for it to be a viable alternative,* to
>
> *[T]he alternative <u>needs to provide the same level of benefits</u>.*

35. In our view, organisations should be required to compare like-for-like alternatives that do have the same outcome for the individual – otherwise, it is not a genuine alternative. We consider this is reflected in the working examples provided in the Guidance on Rule 1.

36. We also note page 23 of the Guidance states:

> *Effectiveness is about whether and to what extent the biometric processing achieves your specific lawful purpose, not about whether the biometric system can do what it is designed to do.*

37. Agencies should be encouraged to consider how efficient the technology is, and how accurate the technology is, when determining whether it is effective, as well as how well it can achieve the stated purpose.

38. Neither the Consultation nor Guidance specify how organisations should demonstrate their biometric systems are achieving Government's intended objectives. To address this, NZBA recommends allowing organisations to follow their internal processes to assess the effectiveness of biometric use by completing a privacy impact assessment. Whether this assessment is published should then be in the organisation's discretion.

39. Further, we understand the effectiveness assessment is an ongoing requirement – however, it is not clear how often this assessment should be undertaken. We seek clarity on how frequently the assessments should be completed.

<u>Proportionality</u>

40. NZBA supports the requirement that organisations should consider the proportionality of biometrics against the benefits to them and their customers. We note that this would typically be assessed in the governing privacy impact assessment.

41. However, we disagree that 'no authorisation' is deemed as higher risk (as proposed on page 32 of the Guidance).

42. Authorisation from an individual for the processing of their personal information is not a mandatory requirement under the Privacy Act; it is one of the grounds on which it can be undertaken. In some circumstances, obtaining authorisation may prejudice the purposes of the collection: for example, fraudsters would not authorise collection by a biometrics fraud prevention tool.

    42.1. In the example of fraud protection, requiring authorisation prior to biometric processing could place individuals who do not authorise the collection of their biometric information at greater risk of fraud and financial loss, as well as at a disadvantage. This would apply in particular with certain vulnerable customers who are already more susceptible to fraud, such as the elderly. We ask that OPC provide an acknowledgement that lack of authorisation does not equate to higher risk processing for fraud detection.

43. It would be helpful for OPC to include additional guidance specifically covering proportionality in fraud prevention. It is our view that, where organisations have taken the following steps, the collection and processing is not high risk where authorisation has not been obtained:

    43.1. Provide sufficient transparency to individuals

    43.2. Specify the processing of biometric information is for fraud detection and prevention purposes only

    43.3. Have clear benefits for the individuals, which would directly help to protect them from financial losses

    43.4. Ensure the biometric information is of lower sensitivity and cannot, on its own, identify an individual

    43.5. Ensure the biometric processing will not have bias against individuals.

44. We disagree with the categorisation of "medium risk" where information is transferred overseas – particularly if the new Rule 12 of the Code is complied with, where there are comparable laws or safeguards in place.

45. In respect of cultural impacts (both for Māori and other cultures), we consider organisations should be permitted to undertake their assessments based on their own internal processes, such as completing a PIA, which includes a proportionality assessment. As noted above, it should then be for the organisation to determine whether to publish the assessment.

46. We understand that our members do not collect information on ethnicity via biometric systems, and are therefore unable to distinguish between Māori and non-Māori data generally.

47. NZBA agrees with the three factors organisations must consider when assessing proportionality.

Reasonable Safeguards

48. We support the requirement for agencies to adopt privacy safeguards that are reasonable in the circumstances. We do not consider, however, that those safeguards should be stronger than any of the other safeguards banks have over existing personal information they hold as banks.

49. We support the OPC's decision to move examples of privacy safeguards from the Code to the Guidance and recommend this is retained in the final versions of both. This approach provides organisations with the flexibility to apply appropriate safeguards that are suitable and relevant to their business and technology environment.

    49.1. However, we consider the Guidance goes further than the Code by stating (at page 42) that if a privacy safeguard is 'relevant and reasonably practicable' then it must be implemented.

    49.2. In comparison, Rule 1(d) of the Code requires agencies to implement such privacy safeguards as are 'reasonable in the circumstances'.

