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?
	Uptake without designation will be low. This has been seen in just about every market around the world who looks at open banking. There are many reasons why, but here are some common ones I have seen working for SISS and other aggregators for the last 20+ years. 1. Banks view the data as proprietary to them and a competitive advantage. They already make money from supplying data using a direct transfer mechanism (delivery of overnight files to companies, which has been done in NZ since 1996 – primarily to BankLink (– now MYOB), and Xero). Keeping an existing revenue stream for a secure solution which costs little to run is to their advantage. 2. Not all data will be made available due to: a. The difficulty in extracting some of it from the source systems. Banks often have many internal systems housing data for Business Accounts, Retail Accounts, Credit Cards etc. The costs of extracting the data and supporting the maintenance of the extractions may be deemed too high. b. Depending on the use cases, Banks may choose to hold data back to encourage people to get the 'right' kind of account to make data available. This is most often seen with personal Credit Cards being used by people running micro businesses. The banks would prefer people have Business Credit Cards for their businesses, where they can charge fees. 3. Screen Scraping is really the alternative to Open Banking, and unless the signup journey is straight forward and the data is as complete as Screen Scraping (even with the issues with Screen Scraping), FinTechs and their customers will not make use of it.
2.	Do you have any comments on the problem definition? How significant are the risks of suboptimal development and uptake under the status quo?
	If the standards are not strictly defined, allowing for interpretation, data quality will suffer and likely will not be as good or perceived to be as good as Screen Scraping. SISS has been aggregating data from Banks in Australia using the direct transfer mechanism mentioned above for 15 years and is a participant in the Australian CDR. There are many inconsistencies in the CDR data that are couched as misinterpretations. This causes authorised requestors to have to build brittle bank by bank patches and workarounds. If the bank corrects the issue, the patches/workarounds must be undone with new code being deployed. If Customers of the FinTechs see the data issues, or data is unavailable, they will log tickets with the FinTechs, who may not have a way of correcting the issue.

3.	What specific objectives should the government be trying to achieve through a banking designation? What needs to happen to achieve these objectives?
	SISS is in the business of supplying aggregated banking data to business solutions which require accurate banking transaction data, typically these are accounting solutions. We would estimate that 85-90% of the usage of Open Banking is for this data. Our recommendation would be to ensure that all data used by businesses is available through CDR. Primarily this would be all transaction and savings accounts, credit cards, loans, and term deposits. Business and personal accounts need to be made available, allowing for both business and consumer use cases to be served. Consideration should be given to choices which make obtaining access to data difficult. • In the UK not all account types are available, and this has been seen as a contributor to a delayed uptake. • In Australia, the focus has been on Consumers, with solutions for Businesses being added after the fact (Trusted Adviser and Business Disclosure). • Also in Australia, additional authorisation requirements (Nominated Representative) required before a consumer can obtain access to CDR data for businesses creates a barrier that means more business users just abandon the attempt and return to simpler solutions (such as Screen Scraping).
4.	Do you have any comments on the criteria that should be used to assess designation options?
	Any bank which provides business products should be in scope for Open Banking, as these will be primary drivers in uptake.
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?
	We agree that the banks covered, and the timeframes should be based on the API Centre Minimum Open Banking Implementation Plan. As the four largest banks are owned by Australian Banks who themselves were the first designated in Australian CDR, they should be reasonably well prepared for delivery of the APIs. There should also be disincentives for not progressing towards the dates?

