Mr Rod Sims
Chair
Australian Competition and Consumer Commission
GPO Box 3131
Canberra ACT 2601

By email: ACCC-CDR@accc.gov.au

Verifier Holdings Pty Ltd

Submission on proposed Consumer Data Right Rules Framework

About Verifier

Verifier is a permission-based private data exchange platform for regulated markets that applies renowned Privacy-by-Design principles, respecting the information security needs of consumers and income data providers. Our clients include banks and non-bank financial institutions.

Lisa Schutz is Verifier's founder and CEO. Lisa was instrumental in founding the RegTech Association in 2017 (a sister organisation to the FinTech Association) and is currently a director of that Association. She was awarded the inaugural *FinTech Leader of the Year* in the Women in Finance Awards of 2017 and *Thought Leader of the Year* in the Women in Finance Awards of 2018.

Purpose of Verifier's submission

Verifier welcomes the opportunity to provide comments on the Consumer Data Right Rules Framework (**Framework**) that has been proposed by the Australian Competition and Consumer Commission (**ACCC**).

We note specifically the goals expressed in the *Final Report* of the Review into Open Banking in Australia, published on 9 February 2018, being the creation of a system that:

- is customer focussed
- promotes competition
- encourages innovation, and
- is efficient and fair.

The purpose of our submission (and therefore the focus of our submission) is to advocate for the implementation of regulation that is efficient and fair and which embodies competitive neutrality.

Verifier's comments and recommendations

1. Screen-scraping

A fundamental shortfall of the *Treasury Laws Amendment (Consumer Data Right) Bill 2018* (**CDR law**) is that it does not address the practice of "screen-scraping".

We do not agree with the view expressed in the *Final Report* of the Review into Open Banking in Australia (published on 9 February 2018) that the practice of screen-scraping could be made redundant simply by "*facilitating a more efficient data transfer mechanism*" (that is, by implementing the open banking reforms).

If screen-scraping is not prohibited, there will be a race to the bottom by those who use the "back door" to avoid the significant regulatory burden (including costs) of accessing and sharing CDR data in the transparent and informed consent driven model contemplated by the CDR law and the Framework. A consequence of this would be to create a data access and sharing environment that lacks both competitive neutrality and appropriate protections for CDR data.

Our strong view is that the ACCC should follow the lead of the European Commission's revised Payment Services Directive (PSD2), which (from mid 2019) prohibits accessing data through the use of screen-scraping techniques.[1] France, the UK, Germany, Luxembourg and Poland have finalised implementation of PSD2 and a number of other EU member states are working towards implementation.[2]

Apart from the widely recognised transparency flaws and security risks associated with screen-scraping, failing to prohibit the practice will confer an unfair competitive advantage on those who provide and implement screen scraping.

Competitive neutrality:

There is a compelling public policy basis for our recommendation that screen scraping be prohibited. That is, in order to facilitate market efficiency, regulation should not create a competitive bias in favour of particular products or providers within a given market segment.

One of the principles of "good" regulation is that it should not impose competitive disadvantages – it should embody competitive neutrality.

[1] European Commission – Fact Sheet. *Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling customers to benefit from safer and more innovative electronic payments* MEMO/17/4961, Brussels 27 November 2017

[2] http://www.hoganlovellspayments.com/PSD2#

Verifier's recommendation:

We strongly recommend that when the power to make rules under the CDR law vests in ACCC, the ACCC should make a rule[3] that prohibits the use of screen-scraping to obtain CDR data.

2. Deletion of CDR data

We support the ACCC's proposal to make rules to the effect that CDR data should only be kept by an accredited data recipient for as long as is necessary to provide the uses consented to by the consumer ("deletion rule").

However, under the reciprocity arrangements an accredited data recipient may, as a recipient of CDR data, also fall with the definition of "data holder" of that CDR data (under section 56AG of the CDR law). As a result, our view is that it will be necessary for the rules to clarify that in this case, the deletion rule will continue to apply to the data recipient in its capacity as a data holder.

3. Quality of CDR data

We note that the ACCC does not propose to make any rules in relation to privacy safeguard 10 (quality of CDR data) in the first version of the rules.

We strongly disagree with this approach.

The integrity and efficiency of the data-sharing environment will be compromised and undermined if poor quality CDR data is introduced into the system – and it will suffer the GIGO syndrome (garbage in, garbage out). Moreover, if screen-scraping is not prohibited, then the reality is CDR will be offering lower quality data with higher controls. The current fintechs who use screen-scraping will have no incentive to switch.

