10 October 2024

Consumer Policy Team
Ministry of Business, Innovation and Employment
15 Stout Street
PO Box 1473
Wellington 6140

Via consumerdataright@mbie.govt.nz

Tēnā koe Consumer Policy Team,

Securities Industry Association submission: Open banking designation regulations under the Customer and Product Data Bill

The Securities Industry Association (**SIA**) appreciates the opportunity to submit on the "*Open banking designation regulations under the Customer and Product Data Bill*" (**Regulations**) consultation.

About Securities Industry Association

SIA represents the shared interests of sharebroking, wealth management and investment banking firms that are accredited NZX Trading and Advising Market Participants. Our members are a vital part of the capital markets ecosystem. They employ more than 500 accredited NZX Advisers, NZDX Advisers and NZX Derivatives Advisers, and more than 500 Financial Advisers nationwide. Our members work with over 300,000 New Zealand retail investors with total investment assets exceeding $90 billion, including more than $40 billion held in custodial accounts. Members provide financial advice and services to help New Zealanders plan, save and invest for sustainable financial independence. They also work with local and global institutions that invest in New Zealand.

Feedback summary on Open banking designation regulations under the Customer and Product Data Bill

SIA supports policy frameworks that encourage and enable New Zealanders to receive financial advice, products and services tailored to their goals, needs and circumstances. SIA generally supports the intent of the of the Customer and Product Data Bill (**Bill**) framework to enable greater access to and sharing of customer and product data between businesses. We support the intent of the Bill to help customers (i.e. individuals and entities) have greater control over how their customer data is accessed and used. It has the potential to promote innovation, encourage competition, and facilitate secure, standardised, and efficient data services.

In our submission attached, we comment on the following issues:

1. **Status quo and problem definition**
    - SIA supports a sector-by-sector rollout implementation of the framework as it will enable any emerging issues to be addressed before a more comprehensive implementation and provide an opportunity for other sectors to prepare the required systems, processes, education and training, and technology changes.

- While the banking sector will be the inaugural sector to implement the regime, it is recognised that some other parts of the financial services sector will be captured and that reasonable timeframes should be included for those parties to get up to speed and transition concurrently. The potential timeframes for the implementation of these changes need to be realistic. It should be clarified at what point a firm's data-sharing systems are expected to be aligned with banks in these scenarios and the timeframe for this. Businesses outside the scope of the designated banks may not be as 'up to speed' or readily able to update or implement new technology due to cost or resource limitations.

2. The Scope of an open banking designation

- SIA agrees with the proposed list of banks and the implementation timeframe. However, we note the impact on the wider sector, as above.
- We agree that only requests by accredited requestors should be designated.
- SIA supports sharing product data with a customer's permission as this supports a competitive environment.

3. The benefits, costs and risks of an open banking designation

- SIA anticipates that being a regulated and licensed financial advice provider should have some standing in the application to become accredited.
- We support the necessary robust processes and systems proposed, such as record keeping and data storage, to maintain the integrity of data and ensure that data and information are only used for the permitted purposes granted by the consumer and the prescribed approach to complaint processes and dispute resolution should any issues or concerns occur.
- Technical specifications and standards relating to technology, security systems and privacy controls will need to be carefully worked through to ensure they are workable, future-proofed and compatible with standard existing systems.
- Given the potential for data misuse by third parties, vetting and data security standards need to be robust. We support introducing a register for accredited requestors as this would provide transparency on the entities vetted or approved to share, manage, protect, and store data to the required standards. However, we note that the data providers should not be solely responsible for ensuring the safety of the data as the consumer should also accept some level of risk to whom they consent to access; therefore, consumer education is an important part of risk management and data safety.

4. Accreditation criteria – what specific criteria should business need to meet before they can become accredited to make requests on behalf of consumers?

- SIA believes that large entities such as banks will likely be sufficiently resourced to implement the changes required to comply; however, smaller businesses will likely have comparatively fewer resources, and the cost burden of this additional ongoing work and time for getting up to speed for implementation is likely to be significant. Small businesses may have bespoke systems that would require substantial investment to align with new standards – as a result, this may make them less competitive against larger businesses.
- The challenge of balancing security and privacy with the need for innovation and accessibility highlights the issue of setting appropriate barriers to entry for third-party data consumers, particularly for startups. There is a need for those businesses to be accountable and have sufficient capacity and capability to meet standards.

