24 July 2023

Consumer Data Right Project Team
Commerce, Consumers and Communications
Ministry of Business, Innovation & Employment
PO Box 1473
Wellington 6140
New Zealand

By email: consumerdataright@mbie.govt.nz

Tēnā koe Consumer Data Right Project Team,

Subject: Securities Industry Association submission: Consultation paper – Unlocking value from our customer data

Please find attached the submission prepared by the Securities Industry Association (**SIA**) in response to the Consultation paper – *Unlocking value from our customer data (June 2023).* We thank the Ministry of Business, Innovation & Employment (**MBIE**) for the opportunity to present our comments on the proposals regarding the draft Product and Customer Data Bill.

About SIA
SIA represents the shared interests of sharebroking, wealth management and investment banking firms that are accredited NZX Market Participants. Our members 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 900,000 New Zealand retail investors with total investment assets exceeding $90 billion, including more than $45 billion held in custodial accounts.

Some SIA member firms may submit an individual firm based on issues specific to their business. Those issues and views may not be reflected in this submission. No part of this submission is required to be kept confidential.

Please get in touch should you have any questions about this submission or require further information.

Nāku noa, na

Bridget MacDonald
Executive Director

SECURITIES INDUSTRY ASSOCIATION
Privacy of natural persons W: www.securities.org.nz

Submission on discussion document: *Unlocking value from our customer data*

Your name and organisation

Name	Bridget MacDonald
Organisation (if applicable)	Securities Industry Association (**SIA**)
Contact details	Privacy of natural persons

Responses to discussion document questions

How will the draft law interact with protections under the Privacy Act?	
1	*Does the proposed approach for the interaction between the draft law and the Privacy Act achieve our objective of relying on Privacy Act protections where possible? Have we disapplied the right parts of the Privacy Act?*
	Given the intention is to rely on Privacy Act protections to govern the operation of Consumer Data Rights (**CDR**), SIA believes it would make sense to review and update the Privacy Act alongside the CDR legislation. For example, to expand the Privacy Act to cover a broader subset of data covered by CDR, i.e. information relating to corporate entities.
Consent settings: respecting and protecting customers' authority over their data	
2	*Should there be a maximum duration for customer consent? What conditions should apply?*
	We support customers in having a better understanding and control of the information relating to them. Recognising that customers are likely to have data with multiple businesses and agencies, we believe it would minimise the administrative burden for customers and businesses not to have to renew or authorise consent on an ongoing short-term basis during the relationship with the customer due to a maximum prescribed duration. While a maximum duration could provide healthy tension with customers to keep their data current and accurate, the times frames of the Australian (12 months) and UK (90 days) appear to be very short, which becomes tedious for both the customer and the business. We acknowledge these renewal and opt-in/out processes can be managed through automated systems, however additional staffing resources would still be required to provide customers with the requisite level of assurance. These technology and human resource capabilities come at a significant cost to businesses. This could be a barrier to entry for many firms who do not have existing or the scale of resources to set up, monitor and manage these systems.

