Gateway Network Governance Body
contactus@gngb.com.au
www.gngb.com.au
28 October 2020

Australian Competition and Consumer Commission
ACCC-CDR@accc.gov.au

RE: GNGB Submission to the ACCC's CDR rules expansion amendments

The Gateway Network Governance Body (GNGB) welcomes the opportunity to make this submission to the *ACCC*. GNGB is an industry-owned governance body responsible for governance of the data infrastructure known as the Superannuation Transaction Network (STN). The STN is made up of Gateway Operators who perform an intermediary role between Superannuation Funds and Employers in the routing switching and packaging of superannuation transactions (contributions and rollovers). More about GNGB can be found following this submission.

GNGB continues to follow the developments of the CDR environment, further to our submission to the Senate Committee on Financial and Regulatory Technology in early 2020.   In the best interests of our members, GNGB monitors the progression of CDR rules within the banking sector, as well as the planning for CDR expansion to Energy and Telecommunications sectors in anticipation of a possible adoption within the Superannuation environment.

GNGB offers this summary response to the ACCC's consultation paper, focussed on Section 3, Increasing the number and type of businesses that can participate in the CDR.

Risk Based approach to accreditation of data recipients

Lowering accreditation requirements, particularly for restricted data access, is likely to encourage participation in the system, which in turn will increase innovation in products utilising data made available via the CDR, notwithstanding consumer demand will drive ultimate participation. However, the approach to accreditation thresholds based on risk assessment of the data types may present challenges due to:

- Risk assessment needs to be maintained in line with changing external environments, i.e. as attack vectors evolve, which may impact relative risk of a particular data set and its role in the ability to impersonate individuals or businesses when combined with other data or intelligence.
- Risk assessment and appetite varies between organisations who may be procuring intermediary or data recipient services and therefore these amendments may not lead to realisation of the full benefit the ACCC is seeking.

Regarding the preliminary risk assessment provided within the consultation paper, GNGB recommends Basic Customer Data to be increased to medium. Based on our own risk assessment, this would be assessed as medium risk based on the ability to be used to derive other data from separate, publicly available sources – e.g. business name/numbers used to derive business address.

GNGB considers that there is a high degree of alignment with the ADR framework being proposed, including table 3.5 of the consultation paper, to the existing information security framework in place across the STN including:

- All Gateway Operators are required to demonstrate compliance with the STN Information Security Requirements (STN ISR). This is made up of 3 separate requirements:
  - ISO27001 compliance,
  - Additional specific control requirements based on the ASD's Information Security Manual (ISM); and
  - An annual independent audit by a suitably qualified information security audit professional to demonstrate ongoing compliance to these requirements, and prior to commencing the provision of Gateway services
- The STN ISR's minimum specified scope includes all data, systems and processes within the Gateway Operator's organisation that are part of its STN gateway operations. This includes all systems and processes that handle or safeguard STN messages and the data they contain, including any relevant activities that may be managed by a third party.
- A key difference to the proposed CDR regime is that accreditation does not change based on risk assessment of the role played within the network, as all gateways are similar in the services they provide, and all carry highly sensitive superannuation data.

GNGB's interpretation of the proposed changes to the CDR rules indicates all Gateway Operators would meet the CDR requirements for participation at a sponsor or unrestricted level and position STN participants, Gateway Operators, as a logical part of the solution for any future Open Super environment. Widespread connectivity to the Superannuation Fund community and employer businesses, as well as the ATO as a data recipient ensure readiness of the STN to play an important role in when the Consumer Data Right becomes available within the Superannuation sector. Subject to the aforementioned challenges in relation to a risk based approach for accreditation of other categories of ADR's, the additional categories of participants would provide flexibility for Gateway Operators to consider during development of product utilising CDR data.

GNGB welcomes further dialogue in relation to ACCC CDR consultation, please do not hesitate to contact us for further information.

Kind Regards

contactus@gngb.com.au

About us

The Gateway Network Governance Body Ltd (GNGB) was established in 2016 as an industry owned, not-for-profit governance organisation whose main purpose is to manage the security and integrity of the Superannuation Transaction Network (STN).