- We support accredited requestors in open banking being required to be a member of a financial services disputes resolution scheme and information security requirements should form part of accreditation. This would enhance confidence in the accredited parties for data providers, requestors and consumers.

5. Fees – what restrictions should there be on fees for providing customer data or initiating payments?

- SIA anticipates that banks will want to charge fees for data access, which will likely depend on the requester type. There is a potential for fees to be a barrier to entry for startups and smaller businesses or for those businesses to be negatively impacted by additional costs arising from fees. There is also the potential for fees to be passed on to customers. Those customers might benefit from the service, and equally, a business might benefit from receiving the customer's data. We appreciate that there needs to be a balanced approach to ensuring that the administrative burden is not solely on the banks. However, we would not want to see fees as a profit-making charge but rather something more fair and reasonable.

6. The detailed rules for open banking

- The Bill requires the data holder to verify the identity of the person who made the request. The regulations should set the manner and standard of verification to a standard consistent with existing verification practices (for example, requiring the customer to log in to the data holder's platform or to verify the identity in the usual way if authorisation is provided over the phone). To facilitate and encourage use by customers, SIA believes this verification should not be overly onerous, but it should be in clear language.
- SIA agrees that a register of accredited persons and requestors is necessary to maintain integrity and transparency across the regime. It will aid in consumer confidence in who has access to their data and the commitment to the standard of how data will be treated. As part of this process, we suggest that licensed financial services are recognised for the high standards they already operate to and that any duplicative administrative burden is recognised and removed.

The standards, regulations and guidance related to all these issues need to be well-considered to ensure they are simple, broadly understood and workable.

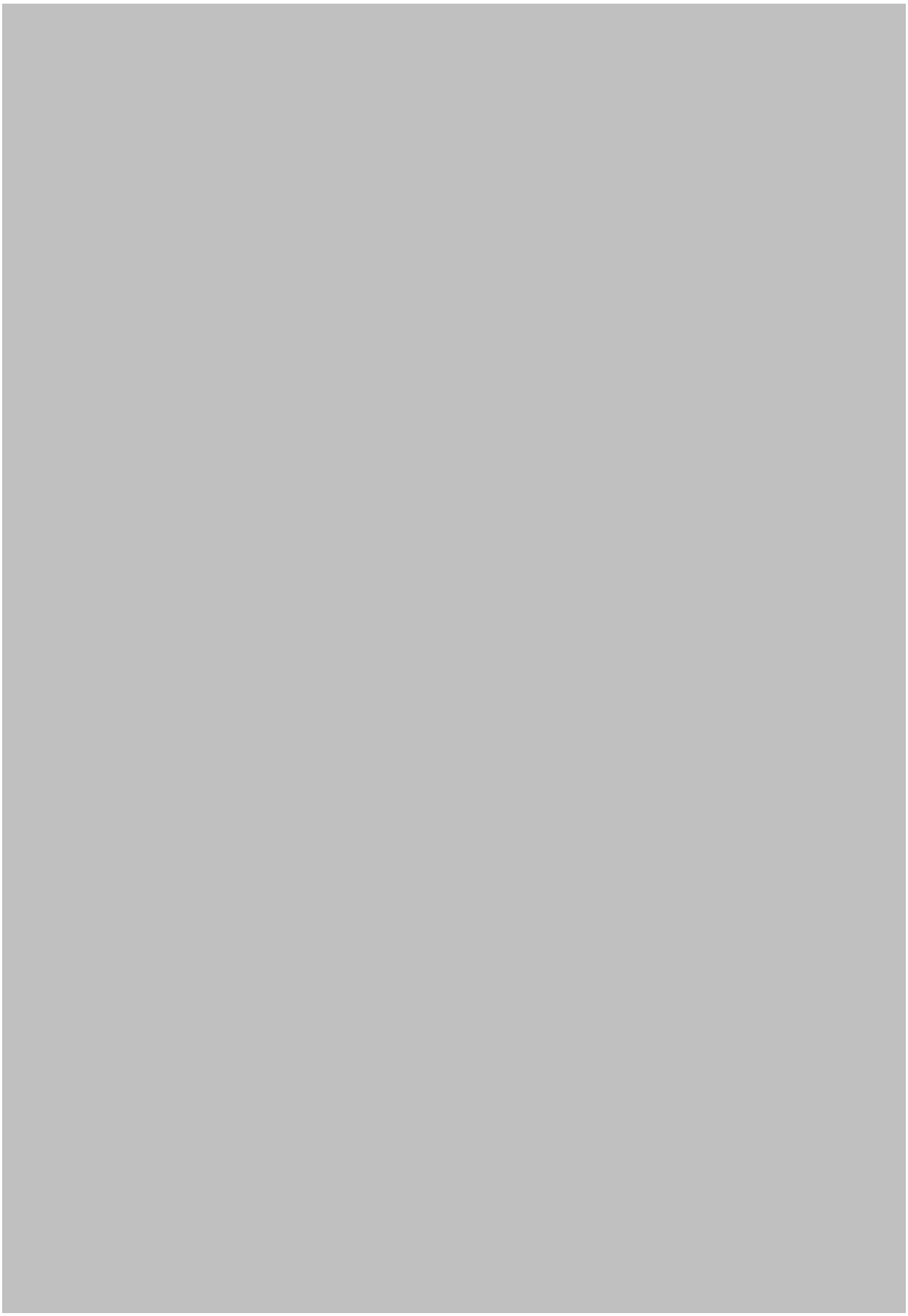
Our submission below (pages 4-17) discusses our industry's concerns and recommendations in more detail. No part of this submission is required to be kept confidential.