    49.3. We submit that the requirements should be consistent with those as set out in Rule 1(d).

    49.4. We also submit that, for authorisation safeguards, whether there is a genuine alternative should not be a consideration. It should further be clarified that this should not be the case where the biometric processing is for the purposes of fraud detection.

    49.5. We consider there should be a carve-out for authorisation safeguards in respect of fraud detection, provided banks take reasonable steps to ensure the collection of biometric information for processing is proportionate, and where privacy risks, benefits and cultural impacts have been assessed. See our submission at paragraphs 42 - 43 above for further detail.

50. Similar to our comments at paragraph 39, we note the guidance refers to conducting an ongoing assessment of whether the privacy safeguards are effective and appropriate, and question what the suggested timeframe for ongoing reviews may be.

51. NZBA supports the proposal to run trials to assess effectiveness. We note the Guidance specifies a maximum trial period of 6 months, with a possible extension of a

further 6 months. We agree that users should be informed if they are participating in a trial.

52. We seek clarity on the governance process for the trial period – for example, are organisations required to obtain the OPC's approval before they can start a trial?

53. In respect of the guidance for Rule 1, we submit:

    53.1. The detailed guidance, risk matrix and example scenarios are helpful (in particular, the example on the fraud detection scenario).

    53.2. We appreciate the flexibility introduced by the Code not stating the privacy safeguards expressly, and providing a non-exhaustive list of examples.

    53.3. We consider whether there are alternatives available with less privacy risk should not be a determinative consideration when assessing whether biometrics is necessary.

    53.4. Lack of authorisation from an individual does not, in our view, always equate to higher risk processing. An acknowledgement should be provided that this should not be the case for fraud detection, where they may be disadvantaged if the information is not collected and processed for their benefit.

    53.5. Fraud detection should hold a heavier weighting for the benefit assessment on page 36 of the Guidance.

Rule 2: Source of biometric information

54. NZBA agrees with stricter requirements for Rule 2 exceptions, given the sensitive nature of biometric information. We appreciate the reference in the Guidance that the 'compliance would prejudice the purposes of collection' exception may apply to fraud investigations.

Rule 3: Collection of information from individual

55. NZBA supports the move towards greater transparency for biometrics, and the recognition that there may be an exception where compliance would prejudice the purpose of the collection.

56. We support the removal of the conspicuous and accessible notice requirements and agree with the new minimum notification rule as this reduces complexity and the compliance burden of Rule 3. Further to our above submission at paragraph 34, we suggest organisations should tell individuals the consequences of not providing their biometric information, instead of available alternatives.

57. However, we consider that notice should be able to form part of an organisation's privacy policy as opposed to a separate notice. We do not think it is practical to expect

individuals to read a privacy policy, general terms and conditions, specific terms and conditions (depending on the product) as well as an additional biometric processing notice – this risks notification overload.

58. We consider that the guidance confirming organisations do not need to advise people repeatedly on the matters outline in Rule 3 will support user experience and help to prevent notification fatigue. We do query, though, whether website content justifies more frequent reminders (as set out on page 81 of the Guidance) and consider that a 12 month timeframe for reminders would be appropriate.

59. We would appreciate confirmation in the Guidance as to whether a reminder can be in the form of a general message to an individual, as opposed to the requirements of notice provided at the time of the collection. Clarification on what would be considered an appropriate timeframe for less obvious collection of biometric information via a website or application would also be helpful. In both respects, we consider that enabling organisations the flexibility to assess what is appropriate in the circumstances would be preferable to strict requirements.

60. In respect of additional matters for notification, we refer to paragraph 62 of our Previous Submission. In addition, it is in our view unnecessary to require notification to customers about their right to complain direct to the OPC in the first instance. We consider a more appropriate approach would be for organisations to attempt to resolve complaints initially. In any event, individuals can rely on s 71 of the Privacy Act to make a complaint to the OPC.

Rule 6: Access to biometric information

61. Clarity on what is meant by the "type" of biometric information an agency holds would be helpful. For example, is 'type' limited to biometric samples, features and templates?

