



FINANCIAL SERVICES FEDERATION

25 August 2023

Office of the Privacy Commissioner  
Wellington

By email to: [biometrics@privacy.org.nz](mailto:biometrics@privacy.org.nz)

Dear Madam/ Sir,

**Re: Potential Biometrics Code of Practice**

The Financial Services Federation (“FSF”) is grateful to the Office of the Privacy Commissioner (“OPC”) for the opportunity to respond on behalf of our members to the consultation on the proposed Code of Practice for Biometrics (“the Consultation”).

By way of background, the FSF is the industry body representing the responsible and ethical finance, leasing, and credit-related insurance providers of New Zealand. We have over 90 members and affiliates providing these products to more than 1.7 million New Zealand consumers and businesses. Our affiliate members include internationally recognised legal and consulting partners. A list of our members is attached as Appendix A. Data relating to the extent to which FSF members (excluding Affiliate members) contribute to New Zealand consumers, society, and business is attached as Appendix B.

As you will see from the FSF member list, our members cover a broad variety of institutions many of which are interested in, and apply, biometric information in their processes in the financial services sector. The purpose of this is for both the ease of the consumer and the transfer of information between different agencies in relation to consumers. Our members do not engage in any non-consensual acquisition of biometric information, nor in any automated collection of biometric data. Rather, our members engage in the use of biometrics predominantly for the purpose of electronic identity verification and other verification purposes required for the provision of financial services.

As a result, our members are well regulated by the existing Privacy Act 2020 and other regimes such as the Anti-Money Laundering and Countering Financing of Terrorism Act 2009. They are also required to report regarding their reporting, collection, and storage of customer information to agencies such as the Department of Internal Affairs (from whom we already have guidance on electronic identity verification), the Reserve Bank of New Zealand and, of course, the OPC. Due to the over regulation of the financial services industry, we request that the OPC considers the impacts of additional burdens on the sector.

## Introductory Comments

In principle the FSF agrees with the idea of a code. As we discussed in our 2022 submission to the OPC on the consultation paper on the privacy regulation of biometrics in Aotearoa New Zealand, a code must be proportionate. Whether unintended consequences are foreseeable will come down to the detail and wording of the code (if the OPC decides to proceed with a code). This submission can be found [here](#) and further outlines the FSF's viewpoint in broader terms.

An introductory point we would like to emphasize is around who is covered under the scope of the code. Biometric solutions are offered by third party identity verification vendors where information is collected and maintained by these vendors. The vendor will ordinarily provide a verification report to a financial service provider instead of sharing the actual biometric data. This assists our members in managing their risk and reducing the compliance burden. It is important that the code covers these vendors and fully understands the way they operate as they will be responsible for collecting and processing the biometric data.

Unless expressly indicated below please assume that we agree with the proposals in the consultation questions. The FSF, as an industry body, has no Māori organisations' feedback to answer questions specifically related to the gathering of Māori biometric data so please assume we have no comment on these questions unless stated otherwise.

## Consultation Questions

- 3. How should a code deal with biometric information that is held for both manual and automated processes, or for hybrid manual/automated processes?*

To allow for future innovation it is imperative that the code remains technologically neutral as much as possible. For this reason, the FSF supports the idea of allowing the code to be drafted broadly and narrowing it down as issues come up rather than having to go back and open the code up if it proves to be narrow. In particular we would like to avoid another situation like the Credit Contract and Consumer Finance Act amendments which have had to be reviewed 3 times since their implementation in December 2021.

- 4. If you think a code should apply to a different set of information, which information should it apply to (or not apply to), and why?*

Our membership is particularly concerned about the inclusion of voice in the definition of biometrics and would like to seek clarification as to whether a voice recording would fall into this category. Many organisations hold voice recordings of customer interactions for purposes such as training. If this falls into the category of biometric information, then this will impose huge burdens on the storage, use of and access to these recordings. For that reason, we submit that voice recordings used for specific approved purposes should not be considered biometric information and should be exempt from the terms of the code.

Another concern that our membership has with the definition of biometric information is the inclusion of keystroke patterns. Many cyber security vendors provide technology solutions which can identify if a person is typing information on the website, or if a bot is being used to complete the form. It can also study the key stroke patterns to assess if it is a potential fraudster or a real customer – this analysis covers speed to enter information, use of shortcuts etc. Currently we don't believe these solutions will be able to identify a particular person. Nevertheless, agencies should not be required to obtain express consent to run these security software programs. Especially as it would be impossible to obtain express consent from a bot.

