FINANCIAL SERVICES FEDERATION

29 January 2021

Dynamic Policy Team
Financial System Policy and Analysis
Reserve Bank of New Zealand
PO Box 2498
Wellington 6140

By email to: cyberresilience@rbnz.govt.nz

Consultation document: Risk management guidance on cyber resilience and views on information gathering and sharing.

The Financial Services Federation ("FSF") is grateful to the Reserve Bank of New Zealand for the opportunity to provide this submission on the consultation document: *Risk management guidance on cyber resilience and views on information gathering and sharing.*

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 sixty members and affiliates providing these products to more than 1.5 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 can be seen from Appendix A, the FSF has three non-bank deposit takers and some registered insurers as members, all of whom are invested in the introduction of this Guidance and the progress made by the Reserve Bank with respect to their expectations of supervised entities in managing their cyber resilience. The FSF commends the Reserve Bank on the work that has gone into developing the Consultation Document and welcomes the identification of a "gap" and the progress made to rectify it.

The FSF is in support of the Guidance proposed and agrees that cyber resilience in the financial system and New Zealand is important, particularly considering the nature of technology which is persistently emerging and ever-changing. The FSF supports the Reserve Bank's intention for the Guidance to be high-level and principles-based, however, the FSF believes that the proposed Guidance does not offer sufficient opportunity for scalability, with insufficient opportunity for the guidelines to be tailored to the nature of each entity.

The FSF will discuss the questions for submitters set out in the Consultation Document in further detail below.

Question 1:
In light of the nature of cyber risk and the range of observed international practices discussed in the previous section, do you support the Reserve Bank's policy stance of being "moderately active" in promoting cyber resilience within the financial sector?

The FSF is largely in support of RBNZ's moderately active stance on cyber resilience. However, the FSF makes reference to the principle of proportionality mentioned on Page 2 of the Guidance document. The FSF agrees that the guidance should be employed in a manner proportionate to the entity, however, is concerned that there is presently not much room for scalability, and thus, a lack of reflection of the Reserve Bank's own principle of proportionality.

A small entity, with a much smaller operation and customer base, is unable to craft cyber resilience to a capacity that a large bank could. In combination with this, the cyber risk a smaller entity possesses is not often to the degree that a large bank would possess. It is then the nature and structure of an entity that is likely to dictate its cyber risk. Therefore, the FSF urges the Reserve Bank to allow more room for scalability in the application of the Guidance based on this rationale.

The FSF also urges the Reserve Bank to consider the resources required for the implementation of the Guidance. The cost of implementation, to its full extent, would be disproportionate to the cyber risk that some small entities possess. Requiring all entities, regardless of size and operation, to apply the same "high-level principles" is unjustified, particularly when considering the variability of resources available to entities, and the disadvantage this would impose on those smaller entities with those fewer resources.

The FSF acknowledges the Reserve Bank's efforts to fill the gap currently present in New Zealand's cyber resilience. The Guidance is an admirable and advantageous policy. However, to ensure that it remains advantageous to all entities, the Reserve Bank must further incorporate scalability into the recommendations, based on the reasons outlined above, in true reflection of the principle of proportionality.

Question 2:
Do you agree with the Reserve Bank's general approach of sticking closely to international practice?

The FSF agrees with RBNZ's approach of sticking closely to international practice. It is encouraging that the Guidance is to be based on international practice as opposed to starting afresh.

Do you have any specific feedback on the draft guidance on cyber resilience?

The FSF queries the Reserve Bank's intent with respect to the status of the Guidance. The Consultation Document and the draft Guidance itself, do not refer to any standing that the

Guidance may have, nor to any consequences that may be brought on as a result of non-compliance. The Reserve Bank has not made it clear whether this is voluntary guidance for entities to comply with, for mutual benefit, or is a set of required "recommendations" for entities to implement.

The FSF believes the term "understand" in A1.2 to be too subjective in its context. Realistically, most boards will only be able to grasp a very rudimentary "understanding", and therefore, the FSF requests that this section be rewritten to provide clarification. More appropriately, the board and senior management should be presented with evidence of an understanding by responsible staff and that practical steps are being made to verify security, with external agencies and testing, such as regular penetration testing and recovery from offline media is happening as per the Guidance.

The FSF would like to direct the Reserve Bank to a typographical error in B2.5, where "life cyber" should be "life cycle".

Question 3:
Do you agree that the guidance should be a set of high-level principle-based recommendations?