	SIA agrees there is a need for "maximum duration" regarding conditions of no negative consent or transferable authority unless in line with existing frameworks like Power of Attorney (**POA**). Having maximum consent periods (of a reasonable timeframe) can be justified by way of data providers implementing mandatory opt-out processes (as prescribed under CDR regulations) for customers during the relevant consent period. We support the customer's ability to access their data, easily withdraw their consent at any time, and have this executed within a reasonable timeframe.
3	*What settings for managing ongoing consent best align with data governance tikanga?*
	SIA submits that controls are needed to promote transparency in how data will be used and ensure the integrity of the data and how it is used. Recognising that this data is a valuable commodity for all parties concerned, it is not unreasonable to align the management of the data with protocols that promote authenticity, security and demonstratable/auditable footprints of any and all changes.
4	*Do you agree with the proposed conditions for authorisation ending? If not, what would you change and why?*
	In some circumstances, it would be reasonable to require additional authorisation for the use of data beyond the relationship in circumstances where the business relationship/service ceases. However, we note that some business relationships are longstanding and ongoing, and other parts of a business may provide services to that customer. For example, it is difficult to define when the relationship ends for a broking customer as a broad range of financial services would need to be considered beyond the initial transaction. In a scenario where an accredited requestor or data provider's accreditation is suspended or cancelled, that would likely be a justifiable condition for authorisation ending. However, prescribing too many conditions for automatically withdrawing consent may become operationally difficult for a data provider to monitor/act on. It may be more practical to rely on consent periods expiring or customers exercising opt-out rights in circumstances where a customer closes or changes their account, as the customer may wish to have control of the consent process themselves.
5	*How well do the proposed requirements in the draft law and regulations align with data governance tikanga relating to control, consent and accountability?*
	SIA believes the approach of the proposed requirements is consistent with what is seen with the developments of the Privacy Act and what is observed offshore with respect to control, consent and accountability.
6	*What are your views on the proposed obligations on data holders and accredited requestors in relation to consent, control, and accountability? Should any of them be changed? Is there anything missing?*
	SIA generally supports the proposed obligations (paragraph 69, page 26) to be addressed in the regulations. We would expect this information to be in the disclosure documents to all customers and can be found, accessed and executed efficiently via relevant platforms, e.g. website, app, phone, email or in writing.

Care during exchange: standards	
7	*Do you think the procedural requirements for making standards are appropriate? What else should be considered?*
	We support standardised data format standards that make it easy for businesses to share and access information and minimise the technology burden for firms to implement successfully. For some data, it will be vital that it is referenced to a legal name and time and date stamped data to reflect a point in time, validity and currency. A couple of considerations are concerned with the authenticity of data when it needs to be correctly applied to a customer and not used in aggregate form—for example, bank account (limit of 20 characters) and account names. Having a longer standardised account name format would be helpful to ensure that data could easily be matched and verified. If JSmith, J Smith, JB Smith, John Smith, John B Smith and John Bartholomew Smith could all be the same person or different people. The integrity of information is essential, so there should be agreed markers to verify information shared with and received by holders and requestors to ensure data is not duplicated. Longer account name formats may help people to use their full legal name. Standards need to be set that are achievable for all forms, whether small or large, recognising that some businesses will not have the technology infrastructure, staffing levels or financial resources of banks. While a 'one-size fits all' approach would be ideal conceptually, in reality, businesses may not have equal capability and resources, so there should be consideration for a tiered, proportionate approach that could be set for basic/mid/advanced standards. We need standards that enable businesses to achieve the highest appropriate level and make it easy to comply without requiring significant overheads.
8	*Do you think the draft law is clear enough about how its storage and security requirements interact with the Privacy Act?*
	SIA supports high standards for data protection, storage and security – this protects customers, businesses and the integrity of the data. The draft legislation is sufficiently clear, and we believe the importance of data security and storage is widely understood; therefore, we think the interaction with the Privacy Act is appropriate.
9	*From the perspective of other data holding sectors: which elements of the Payments NZ API Centre Standards[1] are suitable for use in other sectors, and which could require significant modification?*
	-
10	*What risks or issues should the government be aware of when starting with banking for standard setting? For example, could the high security standards of banking API's create barriers to entry?*
	Bank standard settings are high (as is their resource capability and capacity), which is good for data integrity, but we need to ensure that all businesses can access/provide the

[1] New Zealand API standards to initiate payments and access bank account information. They are based on the UK's Open Banking Implementation Entity standards but tailored for the New Zealand market. Market demand has driven development and led to the creation of bespoke functionality for New Zealand.