Verifier's recommendation:

We recommend that the first version of the rules require CDR data to meet data quality standards (and that those data quality standards are developed as a priority by the Data Standards Body). At a minimum, this require that the data

[3] Under section 56BA and section 56BB(a)(b) of the CDR law (the latter section addresses, amongst other things, disclosure and security of CDR data)

flowing within the CDR is at least as good as that available to the consumer on their banking portals.

4. Consent

Dashboard access and management

The ACCC proposes to makes rules that will require all accredited data recipients to have a system in place which allows consumers to readily manage their consents. We make the following comments about these "consent dashboards":

- the rules should provide for read and write API access to consents so that consumers can aggregate multiple dashboards into a single dashboard (to simply management of multiple consents)
- the rules should permit a change to, or deletion of, consents by an intermediary acting on behalf of the consumer
- the rules should encompass an obligation on the data recipient to include in their consents details of any downstream data sharing they did on behalf of the consumer. In other words, there needs to be a way for the consumer to see all consequent sharing in the chain of data and be able to control that use
- the rules should address the consequences of revocation of consents. Depending on the situation, there will be circumstances where consumers will want different outcomes:
    - "I don't trust you anymore" scenarios – where the consumer would want to be totally "forgotten"
    - "I don't want you to have my data but I still want to keep dealing with you from my old data" – in which case revocation is just ceasing the ongoing data feeds
    - "I am terminating the arrangement" – in which case – the data recipient needs to keep the data it needs operationally but delete anything surplus to that. In this situation the criteria around acceptable levels of de-identification need to be established (noting that with the type of data available in the open banking system – de-identification is a flawed concept, and it is not really possible)

Details of consents

In addition, from a technical perspective it is imperative that the ACCC make rules that specify the details that must be included in a consent, since these details will need to be incorporated into the technical standards.

Designation of consents

While it is not a matter within the ACCC's remit under the CDR law, we note that in our submission to the Treasury with respect to the revised exposure draft of the CDR law, we have recommended that consent data associated with CDR data should also be designated by legislative instrument as CDR data.

5. Authorisation

We wish to draw attention to the criticality of authorisation in achieving the goals of the CDR law regime. Without easy access (safely) users will simply not exercise their data rights – for an interesting perspective from the UK see the article available here: http://www.techuk.org/insights/reports/item/13974-open-banking-view-from-the-fintechs

Similarly, consumers who do not have online access, or in sectors where this is less common, need to be catered for. Otherwise, the CDR law regime will not meet its goal of facilitating economy wide data sharing.

Currently the ACCC is proposing strong customer authorisation (as under the PSD2 and the accompanying Regulatory Technical Standards). The authentication of the person and their authorisation are combined, in a sense, in their proof of their ability to complete a strong OAuth process.

However, reflecting the PSD2 model with the focus on OAuth options is problematic for two reasons:

- PSD2 is focused on securing payments, which obviously has a higher standard of security required,
- the CDR law regime is an economy wide data sharing solution, and while risks must be mitigated, more nuanced approaches to getting the authentication (making sure the person is the person) and authorisation (getting their permission) are possible.

In our view, the ACCC should support new, emergent authorisation models. However, since Australia is leading the world in focusing on economy wide date sharing, the ecosystem must build for a plurality of baseline authorisation models from day 1 – or risk never achieving the target end state. The ACCC should give

further consideration to authentication and authorisation requirements, and while for a start OAuth might be the standard, there should be an expectation set that for limited accesses and higher trust parties, different models might be used.

Verifier's recommendation:

We recommend that the ACCC specify a range of options and a set of requirements for them as follows:

- Oauth (for 1 July)
- Paper based (as an alternative process for 1 July)
- Identity driven authentication + contractual permission driven authorisation – for high trust data recipients

We further recommend that the rules include a process that provides for consideration of new, emergent authentication + authorisation methodologies. If they satisfy ASIC requirements, they might be implemented (instead of the baseline models) for smaller (opt-in) cohorts of data recipients and data holders.

Finally, we would be happy to discuss any aspect of our submission with you or your staff. Please contact me in the first instance.

Sincerely
Lisa Schutz, CEO
Verifier Holdings Pty Ltd