Thank you for the opportunity to present our comments on this draft Bill. Please get in touch with us should you have any questions about this submission or require further information.

Nāku noa, nā

Bridget MacDonald
Executive Director
SECURITIES INDUSTRY ASSOCIATION

T: 021 345 973 | E: bridget@securities.org.nz | www.securities.org.nz



Responses to questions

The Consumer Policy team welcomes your feedback on as many sections as you wish to respond to, please note you do not need to answer every question.

Status quo and problem definition	
1.	How do you expect the implementation and use of open banking to evolve in the absence of designation under the Bill? What degree of uptake do you expect?
	1.1 SIA expects that there would be slow development and implementation without the banking sector being designated in the Bill. We also anticipate caution from members of the public in the uptake of open banking should appropriate guardrails not be provided to protect consumer interests and instil confidence.
2.	Do you have any comments on the problem definition? How significant are the risks of suboptimal development and uptake under the status quo?
	2.1 The problem definition recognises that there is an opportunity for consumers to benefit from their personal data through new tools, goods and services, and the Bill opens the pathway for this. 2.2 It further recognises the rightful owners of the data, i.e., consumers, and that consumers should have control over their personal data and that third parties require access to it to innovate and add value to the consumer.
3.	What specific objectives should the government be trying to achieve through a banking designation? What needs to happen to achieve these objectives?
	3.1. Government should provide the mechanisms, standards and guardrails to enable the implementation of the consumer data right framework – recognising the challenges and opportunities experienced in other jurisdictions. Facilitating banking as the foundation sector is logical as this is a significant sector with touchpoints for most New Zealanders and the capacity, capability, and suitable regulatory oversight to undertake its responsibilities to implement the framework in what we expect to be transparent and trustworthy.
4.	Do you have any comments on the criteria that should be used to assess designation options?
	4.1 SIA supports a sector-by-sector rollout implementation of the framework as it will provide an opportunity to identify and remedy issues before more comprehensive implementation and for other sectors to prepare the required systems, processes, education and training, and technology changes. *Bilateral agreements between banks and data requesters/providers* 4.2 In the initial implementation phase, other industries, particularly in the financial services sector, may play a role as data providers. In the natural