	same level of systems, formats and technology. In general, this is a real risk for smaller and a potential barrier to entry. Careful consideration needs to be given to the cost of compliance for smaller businesses. Alternatively, this could be where an 'intermediary' type solution comes into effect, e.g. an NZX Participant Firm meets all the thresholds of holding customer data as a "custodian of data", and a small advisory firm engages the NZX Participant Firm for a notional fee to access customer data. When considering the range of data that can be shared, some elements form the basis of AML/CFT customer due diligence processes, in particular, identity verification. Banks already play a significant role in this. We think that there needs to be a consideration for RealMe as an increasingly important identity verification tool relating to the consumer data right and how data may be utilised in the future, especially streamlining onboarding for customers who often have to undertake the same onboarding activities with each product or service they engage. Further investment into RealMe would reduce an otherwise huge compliance cost burden to businesses from duplicative and inefficient use and sharing of existing data, minimise the burden to customers who want to switch or access products and services, and reduce the barriers to them being 'locked in'. SIA supports investment into RealMe as a centrally reliable 'single source of truth' customer data repository for accredited businesses to access or update as appropriate.
Trust: accreditation of requestors	
11	*Should there be a class of accreditation for intermediaries? If so, what conditions should apply?*
	SIA supports an accreditation programme, as it provides assurance to customers and other businesses they are interacting with, in addition to further due diligence activities. We agree with the proposed classes of accreditation.
12	*Should accredited requestors have to hold insurance? If so, what kind of insurance should an accredited requestor have to hold?*
	SIA does not think this is any different from businesses today holding cyber insurance, which covers data loss. Therefore, it would not be unrealistic to be expected to have the appropriate insurance in place. We would assume that the regulated insurance industry would accordingly and appropriately evolve its cyber offering to accommodate this government requirement.
13	*What accreditation criteria are most important to support the participation of Māori in the regime?*
	-
14	*Do you have any other feedback on accreditation or other requirements on accredited requestors?*
	SIA proposes that there should be recognition of highly-regulated businesses and that financial services entities who are regulated and licenced Financial Advice Providers through the Financial Markets Authority (**FMA**), and our members who are additionally

	regulated NZX Market Participants, should be credited for meeting other related/similar obligations and standards under those regimes as fit and proper persons/entities. We note that many members, for example, who are regulated custodians, already have the necessary data and security frameworks in place, and operating to international standards.
Unlocking value for all	
15	*Please provide feedback on:* • *the potential relationships between the Bill safeguards and tikanga, and Te Tiriti/the Treaty* • *the types of use-cases for customer data or action initiation which are of particular interest to iwi/Māori* • *any specific aspirations for use and handling of customer and product data within iwi/hapū/Māori organisations, Te Whata etc, which could benefit from the draft law.*
	Ref page 21, 34-35
16	*What are specific use cases which should be designed for, or encouraged for, business (including small businesses)?*
	-
17	*What settings in the draft law or regulations should be included to support accessibility and inclusion?*
	-
18	*In what ways could regulated entities and other data-driven product and service providers be supported to be accessible and inclusive?*
	SIA suggests that regulated entities should be grandfathered or at least have a slimmed-down approval process given the frameworks they are required to have in place (as noted in our response to Question 14) that lend themselves to retaining customer data to meet the regulatory environment.
Ethical use of data and action initiation	
19	*What are your views on the proposed options for ethical requirements for accreditation? Do you agree about requirements to get express consent for de-identification of designated customer data?*
	Ethics play a critical role in governance; therefore, SIA supports the ethical steps being considered. Given what is trying to be achieved here with the governance of customer data, we think it makes sense to obtain express consent for de-identification. However, it is difficult to visualise how de-identification data would be used. We welcome further explanation on this.

20	*Are there other ways that ethical use of data and action initiation could be guided or required?*
	-
Preliminary provisions	
21	*What is your feedback on the purpose statement?*
	-
22	*Do you agree with the territorial application? If not, what would you change and why?*
	-
Regulated data services	
23	*Do you think it is appropriate that the draft law does not allow a data holder to decline a valid request?*
	SIA submits that if it is a valid, fair and reasonable request to the data holder and the process provides satisfactory authentication checks and balances, then we would generally support this.
24	*How do automated data services currently address considerations for refusing access to data, such as on grounds in sections 49 and 57(b) of the Privacy Act?*
	-
Protections	
25	*Are the proposed record keeping requirements in the draft law well targeted to enabling monitoring and enforcement? Are there more efficient or effective record keeping requirements to this end?*
	-
26	*What are your views on the potential data policy requirements? Is there anything you would add or remove?*
	-
Regulatory and enforcement matters	
27	*Are there any additional information gathering powers that MBIE will require to investigate and prosecute a breach?*
	-
Administrative matters	
28	*Are the matters listed in clause 60 of the draft law the right balance of issues for the Minister to consider before recommending designation?*
	-