6. *Should a code apply to biometric information about deceased persons? What would be the implications if it did? What are some of the use cases that should be considered? We are particularly interested in hearing from Māori on this issue.*

The only reason we consider biometric information about deceased persons should be protected is for the purposes of fraud prevention however this relates back to the information retention period. In principle we believe the best way to combat this situation is that a deceased person's biometric data should be deleted as soon as the holder is informed the person is deceased.

8. *How might an agency demonstrate that it has assessed the effectiveness and proportionality of its proposed collection and use of biometric information covered by a code?*

The financial services industry has existing legal requirements to ensure that people have been identified correctly as it is necessary for both money laundering prevention purposes and to ensure that fraudulent behaviour is not occurring. Sector wide this should be enough to assure the OPC that verification by way of biometric information is both effective and proportionate.

10. *Should a code provide for proportionality assessments to be undertaken at a sector rather than an agency level in some cases? How might this work?*

As discussed above at question 8, the entire financial services industry has existing legal requirements that they need to adhere to in this sphere. Due to this it could be useful to tie a proportionality assessment into AML/CFT sector assessments.

11. *Should any purposes for the collection of biometric information covered by a code be ruled out altogether, or is the proposed requirement for a proportionality assessment enough?*

We submit that the proportionality assessment should be enough.

12. *Do you agree that agencies should not be allowed to collect biometric information covered by a code for:*
- a. *marketing*
  - b. *classification using prohibited grounds of discrimination*

- c. *inferring emotional state*
- d. *inferring health information.*

We have a couple of comments on the proposed list of biometric information that should and should not be covered by the code.

The first comment is that as mentioned above the code needs to allow for innovation. While presently none of our members use biometrics for marketing purposes its very limiting to rule it out entirely even though we're unaware where this technology could go. However, on the other side of this coin there is a danger that a marketing department could overlook privacy concerns when marketing to individuals so there would need to be a massive education project in this regard for agencies.

Our second comment is that b contradicts later information in the discussion document. Questions particularly around the collection of Māori biometric data leads us to believe that on a certain level Māori data may need to be treated differently to other biometric data. This would be impossible to do if agencies are not allowed to collect data on the prohibited grounds of discrimination such as ethnicity. For clarity our members absolutely do not want the burden of collecting and protecting data on these grounds.

Our final comment is on the potential public good that could come from collecting data on the grounds of c, inferring emotional state. If for example you could tell when someone is distressed and offer them faster service as a result, surely this would overrule potential negative uses. For example, with fraud help lines, if the hold line could tell that someone was particularly distressed (because for example they had potentially been defrauded out of their life savings) and could offer them quick service they could potentially recall the money due to the quick action. It seems premature to rule out this ground of collection at such an early stage because, as mentioned earlier the code needs to ensue that innovation can still continue in the industry.

We have no issue with ground d. that agencies should not be allowed to collect biometric information inferring health information.

*13. What exceptions, if any, should apply to disallowed purposes?*

When looking at prohibiting the use of these kind of technologies there's a real need to maintain flexibility to ensure good customer outcomes. This also comes back to our above points regarding innovation and ensuring the code is not overly restrictive.

*18. Do you agree that there should be an exception to IPP 2 for collection of biometric information for testing or training automated biometric systems? If so, do you agree with OPC's proposed framing of the exception?*

Yes, we do agree with this and the way it's framed.

23. *Do you agree that agencies should let the public know if a Privacy Impact Statement (PIA) has been carried out? Are there any other provisions you think should be included in a code, to encourage agencies to undertake and publish PIAs?*

We don't have any concerns with the idea of letting the public know that a PIA has been carried out, but we do disagree with the idea that PIAs should be publicly available. They often contain discussions which could be considered commercially sensitive. This may have the effect of impacting on competition in the market which is something that needs to be avoided at all costs.

27. *Should the individual be prompted at regular intervals to check whether they still consent to the collection their biometric information?*

Does this refer to ongoing collection or is it in regard to biometric information that is being retained for the relevant period? If it is in regard to ongoing collection, then we see no issue with this however if it refers to information that is being retained then it runs the risk of consent fatigue.