	course of business and sharing information, the banking sector may require some financial services stakeholders to align with open banking systems and processes. This is because banking transactions do not always operate in isolation. Entities may become customer data providers to a bank or receivers of information. For example, a customer may permit their bank to request their KiwiSaver balance, or for AMLCFT purposes, a firm may request verification of an address or source of funds from a bank. The firm may be permitted to rely on the due diligence information that the bank has obtained, but the data still needs to be shared with the firm. In either of these scenarios, a bank may require that firm to have new compatible software or systems to share the data, which will also require firms and suppliers of the software to be aligned and accredited. It should be clarified at what point a firm's data-sharing systems are expected to be aligned with banks in these scenarios and the timeframe for this. Businesses outside the scope of the designated banks may not be as 'up to speed' or readily able to update or implement new technology due to cost or resource limitations. 4.3 Equally, data sharing is a two-way system; often, there is a bilateral agreement between banks and other entities. Banks may request information from firms and require them to provide it in a new format and standard. Updating systems, processes, technology, and training will take time and cost. Banks have already had a longer lead time to prepare in some way for the move to open banking. Furthermore, increasing data-sharing will require additional human and technology resources, and businesses need time and cost to arrange this. 4.4 While the banking sector will be the inaugural sector to implement the regime, it is recognised that some other parts of the financial services sector will be captured. Therefore, it is crucial to include reasonable timeframes for those parties to get up to speed and transition concurrently. The potential timeframes for the implementation of these changes need to be realistic to ensure a considered and effective process.
The Scope of an open banking designation	
5.	Do you agree that the banks covered and timeframes should be based on the API Centre Minimum Open Banking Implementation Plan? Do you have any concerns about the specific implementation dates suggested?
	5.1 We agree with the banks proposed and implementation timeframe, however we note the impact on the wider sector, as noted in our response to question 4.
6.	Do you have any views on the costs and benefits of designating a wider range of deposit takers, beyond the five largest banks?
	-

7.	Do you agree that, in the first instance, only requests by accredited requestors be designated? Do you have any comments on when and how direct requests by banking customers could be designated under the Bill?
	7.1 Yes, SIA agrees that only requests by accredited requestors should be designated. It will need to be clear to the customer which companies are registered as accredited requestors, as their expectations may be that a wide range of entities can share data easily, where there may be issues that need to be resolved, such as technology compatibility, before a company is an accredited requestor or that they even elect to become one. The process should be opt-in for all parties outside of the designated banks.
8.	Do you have any comments on the customer data to be designated?
	8.1 We appreciate the scope of what is meant by designated data being outlined and the 7-year duration to which previous transaction information can be requested and provided. This is in accordance with other legislative requirements for the duration that information is retained. *Future-proofing the legislation* 8.2 Technological advances move relatively swiftly, and lifestyle and societal changes also impact what data is important and how data is treated and valued. For example, a shift away from paper-based address-based identification for Know Your Customer (**KYC**) purposes (it is not a good form of evidence for transient or young clients) and biometric data might more effectively confirm that someone is who they say they are. A standards-based approach to client identification, data-sharing, data retention and the possibility of incorporating biometric data supports a more future-proofed approach. *Biometric data* 8.3 While the Privacy Commission has regard for biometric data, there should be a clear reference to whether the biometric data itself is shared or whether it will be that the data is 'authenticated', and then the information shared is that the data is satisfactory and can be relied upon. Biometric data is considered sensitive information and requires sufficient infrastructure and processes within an organisation to protect it. Accordingly, if biometric data was designated data to be shared with a data requestor, the criteria for being a data requestor would need to certify them as meeting the appropriate standards.
9.	Do you have any comments on whether product data should be designated? What product data should be included? When should the product data designation come into force?
	9.1 SIA supports that product data can be shared with a customer's permission. We think this supports a competitive environment.

10.	Do you have any comments on designating payments under the Bill? Should other actions be designated? If so, when?
	--
The benefits, costs and risks of an open banking designation	
11.	Do you agree with our assessment of how the designation will affect the interests of customers (other than in relation to security, privacy and confidentiality of customer data)? Is anything missing? For businesses: What specific applications and benefits are you aware of that are likely to be enabled by the designation? What is the likely scale of these benefits, and over what timeframe will they occur?
	11.1 While there will be benefits to data sharing, maintaining trust and data integrity is essential for all. We anticipate that already operating to high standards, such as being a regulated and licensed financial advice provider, would have significant standing in the application to become accredited.
12.	Do you agree with our assessment of the costs and benefits to banks from designation under the Bill (other than those relating to security, privacy or confidentiality)? Is anything missing? For banks: Would you be able to quantify the potential additional costs to your organisation associated with designation under the Bill? i.e. that would not be borne under the Minimum Open Banking Implementation Plan.
	12.1 We refer to our comments to question 4 about costs.
13.	Do you agree that the designation will promote the implementation of secure, standardised, and efficient regulated data services?
	--
14.	Do you have any comments on the benefits and risks to security, privacy, confidentiality, or other sensitivity of customer data and product data?
	14.1 It is critical that the consumer has control over their data. Consumer trust and confidence in the framework are vital. We support the necessary robust processes and systems proposed, such as record keeping and data storage, to maintain the integrity of data and ensure that data and information are only used for the permitted purposes granted by the consumer and the prescribed approach to complaint processes and dispute resolution should any issues or concerns occur. Much of this should align with the requirements of existing legislation, such as the Financial Services Legislation Amendment Act 2019 (**FSLAA**) or the Financial Markets Conduct Act 2013 (**FMCA**). However, we note that technical specifications and standards relating to technology, security systems and privacy controls will need to be carefully worked through to ensure they are workable, future-proofed and compatible with standard existing systems. *Privacy Act and financial records compatibility*