The FSF agrees that the guidance should be a set of high-level principles-based recommendations, as opposed to the alternative prescriptive approach. Notwithstanding, the FSF has found the guidance to be more prescriptive than principles-based in some areas. These prescriptions undermine the Guidance's scalability and flexibility, both of which have been emphasised as significant to the appropriate application of the Guidance. Examples of areas of prescription include Part A2.1.1, A2.1.2, and B2.6. There are often instances in these sections where the term "should" can be replaced with "could", softening the prescriptive tone. The FSF would like to see a change in the terminology throughout the Guidance, as a reflection of principles as opposed to prescription.

The FSF also refers to scalability in this context. A completely prescriptive approach would undermine the principle of proportionality. Entities would be unable to apply the Guidance appropriately to reflect the nature of their entity, but rather as required wholly by its prescription. In light of our argument for further scalability, principle-based recommendations are also most appropriate.

Question 4:
What is your view on the principle of proportionality and a risk-based approach adopted by the Guidance?

The FSF is supportive of the Guidance adopting the principle of proportionality and a risk-based approach.

Question 5:
Do you agree that the guidance should apply to all regulated entities of the Reserve Bank?

The FSF agrees with this view, however, has two points to make regarding this question.

Firstly, with reference to the answer provided in Question 1, the Guidance should apply to all entities but with considerable scalability. Entities that do not have such size, structure, and operation, ultimately manifesting into a smaller cyber risk, should not have to comply with the Guidance to the same extent as an entity which may have a large effect on New Zealand's financial security. Guidance that has adopted such scalability may differentiate between the lesser recommendations for smaller entities and higher-level recommendations for those entities who operate on a larger scale.

Secondly, the FSF queries the rationale behind limiting the application of the Guidance to only those regulated by the Reserve Bank. Undoubtedly, some entities outside the Reserve Bank's supervision are large and have the potential to affect New Zealand's financial security immensely. The FSF encourages the Reserve Bank to consider those unregulated entities and co-ordinate with the Financial Markets Authority and the Commerce Commission through the Council of Financial Regulators to appropriately extend the application of the Guidance.

Question 6:
What is your view on the Reserve Bank's collaborative and coordinated approach to information gathering and sharing?

The FSF supports a collaborative and coordinated information gathering and sharing approach. However, the FSF does not support an obligation being imposed on entities to inform an unlimited list of contacts. The logical approach to information sharing would be for entities to notify the Reserve Bank, which then would place the onus on the Reserve Bank to notify other relevant parties and agencies.

The FSF agrees that the entity should definitely continue to share information with its own stakeholders such as their board, trustees, and management. The FSF believes that this is the most appropriate assignment of roles: the Reserve Bank should act as the "gate-keeper" in relation to information, ensuring it is disseminated correctly and mitigating the risk of privacy breaches.

It is from this view that the FSF encourages the Reserve Bank to reconsider the wording in Part C of the Guidance, to ensure this burden is not imposed on all entities, and rather only a recommendation to notify the Reserve Bank.

Question 7:
Do you support the Reserve Bank's intention to broadly follow the international practices and establish a cyber data collection for all prudentially regulated entities?

The FSF agrees with the intention to broadly follow international practices to establish a cyber data collection for all prudentially regulated entities.

Do you have any particular concerns or issues that you would like the Reserve Bank to take into account when further developing its plan?

The FSF would like to ensure that the Reserve Bank does not impose stringent and significant reporting requirements on entities. Establishing cyber data collection may redirect resources and expertise, potentially taking away from the primary strategy of identification and resolution of cyber risks.

The FSF encourages the Reserve Bank to reconsider the wording in some parts of Part D. Firstly, the FSF queries the definition of "interconnection" in D6.1. Whether this refers to a purely technological "connection" or a relationship of any calibre, is not clear. Clarity on this definition would be appreciated. The FSF also refers to D7.1, where it recommends that an entity should establish a termination/exit strategy. The FSF notes that termination is often contractually set out for third parties, and therefore, is uncertain on the intention the Reserve Bank has for the application of this recommendation in such circumstances. Clarity on this recommendation would also be appreciated.

Thank you again for the opportunity to provide FSF's views on the consultation document proposing the risk management guidance on cyber resilience and views on information gathering and sharing.

Please do not hesitate to contact me if you would like to discuss any aspect of the submission or if you require anything further.