40. *Are there any cultural perspectives, including tikanga Māori perspectives, that should be considered as part of retention and disposal requirements for biometric information covered by a code?*

See above answer to question 12. However, a further comment on the retention period is that we believe it should align with existing requirements such as those contained in the AML/CFT Act or the IRD's record keeping requirements.

45. *How should a code cover use of biometric information for automated processing, where the information was not originally collected for use in automated processing?*

This depends on what the definition of automated processing is.

47. *What specific existing uses of biometric information should a code provide for that are not already covered by exceptions or exemptions in the Privacy Act or proposed new exceptions discussed in this paper? How do you think a code should provide for these uses?*

Our members use biometric verification for fraud prevention purposes as well as identification purposes. We believe that this should be provided for in the code as an approved purpose to collect biometric information. This will also assist with the keystrokes issue we outlined earlier in our submission.

48. *Are any other transitional provisions needed, including any implementation period that might be needed for a code as a whole, or for particular proposals?*

We propose an implementation period of one year.

*52. Overall, do the proposals in this paper strike the right balance between flexibility and technological neutrality, and clarity and certainty for regulated agencies?*

It is clear from the discussion paper that the OPC is attempting to achieve this, and we believe it is a great start but will come down to the actual details of the code.

*54. Are there any ways in which our proposals could have unintended consequences? If so, please let us know what these are and how they could be addressed.*

As above the proof will be in the code.

*56. Are there any biometrics issues you think should be dealt with using other regulatory tools (such as guidance, standards, or legislation), instead of in a code?*

As above need to see what the code ends up looking like.

In summary while the FSF is generally supportive of the idea of a code for biometrics in order to provide agencies with clarity and guidance around the use and storage of this sensitive information we also believe that the code must allow for innovation and flexibility in order to ensure good customer outcomes.

Please do not hesitate to reach out if you wish for us to speak further on any of the points made in this submission.

Yours sincerely,



Katie Rawlinson  
Legal and Policy Manager  
Financial Services Federation

## Appendix A



## FSF Membership List as at July 2023

Non-Bank Deposit Takers, Specialist Housing/Property Lenders, Credit-related Insurance Providers	Vehicle Lenders	Finance Companies/ Diversified Lenders	Finance Companies/ Diversified Lenders, Insurance Premium Funders	Affiliate Members	Affiliate Members contd., and Leasing Providers
XCEDA (B)  Finance Direct Limited ➤ Lending Crowd  Gold Band Finance ➤ Loan Co  Mutual Credit Finance  <u>Credit Unions/Building Societies</u>  First Credit Union  Nelson Building Society  Police and Families Credit Union  <u>Specialist Housing/Property Lenders</u>  Basecorp Finance Limited  First Mortgage Managers Ltd.  Liberty Financial Limited  Pepper NZ Limited  Resimac NZ Limited  <u>Credit-related Insurance Providers</u>  Protecta Insurance  Provident Insurance Corporation Ltd	AA Finance Limited  Auto Finance Direct Limited  BMW Financial Services ➤ Mini ➤ Alpera Financial Services  Community Financial Services  Go Car Finance Ltd  Honda Financial Services  Kubota New Zealand Ltd  Mercedes-Benz Financial  Motor Trade Finance  Nissan Financial Services NZ Ltd ➤ Mitsubishi Motors Financial Services ➤ Skyline Car Finance  Onyx Finance Limited  Scania Finance NZ Limited  Toyota Finance NZ ➤ Mazda Finance  Yamaha Motor Finance	Avanti Finance ➤ Branded Financial  Basalt Group  Blackbird Finance  Caterpillar Financial Services NZ Ltd  Centracorp Finance 2000  Finance Now ➤ The Warehouse Financial Services ➤ SBS Insurance  Future Finance  Geneva Finance  Harmony  Humm Group  Instant Finance ➤ Fair City ➤ My Finance  John Deere Financial  Latitude Financial  Lifestyle Money NZ Ltd  Limelight Group  Mainland Finance Limited  Metro Finance  Nectar NZ Limited	NZ Finance Ltd  Personal Loan Corporation  Pioneer Finance  Prospa NZ Ltd  Smith's City Finance Ltd  Speirs Finance Group(L &F) ➤ Speirs Finance ➤ Speirs Corporate & Leasing ➤ Yoogo Fleet  Turners Automotive Group ➤ Autosure ➤ East Coast Credit ➤ Oxford Finance  UDC Finance Limited  Yes Finance Limited  <u>Insurance Premium Funders</u>  Elantis Premium Funding NZ Ltd  Financial Synergy Limited  Hunter Premium Funding  IQumulate Premium Funding  Rothbury Instalment Services	Buddle Findlay  Chapman Tripp  Credisense Ltd  Credit Sense Pty Ltd  Experian  Experieco Limited  EY  FinTech NZ  Finzsoft  Happy Prime Consultancy Limited  KPMG  Lendscape Ltd  Loansmart Ltd  LexisNexis  Motor Trade Association  One Partner Limited  PWC  Sense Partners  Simpson Western <u>Credit Reporting, Debt Collection Agencies,</u>  Baycorp (NZ)	Centrix  Credit Corp  Debt Managers  Debtworks (NZ) Limited  Equifax  Gravity Credit Management Limited  IDCARE Ltd  Illion  Quadrant Group (NZ) Limited  <u>Leasing Providers</u>  Custom Fleet  Euro Rate Leasing Limited  Fleet Partners NZ Ltd  ORIX New Zealand  SG Fleet   Total 94 members