29	*What is your feedback on the proposed approach to meeting Te Tiriti o Waitangi/Treaty of Waitangi obligations in relation to decision-making by Ministers and officials?*
	-
30	*What should the closed register for data holders and accredited requestors contain to be of most use to participants?*
	-
31	*Which additional information in the closed register should be machine-readable?*
	-
32	*Is a yearly reporting date of 31 October for the period ending 30 June suitable? What alternative annual reporting period could be more practical?*
	-
33	*Should there be a requirement for data holders to provide real-time reporting on the performance of their CDR APIs? Why or why not?*
	-
34	*What is your feedback on the proposal to cap customer redress which could be made available under the regulations, in case of breach?*
	-
Complaints and disputes	
35	*In cases where a data holder or requestor is not already required to be member of a dispute resolution scheme, do you agree that disputes between customers and data holders and/or accredited requestors should be dealt with through existing industry dispute resolution schemes, with the Disputes Tribunal as a backstop? Why or why not?*
	Dispute resolution processes need to be well-established to provide further confidence to businesses and consumers. Given SIA's members already have this requirement in place, it would be reasonable to expect every data holder or requestor to be a member of a dispute resolution scheme. The establishment of a Financial Services Ombudsman as in Australia could be implemented here, or the remit and resources of the banking ombudsman could be expanded. Whilst the penalties for breaches are significant, we would expect all accredited parties to take their obligations seriously and that these act as a suitable deterrent to not meeting those obligations.

Other comments

The Securities Industry Association generally supports the proposed approach to improving customer access and control of their data, standardising how data is exchanged, and ensuring those who request access to data are accredited and trustworthy. We also agree that it is necessary for the draft

Customer and Product Data Bill to have rules to guide standardisation and permissions for cusomter and product data.

The cross-border nature of our business environment means that information, products and data will be required to comply with UK, European, Australian and New Zealand regulations. It is important that New Zealand introduces standards that align with global best-practice and reflects on the lessons learned in other jurisdictions. Some organisations in our sector operate in a global business environment. We note that overseas suppliers or services play a role in the financial services sector, and that some customers are domiciled globally.

Next sector to be included

Given the banking sector is the first designated sector for the Bill to be applied, SIA believes once this is embedded, it would be a natural progression to expand to the broader financial services as these businesses interact with banks regularly. Some act as intermediaries and would likely need to align with the banking sector standards as part of the business relationship.

We also believe this will increase innovation, competition and productivity in the financial services sector and more broadly. This will result in better consumer outcomes by giving customers more control over their data, increasing choices for the consumer and the ability to switch easily, and creating an impetus for businesses to work much harder for and add value to their customers.

It is vital to signal early to the next sector/s so they can prepare for the required changes, develop a vision for new product service ideas and opportunities, and prepare for infrastructure and technology or systems changes to meet the required standards. Taking the customer on the journey and gaining their confidence and providing assurance that this can be well managed and to their benefit is also essential.

Compliance costs

Businesses already have systems and processes to protect and manage data, which can have significant and ongoing technology and compliance costs to protect, store and manage customer information and data.

We note that there is value to data, and although there will likely be advantages to both businesses and consumers for moving to the new regime, doing will also come at an additional expense to businesses already investing in technology and compliance systems and processes. This needs to be recognised in terms of any additional costs to businesses. As noted previously, we believe investment into expanding on the capability of RealMe as a centralised repository for a known scope and standard of 'core' customer data would significantly reduce the burden on all businesses and give consumers the confidence that only accredited businesses have access to that data.

SIA appreciates the opportunity to respond to this consultation and welcomes the opportunity to speak to our submission, provide further information or respond to any questions.

Please contact:
Bridget MacDonald, Executive Director, Securities Industry Association
bridget@securities.org.nz | Mob: 021 345 973 | www.securities.org.nz