6.	Do you have any views on the costs and benefits of designating a wider range of deposit takers, beyond the five largest banks?
	In Australia, a lot of the smaller banks utilise core systems delivered by a limited set of providers. Some of these progressed their Open Banking implementations in a timely manner. A company was also setup to provide Open Banking APIs for many of these smaller banks, which helped many meet their compliance goals. Smaller NZ banks may be using similar core systems or may be able to source a plug in open banking implementation. The benefits to more banks being available is that it lowers the objections from businesses and customers on the use of CDR, and it allows for those offering services to obtain a fuller picture of their financial standing. Smaller banks will make use of Open Banking to help customers to move to them. This may be seen as unfair by the designated banks. Consumers may not be presented with the full picture of what is best for them if the data from the smaller banks is not available.
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?
	We agree that, in the first instance, only requests by accredited requestors be designated. One reason for not enabling direct requests initially is that Consumers may be tricked into providing information to sources they would not knowingly send data to. If designated requestors are required, users are sending data to known entities, and there are penalties on those organisations if data is misused.
8.	Do you have any comments on the customer data to be designated?
	The data set suggested will meet the needs of many groups, especially those related to businesses.
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?
	SISS does not make use of product data, so we have a limited view of its usefulness. We did provide a service to make product data available, and we observed that it needs to be clearly defined at the outset as to what is required, and documenting what data is required for each area of the product data needs to be very clear. A lot of time was spent supporting clients in keeping up with changing requirements on what should be in each field or section. If the specifications have not already been developed, then Product Data should be available within 12 months of the consumer data for each bank. If the specification is already clearly defined, then it should be available at the same time.

10.	Do you have any comments on designating payments under the Bill? Should other actions be designated? If so, when?
	For business needs, payments are key. For consumers, it may be frustrating to get to the end of a process suggesting that you would be better off with Bank B and their Product A, and then must interact with banks to move to the correct product.
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?
	Customers benefits will take some time to gather pace, but the inclusion of payments will drive interest from more FinTechs, as several who have dropped out of the Australian market had services which are derived from payments. A primary use case is getting data into systems their advisers use, such as accounting solutions. New Zealand only has a couple of providers with direct relationships with banks enabling this functionality. Enabling Open Banking for businesses may allow them to choose other solutions to meet their needs, especially if their business becomes too complex for one of the existing incumbents. SISS has seen several businesses migrate to Microsoft Business Central, or SAP B1, and, before our product existed, they were disappointed that they could not obtain data as they did in their previous product. Open Banking could allow companies more flexibility over their accounting solutions.
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.
	Yes, SISS agrees with the statement. Our one observation is that if the Open Banking data can be at or better than the quality level of Screen Scraping, and Screen Scraping is banned, the banks may be able to balance a small portion of the costs because there will be less load on the Internet Banking infrastructure.
13.	Do you agree that the designation will promote the implementation of secure, standardised, and efficient regulated data services?
	Yes, SISS agrees with the statement. Negotiating contracts between Banks and FinTechs consumes a lot of time, money and effort for both parties. By removing this requirement, the savings can be reallocated elsewhere.

14.	Do you have any comments on the benefits and risks to security, privacy, confidentiality, or other sensitivity of customer data and product data?
	SISS doesn't believe any of the mentioned risks apply to the Product Data, as this is generally already publicly available on bank websites. The benefits to making it available is that this enables FinTechs to easily enable services to identify if they have the best product. It also enables data holders themselves to compare their products and optimise them to customers needs, which possibly fosters competition in the banking space. Customer data, by its very nature, will contain PII data, and all the mentioned risks apply. Customer data should go to where the customer directs it. The customer must have confidence that the accredited requestor has mechanisms in place to protect their data. Similarly, if the accredited requestor offers the capability to supply the data on to other services that the customer already uses, the customer should be confident that the accredited requestor will only direct the data to where the customer directs it.
15.	Are there any risks from the designation to intellectual property rights in relation to customer data or product data?
	SISS is not aware of any.
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?
	SISS will be seeking accreditation, as we have many customers, both customers of data holders and FinTechs with NZ customers who want to access NZ bank accounts via our services. There will always be a cost to accreditation, which may be beyond many. Being able to use an aggregator to test out ideas, or as a risk mitigation activity allows FinTechs to pay for what they use, rather than pay an upfront cost of accreditation. Over time, they may wish to transition to an accredited designated recipient.
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?
	Yes, SISS agrees with this statement.

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?
	Yes, SISS agrees with this statement. SISS would also suggest that similar Australian bodies be considered for companies which are not NZ Domiciled.
19.	Do you consider that, in the absence of insurance or guarantee requirements, there is a significant risk 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?
	Yes, SISS believes that accredited requestors should carry adequate insurance to cover losses from breaching its obligations.
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?
	SISS believes the insurance is part of the cost of doing business where you utilise a customer's financial data. All FinTechs should have insurance when holding customers PII data, for the purpose of providing users with compensation if something goes wrong. This is not a requirement for Screen Scraping, or if it is, there will be many restrictions to limit payouts.
21.	Do you agree that a principles-based approach similar to the Australian CDR rules is an appropriate insurance measure?
	Yes, SISS agrees with this statement.
22.	Do you agree that accredited requestors in open banking should be required to be a member of a financial services disputes resolution scheme?
	Yes, SISS agrees with this statement.