14.2 This legislation needs to align closely with other relevant legislation, such as the Privacy Act, particularly around what and how data is shared and stored. The SIA agrees with the consideration of the Privacy Act in the Bill, noting that:

(a) under the Privacy Act, IPP 8 sets out that agencies must take steps to ensure that the information they receive is accurate, up to date, complete, relevant and not misleading. The Consumer and Product Data regulations should allow data requestors to presume this standard is met for any information provided by data holders (subject to accuracy standards on the data holders);

(b) a data requestor's use of information received will still be subject to that data requestor's privacy policy. The customer should be made aware of the privacy policy before any data can be shared with the data requestor.

Data security standards must be robust, given the potential for data misuse by third parties. New Zealand needs to learn from privacy issues from other jurisdictions that have been dealing with these issues for a longer time, such as the EU, and make any necessary amendments to the Privacy Act to ensure it offers the appropriate protections, for example, if data is being used for a purpose than it was initially collected for.

Deleting data

14.3 Consumers will and should have the right to withdraw data. However, we note that deleting data is not an insignificant or easy issue to address. In particular, deleting data from aggregate data can be complex, and there may be challenges with eliminating specific data from financial services and artificial intelligence (**AI**) models and algorithms as they are based on aggregate data at a point in time. Deleted data may still need to be kept separately for record-keeping purposes to meet other legislative obligations (for example, AMLCFT, FMCA, FSLAA) should the information be required for investigative or audit purposes. Accordingly, in the event the regulations require an accredited requestor to remove or anonymise the customer's information, this must be subject to the accredited requestor's record-keeping obligations.

Confidence in third-party protections

14.4 We support a register and approval process for accredited requestors, which would provide transparency on the vetted or approved entities to share, manage, protect, and store data to the required standards. We expect businesses will have robust data-sharing agreements with any third party they receive or provide data to as a further way to ensure legislative obligations are met and maintain the confidence of consumers and businesses that it is safe to share data. Businesses have little to no control over a third party, so it would need to be established what is considered appropriate due diligence if anything is beyond that they are an accredited/registered entity, which would indicate they have demonstrated they would meet the stringent standards. Once information is transferred, it would be expected that the information provider will not be responsible for a third party's actions concerning the data.

	14.5 A data provider should not be solely responsible for ensuring the safety of the data as the consumer should also accept some level of risk to whom they consent to have access. There needs to be an element of consumer education regarding understanding a data provider's accreditation and security measures, what the consumer is giving consent for, and how the data will be used and stored/protected. There is a need for clear disclosure from the data holder/provider about what it means if the data is sent to a requestor and how they will be responsible for protecting it. It needs to be clear that the consumer consented to this and understands the consequences. 14.6 We recognise that the data can then be shared with another requestor and so on and used for a multitude of purposes, each consented to by the consumer.
15.	Are there any risks from the designation to intellectual property rights in relation to customer data or product data?
	--
Accreditation criteria – what specific criteria should business need to meet before they can become accredited to make requests on behalf of consumers?	
16.	Do you have any insights into how many businesses would wish to seek accreditation, as opposed to using an accredited intermediary to request banking data? For businesses: How likely are you to seek accreditation? What would make you more or less likely to apply?
	A barrier to entry and a risk to competition if accreditation is onerous or costly for smaller firms 16.1 Large entities such as banks will likely be sufficiently resourced to implement the changes required to comply; however, smaller businesses will likely have comparatively fewer resources, and the cost burden of this additional ongoing work and getting up to speed for implementation will likely be significant. Small businesses may have bespoke systems that would require substantial investment to align with new standards – as a result, this may make them less competitive against larger businesses. Businesses may also have other technology priorities and programmes in progress or other resource constraints that do not allow this work to be undertaken concurrently or for some time. Accordingly, smaller businesses should be given sufficient time to implement changes. 16.2 The challenge of balancing security and privacy with the need for innovation and accessibility highlights the issue of setting appropriate barriers to entry for third-party data consumers, particularly for start-ups. There is a need for those businesses to be accountable and have sufficient capacity and capability to meet standards. However, we note that even larger organisations can have challenges adapting to new regimes, such as new security requirements and flexible approaches for all accredited requestors, including smaller or new businesses, needs to be considered. For example, it would be unreasonable to set the bar accreditation to have $10 million in capital reserves or be operating for ten years, as a start-up company would not overcome that hurdle. However, equally there will need to be credibility and evidence-based