FINANCIAL SERVICES FEDERATION (FSF)

## THE NON-BANK FINANCE INDUSTRY SECTOR - 2022



# 48%



of personal consumer loans are financed by the **non-bank sector** represented by FSF members.

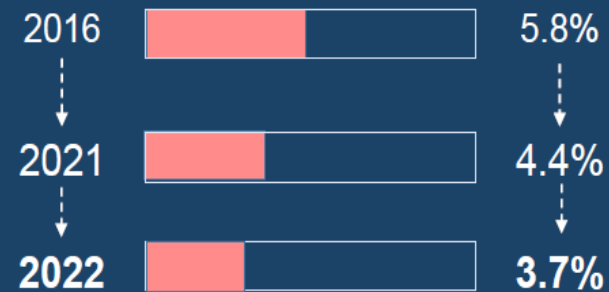
*Setting industry standards for responsible lending, promoting compliance and consumer awareness.*

### Percent of Loan Requests Approved

## 46%



### Percent of Loan Book in Arrears





# KEY FACTS: THE NON-BANK FINANCE INDUSTRY SECTOR

## FSF Members (as at 28 Feb 2022)

Number of Members	57
Number of Employees	3,561
Applications Processed	1,085,739
Loan Requests Approved	495,434
Percent of Loan Book in Arrears	3.7%

## Bank Sector (as at 28 Feb 2022)

Value of Mortgage Loans	\$329B
Value of Consumer Loans	\$7.6B
Value of Business Loans	\$118B

## Non-Bank Sector Share (as at 28 Feb 2022)

% of Total Mortgage Loans	0.4%
% of Total Consumer Loans	47.7%
% of Total Business Loans	5.9%

## Insurance Credit Related (as at 28 Feb 2022)

Number of Employees	237
Number of Policies	311,409
Gross Claims (annual)	\$27.2M
Days to Approved Claim	20 days

## Consumer Loans (as at 28 Feb 2022)

Total Value of Loans	\$8.1B
Number of Customers	1,699,683
Number of Loans	1,584,984
Monthly Instalments:	\$330M

### Average Value of Loan:

Mortgage	\$171,932
Vehicle Loan	\$12,393
Unsecured	\$2,467
Other Security	\$5,754
Lease Finance	\$2,804

### Average Monthly Instalment:

Mortgage	\$257
Vehicle Loan	\$463
Unsecured	\$144
Other Security	\$302
Lease Finance	\$241

## Business Loans (as at 28 Feb 2022)

Total Value of Loans	\$7.3B
Number of Customers	136,830
Number of Loans	264,827
Monthly Instalments:	\$590M

### Average Value of Loan:

Mortgage	\$443,784
Vehicle Loan	\$28,869
Unsecured	\$7,443
Other Security	\$32,374
Lease Finance	\$24,921

### Average Monthly Instalment:

Mortgage	\$2,281
Vehicle Loan	\$1,064
Unsecured	\$799
Other Security	\$11,044
Lease Finance	\$939