62. If 'type' is limited to these three categories, we support that organisations should provide information to individuals on the broad category, although note it may be complex for customers to differentiate between the types without an understanding of the Code.

63. While we understand Rule 6 is subject to Part 4 of the Privacy Act, we request examples from the OPC (in the Guidance) as to when a refusal to provide access may apply under the Code (in particular s 52 of the Privacy Act).

64. In relation to the working examples on Rule 6 as set out in the Guidance, we consider these are generally helpful.

65. We note that on page 88 of the Guidance, it is stated that if an individual requests access to their biometric information, an organisation must also confirm the type of biometric information it holds about them. However, the wording of Rule 6 states the

individual is entitled to receive 'on request' confirmation from the agency as to whether it holds any biometric information about them, and confirmation of the type of biometric information held. This distinction suggests an organisation would only have to explain the type of biometric information held about an individual if this is specifically requested.

Rule 10: Limits on use of information

Rule 10(1)

66. We agree with the OPC's proposed modification, and consider it is important in the context of increasing use of AI technologies.

Rule 10(5)

67. NZBA agrees that there should be limits around using biometric emotion recognition. This is highly sensitive information. We appreciate the enabling of collection of biometric information to categorise the individual according to their age under Rule 10(5)(c), and also to use biometric to obtain, infer to detect personal information about the individual's state of fatigue, alertness or attention level under Rule 10(6).

68. We also agree with the restriction on creating categories that reflect grounds of discrimination under the Human Rights Act 1993.

69. We submit that the Code should permit biometric processing under 10(5)(b) and (c) if either of the following criteria are met: (i) fraud prevention; or (ii) for a purpose that is beneficial to the individual and not discriminatory in nature.[4]

    69.1. In respect of (i), for example, the presence of an 'accessibility mode' on a device might make it easier to commit device takeover and facilitate fraudulent transactions through malware which can grant extensive control over the device. Technology identifying the presence of an 'accessibility mode' can therefore be very beneficial in enabling banks to identify possible fraud in comparison to other non-biometric forms of technology, especially in situations where a customer may otherwise be vulnerable.

    69.2. In respect of (ii), for example, banks might use biometric processing for a purpose that is beneficial to the individual and not discriminatory in nature in circumstances where we provide an 'accessibility mode' on a device that is designed to assist users with disabilities by providing alternative ways to

[4] *Note that Article 6 of the General Data Protection Regulations enables biometric processing where there is a lawful basis, and the required condition for processing special category data under Article 9(2) is satisfied, which includes where the processing is 'necessary for reasons of substantial public interest', which would include fraud detection. See: How do we process biometric data lawfully? \| ICO; Article 6 of the UK GDPR; and Article 9(2) of the UK GDPR.*

interact with their devices. These services can perform various potentially helpful actions, such as reading text aloud, automating repetitive tasks, and simplifying navigation.

70. It would be helpful for the OPC to provide additional examples in the Guidance on what is meant by 'mental state'.

Rule 10(7)

71. While we support the general exceptions provided under this rule, we propose an additional exception relating to fraud prevention where "the information is necessary to help protect an individual against financial losses caused by potential fraud and scams".

72. We consider this additional exception is necessary to future-proof potential biometrics fraud prevention tools that may collect biometric information as outlined in Rule 10(5), for the purposes of fraud prevention.

Rule 12: Disclosure of biometric information outside New Zealand

73. The proposed Rule 12 is consistent with existing provisions in the Privacy Act. We do note that the new Rule 10(5) provides a more stringent limit of use of biometric information compared to other overseas jurisdictions.

74. This may make it difficult to send biometric information to overseas jurisdictions, as certain New Zealand organisations would be unlikely to rely on other grounds under Rule 12 such as individual authorisation. As a consequence, it is possible that New Zealand organisations may not be able to implement helpful biometric technology, as many of the providers of such technology are based overseas. This could also have an impact on New Zealand-based organisations that form part of global organisations.

75. We submit that OPC clarify the application of this point in the Code and Guidance, noting the difficulties it may create in implementation.