23.	Do you consider that information security requirements should form part of accreditation?
	Yes, SISS agrees with this statement. To build trust in the system, accredited requestors should be held to a standard.
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?
	SISS believes that the evidence requirements of the Australian ACCC are appropriate. If you have a certain level of certification, no additional audit is required, or a limited additional scope is required. The same security standards available in Australia are available in New Zealand. SISS has no view on the costs of obtaining these security standards and certifications in New Zealand, but based on the Australian experience, the costs to become certified (including insurance) will be 50K+. Much of the initial cost would be driven by the gap between the requirements of a standard and what the FinTech has in place.
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?
	As SISS proposes that there be a level of certification, typically these certifications require demonstration of compliance against their policies. If simpler certification options are chosen to avoid certification costs, they are being a being added back in to demonstrate compliance, which would be an audit.
26.	Do you consider any additional accreditation criteria are necessary?
	SISS does not believe there are any additional accreditation criteria required.

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?
	SISS believes that if requests are free, more prospective requestors are likely to participate, and therefore more customers will access data.
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?
	SISS believes that fees will push people to Screen Scraping, i.e. if the fees are too high the accredited requestor may look to pass the costs onto their customers. SISS supports the Premium API model, i.e. if a data holder wishes to provide additional premium APIs to provide additional data above and beyond the base data prescribed in the specifications, they should be able to charge for this data.
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?
	Yes, SISS agrees with the proposals to ensure that consents given to accredited requestors are sufficiently informed.
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?
	Yes, SISS believes that customers should actively choose what to share. However accredited requestors should be able to flag what is required for the service to operate.

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?
	Data delivered via files has a perpetual consent with no notification, so accredited requestors notifying users of their access every year is an improvement. Users should be in control of their data, if a user wishes to set an expiry, that should be their right. The alternative requires that they remember in some other timeframe that they want to cancel. This could be compared to the dark pattern where companies offer you a free trial for 5 days, but ask for your credit card, and bill you after 5 days if you don't cancel.
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?
	Yes, SISS agrees with the proposals.
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?
	Yes, SISS agrees with the proposals.
34.	Do you agree with the proposals in this paper for customer dashboards for viewing or withdrawing consent?
	Yes. SISS agrees with the proposals.

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?
	Yes, SISS agrees with the proposals. In Australia, for consumers the initial Joint Account Management was opt-in, and this created barriers and frustration. Later this has been made opt-out, which has provided consumers with low friction sharing with little going wrong. An important component of this is that data holders MUST inform users within the sharing journey as to why they cannot share an account. To reduce the frustration, they MUST also provide the details in the same location on how to correct the situation. Ideally the resolution should happen online.
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?
	Yes, SISS agrees with the proposals. SISS assumes that if a payment required multiple authorisations, that the bank would do this within their standard processing. Then submitted payments on the API would just have a status of Secondary Authorisation Pending, and the bank would ask for authorisation using existing mechanisms.

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?
	SISS would recommend using the existing controls available to account holders to control access rather than add a new mechanism which is unfamiliar to the account holders and representatives of the data holders. The "Nominated Representative" system in Australia has added so much friction for users: • users ending up at a blank page with no way out because they have not been setup. • users having to go through manual form based processes requiring them to physically present the form to their account manager, sometimes taking 4 weeks to resolve. • staff within banks telling users that this is not a supported process. Having Secondary Users be configured as they are using any existing read or write permissions simplifies the process and maps to what the account owner has specifically set up.
Payment limits	
38.	How should payment limits be set?
	SISS would expect that whatever permissions currently set would still apply. If a payment over a limit (say 10000) was made, this would require additional authorisation. This authorisation would be obtained through the existing bank mechanisms
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?
	Yes, SISS agrees with the statement that accredited requestors should remediate banks for unauthorised payments they request.