The STN is the data infrastructure that connects employers to the superannuation funds of their employees. It is the digital data messaging network over which superannuation transactions, such as rollovers and contributions, are sent between employers and funds via their technology service providers, who are known as Gateway Operators. The STN is currently connected to all Australian Prudential Regulation Authority (APRA) regulated superannuation funds and will incorporate Self-Managed Superannuation Funds (SMSFs) from March 2021. Since July 2018, over 694,000 employers have transacted over the network with an average of approximately 83 million data transactions per year. There are currently nine Gateway Operators within the STN. Since 2016, GNGB has been successful in the implementation of governance across the STN, specifically:

- Undertaking initiatives to promote the security, **efficiency and effectiveness** of the STN
- **Monitoring compliance** with the Gateway Standards, together with developing and providing oversight of the aforementioned Information Security Requirements (ISR)
- Managing **new entrants and exiting gateway operators** to the network
- **Engaging with key stakeholders** in Government and industry
- Coordinating **change management** activities as legislation and associated instruments change, including the facilitation of member forums and opportunities to test and validate interpretation of legislative change, emerging technology and other developments.

It is important to note that the STN is defined by the boundaries around which Gateway Operators interact with each other, in relation to current governance scope. The STN is a four corner model of data exchange, with the STN Governance framework coverage extending across corners two and three. The below diagram outlines scope of the current regime in the example of contributions messages:
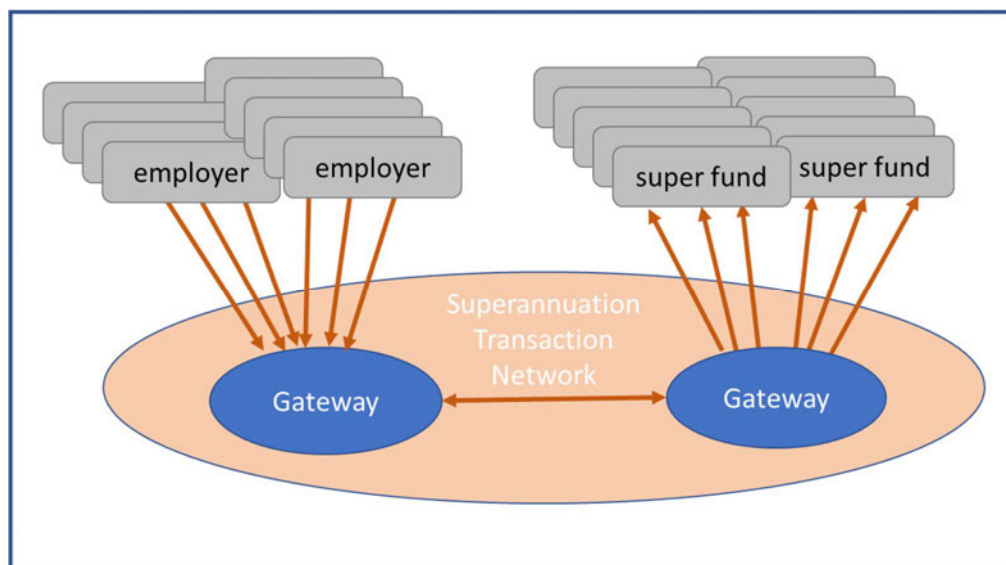
GNGB Stakeholders

The accredited Gateway Operators within the STN range from large bank supported organisations or subsidiaries, to small business operators and fintechs. GNGB is experienced in guiding organisations across the maturity spectrum to identify, develop and implement solutions within a highly regulated environment.

In addition, GNGB's co-sponsor members (i.e. the founders of the organisation) are involved in the design and development of GNGB and are also represented on the GNGB Board. Co-sponsor members include:
- ABSIA – Australian Business Industry Software Association
- ACCI – Australian Chamber of Commerce and Industry
- AIST – Australian Institute of Superannuation Trustees
- ASFA – The Association for Superannuation Funds of Australia
- FSC – Financial Services Council

Current STN Governance Framework

The current governance framework consists of an MoU binding Gateway Operators to each other and to GNGB in respect of their obligations. The MoU outlines compliance with Gateway Standards (framework for interacting) and Information Security Requirements (STN ISR).

STN Governance artefacts framework