Yours sincerely,

Diana Yeritsyan
Legal and Policy Manager

Appendix A

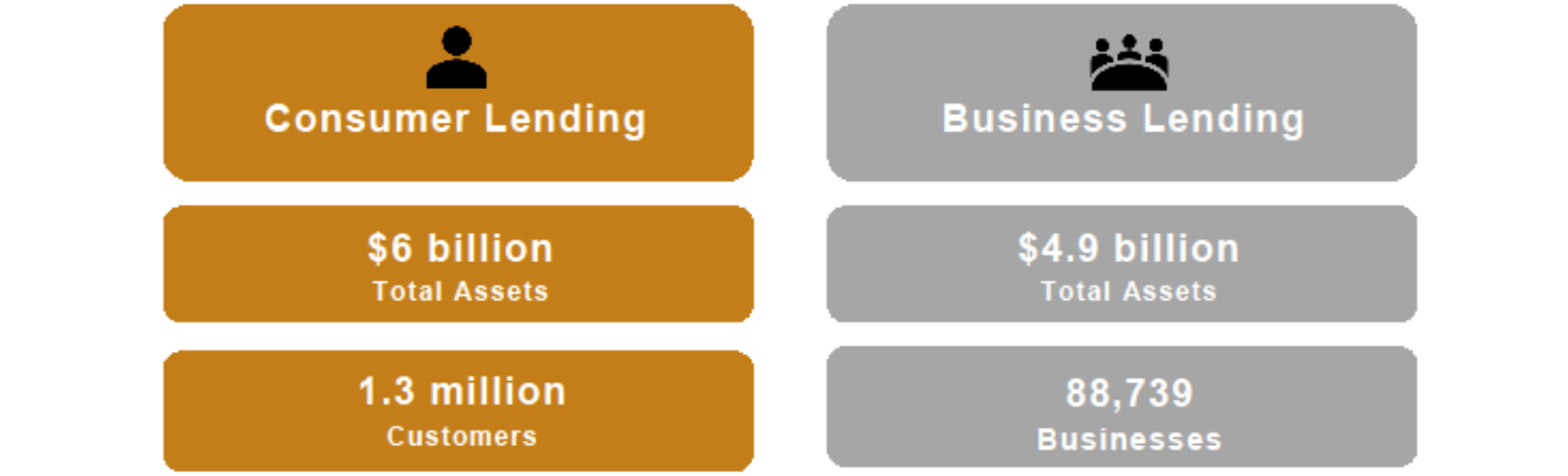
Membership list as at November 2020

Non-Bank Deposit Takers Leasing Providers	Vehicle Lenders	Finance Company Diversified Lenders	Finance Company Diversified Lenders	Credit-related Insurance Providers	Affiliate Members
<u>Rated</u> Asset Finance (B) <u>Non-Rated</u> Mutual Credit Finance Gold Band Finance ➢ Loan Co <u>Leasing Providers</u> Custom Fleet Fleet Partners NZ Ltd Lease Plan ORIX NZ SG Fleet	AA Finance Limited Auto Finance Direct Limited BMW Financial Services ➢ Mini ➢ Alphera Financial Services Community Financial Services European Financial Services Go Car Finance Ltd Honda Financial Services Mercedes-Benz Financial Motor Trade Finance Nissan Financial Services NZ Ltd ➢ Mitsubishi Motors Financial Services ➢ Skyline Car Finance Onyx Finance Limited Toyota Finance NZ Yamaha Motor Finance	Avanti Finance ➢ Branded Financial Caterpillar Financial Services NZ Ltd CentraCorp Finance 2000 Finance Now ➢ The Warehouse Financial Services ➢ Southsure Assurance Flexi Group (NZ) Limited Future Finance Geneva Finance Home Direct Instant Finance ➢ Fair City ➢ My Finance John Deere Financial Latitude Financial Metro Finance Pepper NZ Limited Personal Loan Corporation Pioneer Finance Prospa NZ Ltd South Pacific Loans	Speirs Finance Group ➢ Speirs Finance ➢ Speirs Corporate & Leasing ➢ Yogo Fleet Thorn Group Financial Services Ltd Turners Automotive Group ➢ Autosure UDC Finance Limited <u>Credit Reporting & Debt Collection Agencies</u> Baycorp (NZ) ➢ Credit Corp Centrix Collection House Equifax (prev Veda) Illion (prev Dun & Bradstreet (NZ) Limited Intercoll Quadrant Group (NZ) Limited	Protecta Insurance Provident Insurance Corporation Ltd	255 Finance Limited Buddle Findlay Chapman Tripp Experian EY FinTech NZ Happy Prime Consultancy Limited HPD Software Ltd KPMG LexisNexis PWC Simpson Western Total: 63 members

Appendix B

FINANCIAL SERVICES FEDERATION

The Financial Services Federation (FSF) is the association for responsible finance and leasing companies operating in New Zealand.
This infographic is a snapshot of our 61 members, the membership list can be found at our website: www.fsf.org.nz



FSF lending members data survey period as at 31 July 2019 . Data collected and aggregated by KPMG