	scrutiny in the accreditation and review process to ensure they meet the standards for privacy and security and remain accountable.
17.	Do you agree that directors and senior managers of accredited requestors should be subject to a fit and proper person test? Do you have any comments on the advantages or disadvantages of this test, or other options?
	17.1 It is appropriate to meet the fit and proper standards as set by other relevant legislation to ensure consumer confidence in the companies accessing the data.
18.	Do you agree that requestors whose directors and senior managers have already met the 'fit and proper' licensing or certification test by the Reserve Bank, Financial Markets Authority or Commerce Commission should be deemed to meet this requirement without further assessment?
	18.1 We would consider this a high benchmark and appropriate in the context of meeting the other accreditation requirements.
19.	Do you consider that, in the absence of insurance or guarantee requirements, there is a significant of banks or customers not being fully compensated for any loss that might reasonably be expected to arise from an accredited requestor breaching its obligations?
	19.1 There is an inherent risk anytime anyone shares or stores information. Intentional or careless breaches should not be tolerated, and the penalties need to be significant to deter or compensate losses. Customers need to have clear information about what a breach is, what they need to do should one occur, and set expectations for how it should be handled and remedied, when and how to make a complaint, and the expectations for that process.
20.	Do you have any comments on the availability and cost of professional indemnity insurance and/or cyber insurance, and how this may impact on the ability of prospective requestors to participate in this regime?
	--
21.	Do you agree that a principles-based approach similar to the Australian CDR rules is an appropriate insurance measure?
	--
22.	Do you agree that accredited requestors in open banking should be required to be a member of a financial services disputes resolution scheme?
	22.1 Yes. It would be logical to ensure complaint processes are duly followed, and there needs to be guidance for customers and requestors clearly explaining the process should the issue not be satisfactorily resolved, including in what

	circumstances to approach the scheme, what an appropriate solution or compensation looks like and how the process will be managed.
23.	Do you consider that information security requirements should form part of accreditation?
	23.1 Yes – this would support confidence in the accredited parties for data providers, requestors and consumers.
24.	Do you have any comments on the level of prescription or specific requirements that should apply to information security? For businesses: What information security standards and certifications are available to firms in New Zealand, and what is the approximate cost of obtaining them?
	Data integrity/accuracy of information 24.1 Clear standards are required to ensure accuracy in the information initially collected, verified and then shared. In a scenario where several businesses all hold different data for the same customer, there would need to be standards for which data is the 'single source of truth' and how companies are obligated to share or remedy this. We expect this will be detailed in the regulations along with expectations and obligations for record keeping and maintaining the data, including deleting data.
25.	Do you agree that additional criteria of accreditation be the applicant demonstrate compliance with its policies around customer data, product data and action initiation and with the Act?
	--
26.	Do you consider any additional accreditation criteria are necessary?
	--
Fees – what restrictions should there be on fees for providing customer data or initiating payments?	
27.	What would be the impact of requests under the Bill being free, for banking?
	27.1 We anticipate that banks will want to charge fees for data access, which will likely depend on the requester type. There is a potential for fees to be a barrier to entry for startups and smaller businesses or for those businesses to be negatively impacted by additional costs arising from fees. There is also the potential for fees to be passed on to customers. Those customers might benefit from the service, and equally, a business might benefit from receiving