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?
	SISS believes that friction within the system be avoided wherever possible. Any manual process introduces costs and frustration for all parties. If the accredited requestor has been approved by the registration body, their status should be updated on the register, and they should be able to make a call to any data holder and request credentials. This also helps in cases where bank generated credentials fail, and the accredited requestor can just ask for new credentials (or reregister). This has occurred many times in Australia. The register should have all the required information to assist an accredited requestor provide all the information to a data holder to onboard. The register should also provide all the information required for the data holder to verify the accredited requestor. Information on the endpoints should be held on the register – especially if some items are held publicly and some are restricted (i.e. a data holders product info has a public endpoint, but customer data is only on a private endpoint).
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?
	Lists of requestors and data holders and their statuses, which is used to validate either party. Other items needed in the register would be defined by the agreed process for onboarding accredited requestors with the data holders. If a dynamic client registration (similar to that used in the UK or Australia) is adopted, then all the items required to support this would need to exist in the register. SISS believes that register information should only be available to participants. However, lists of participants could be provided via a website which retrieves only the key pieces of information required to show publicly. This is the model used in Australia.

42.	Is it necessary for regulations to include express obligations relating to on-boarding of accredited requestors? If so, what should these obligations be?
	If the process is automated, valid requests from an accredited requestor should be immediate. If the process is manual, then there needs to be a specified time limit for the request to be processed. Valid requests from an accredited requestor should have a reasonable expectation to be issued credentials within 24 hours.
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?
	Yes, SISS agrees with the proposed content.
Standards for open banking	
44.	Do you agree with the proposed standards? Should any additional standards be prescribed?
	Yes, SISS agrees with the proposed Standards
45.	When should version 3.0 of the API Centre standards become mandatory?
	SISS believes it should become mandatory no later than 6 months after a data holders' implementation against the *Minimum Open Banking Implementation Plan*

46.	If product data were included in the designation, what standards should be adopted or developed for product data?
	Coming from the Australian market, SISS would recommend the Australian version as it is more targeted at the customers product information and it has been designed to handle other sectors outside of Banking.
47.	Do you have any comments on performance standards that should apply?
	SISS would suggest that different endpoints may perform differently, so having blanket 2 second timings for customer data requests may place additional hardware requirements to support service load. For example, large numbers (most) of accredited requestors in Australia start at midnight to collect data. While account lists are small, an accredited requestor asking for 2 years of data for every account every night may cause unexpected load on the services. SISS believes the APIs should be free.
48.	How can MBIE most effectively monitor performance?
	SISS firmly believes that if you don't measure what is happening, and the system is underperforming, you won't have any information on where the issues lie. The key piece of information that MBIE should monitor is fall off during the consent process. In Australia this has been a key point, as accredited requestors are unable to understand what is happening on the data holders' side. Often no response is received, or customers cancel, but no detail is provided. MBIE needs to understand when customers fail to consent their accounts. This could be issues with authentication, joint account, or secondary user issues, or even that a particular system isn't supported. In Australia some corporate banking implementations require users to get their internet banking profile connected to view their corporate accounts. API performance and availability is also important to understand any bottlenecks and load on the overall infrastructure. This can be collected manually, again adding cost in the long run as people must assemble the information. Automating it means it is always reported in the same way and in a timely manner.
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?
	SISS believes that the API Centre is fit for purpose. However, we would suggest that the control and governance should be the responsibility of MBIE. As stated, the banks provide most of the funding, and therefore have significant control on what gets implemented. This may be something that can be traded off against charging for the APIs.

General Comments:
SISS Data Services has been involved in the authorised collection of data from the Australian banks for 15+ years. We have contracts with many Australian Banks and receive data files daily from the Banks for processing and delivery to the locations authorised by the customers. We have been an early active participant in the Australian Consumer Data Right. We have provided CDR solutions for consumers and businesses to provide data to their Advisers and their chosen Software Solutions. Our solutions currently provide data for use in Accounting, Superannuation, ERP and other Financial Systems for over 500K Australians or Australian businesses every day.

Thank you

We appreciate you sharing your thoughts with us. Please find all instructions for how to return this form to us on the first page.