	the customer's data. We appreciate that there needs to be a balanced approach to ensuring that the administrative burden is not solely on the banks. However, we would not want to see fees as a profit-making charge but rather something more fair and reasonable, such as in terms of the cost of the transaction/service.
28.	If requests under the Bill were not free, what limits or restrictions should be placed on charging fees? Do you have any comments on the costs and benefits of the various options?
	--
The detailed rules for open banking	
29.	Do you agree with the proposals to ensure that consents given to accredited requestors are sufficiently informed? Are there any other obligations that should apply to ensure that consents are express and informed?
	Verification of authoriser 29.1 Section 44 of the Bill requires the data holder to verify the identity of the person who made the request. The regulations should set the manner and standard of verification to a standard consistent with existing verification practices (for example, requiring the customer to log in to the data holder's platform or to verify the identity in the usual way if authorisation is provided over the phone). To facilitate and encourage use by customers, this verification should not be overly onerous, but the process should be in clear language. *Consumer requests and management process/standards and resourcing* 29.2 Implementing a consumer and product data right will initiate broader and more frequent data-sharing obligations than currently exist for businesses. The data will also need to be shared in a consistent format, requiring technical details, process information and standards. Doing so will require significant resources from businesses in terms of staffing, time, and technology to change their existing data into this format if needed. Dealing with consumer requests and ensuring the appropriate and consistent processes, formats, standards, and systems or access to third-party products are in place will also come at a cost. They also need to have systems to track consents easily.
30.	Should customers be able to opt out of specific uses of their data that are not necessary to provide the service? Do you have any comments on the advantages and disadvantages of this?
	30.1 Consumers should have control over their data and its use, which should be explicit in the consent process.

31.	Should customers have the ability to set an expiry on ongoing consents? Do you have any comments on the advantages and disadvantages of this?
	--
32.	Do you agree with the proposals in this paper to help ensure that consents given to accredited requestors acting as intermediaries are sufficiently informed? Are there any other obligations that should apply to ensure that consents given to intermediaries are express and informed?
	--
33.	Do you agree with the proposals to ensure that payment authorisations given to accredited requestors are sufficiently informed? Are there any other obligations that should apply to ensure that payment consents are express and informed? Should there be any other limitations on merchants or other unaccredited persons collecting authorisations, or instructing payments?
	--
34.	Do you agree with the proposals in this paper for customer dashboards for viewing or withdrawing consent?
	--
Joint customers	
35.	Should there be any exceptions to joint customers being able to access account information, other than those provided by clause 16 of the Bill? What would the practical impact of additional exceptions be on the operation of open banking?
	--
36.	Are regulations needed to deal with joint customers making payments, or are the default provisions of the Bill sufficient? What would the practical impact of the default provisions of the Bill on the operation of open banking?
	--

Secondary users	
37.	Are there any issues with designating authorised signatories on a customer's account as secondary users? What else should regulations provide for secondary users?
	--
Payment limits	
38.	How should payment limits be set?
	--
Remediation of unauthorised payment	
39.	Do you agree that accredited requestors should remediate banks for unauthorised payments that they request? Are there any other steps that should be required to be taken where unauthorised payments occur?
	--
Content of the register and on-boarding of accredited requestors	
40.	What functionality should the register have? Is certain functionality critical on commencement of the designation, or could functionality be added later?
	40.1 SIA agrees that a register of accredited persons and requestors is necessary to maintain integrity and transparency across the regime. It will aid in consumer confidence in who has access to their data and the commitment to the standard of how data will be treated. As part of this process, we suggest that licensed financial service providers are recognised for the high standards they already operate to and that any duplicative administrative burden is recognised and removed.

41.	What additional information needs to be held by the register to support this functionality? Should this information be publicly available, or only available to participants?
	--
42.	Is it necessary for regulations to include express obligations relating to on-boarding of accredited requestors? If so, what should these obligations be?
	42.1 In addition to complying with the relevant Consumer and Product and privacy legislative and regulatory requirements, we would be highly concerned if banks expect accredited requestors to expressly comply with their terms and conditions as this would create another layer of unworkable compliance or overreach. This could be a barrier to entry and costly for businesses and consumers.
Content of policies relating to customer data and action initiation	
43.	Do you agree with the proposed content of accredited requestor customer data policies? Is there anything else that should be required to be included?
	--
Standards for open banking	
44.	Do you agree with the proposed standards? Should any additional standards be prescribed?
	--
45.	When should version 3.0 of the API Centre standards become mandatory?
	--
46.	If product data were included in the designation, what standards should be adopted or developed for product data?
	--

47.	Do you have any comments on performance standards that should apply?
	--
48.	How can MBIE most effectively monitor performance?
	--
49.	Are existing institutional arrangements with the API Centre fit for purpose, to achieve desired outcomes? If not, what changes should be considered? How should the approach change over time as other sectors are designated?
