October 24, 2022

Submission by Adatree Pty Ltd regarding amendments to the *Competition and Consumer Act 2010*

Executive summary:

Adatree is pleased to provide commentary on the Government's proposed amendments to the *Competition and Consumer Act 2010* to expand the Consumer Data Right to enable Action Initiation, as per the recommendations of the *Inquiry into Future Directions for the CDR* (*CDR Inquiry*). This represents a fantastic step forward for consumer empowerment, and we are eager to provide our views on how this can best be enabled. Through Action Initiation, CDR will cement itself as a cornerstone for Australia's digital economy at large.

We acknowledge and appreciate the clear amount of work which has gone into designing these amendments. We agree with the overarching approach whereby the existing CDR legislative framework and technical infrastructure will be leveraged wherever possible. We strongly disagree with the Government's apparent interpretation of what constitutes 'CDR data', as well as the proposed extension of the Privacy Safeguards to the CDR instruction layer. These measures will significantly increase the system's complexity and inappropriately extend the remit of the CDR's bespoke privacy protections well beyond their intended scope to a point where they do not provide benefits to consumers while inhibiting uptake of the Action Initiation framework.

Key points raised in our submission are:

- **Consistent obligations need to be applied to all data shared in the instruction layer**. These obligations should not rely on the Privacy Safeguards or the definition of 'CDR data'. Instead, they should continue to rely on the requirements set through the CDR Rules and standards.
- **CDR data sharing already features both an action and an instruction layer;** the regulated disclosure of CDR data from a Data Holder to an Accredited Person is itself an action made available to those with read access. The Privacy Safeguards regulate how data shared through this action is made available by Data Holders and used by Accredited Data Recipients. They do not and should not apply to the instruction layer.
- The interpretation in the explanatory materials that 'CDR data' includes information collected by an Accredited Person directly from a consumer

P: 02 8005 1826
W: adatree.com.au
A: Suite 1408, 3 Spring St, Sydney

inappropriately increases the scope of the CDR's regulatory remit and has not been communicated to or tested with industry. Again, the Privacy Safeguards' primary purpose is to regulate consumer data that is disclosed under a CDR read access instruction. They should not be used to further increase the general regulatory obligations on Accredited Persons who hold consumer information collected outside the CDR.

- The **definition of 'CDR data' needs to be amended** to be made both clearer and more strictly bounded. The current definition is overly broad, poorly understood and generally not fit for purpose, especially as it inhibits many use cases from being implemented to the detriment of consumers. The definition needs to be amended to allow 'CDR data' to lose this tag in certain instances - including when it is integrated into an Action Initiation instruction or disclosed under a certain consent.
- We agree that information shared in the instruction layer should be subject to protections, though we think this is best enabled through the **existing security requirements imposed on these instruction layer messages, as well as through additional specific data standards** to prevent excessive or unnecessary information being shared. If there are concerns about data collected by Action Service Providers (ASPs) or Accredited Action Initiators (AAIs) being used inappropriately, then this should be addressed at its core through consistent and stricter general privacy regulations through the *Privacy Act 1988*.
- We caution **against allowing ASPs to charge for access to CDR Action Initiation** APIs. We note that services that mirror aspects of Action Initiation are being made available in some instances. It is necessary to effectively isolate what aspect of such a service should be considered when determining whether a fee should be permitted to be charged. We also note that UK open banking is free to use.
- CDR Action Initiation needs to accommodate sending instructions to ASPs who do not have an existing relationship with a consumer. This will be vital for ensuring that the CDR will be able to assist consumers switch products. Consideration should also be given to how CDR can interact with other emerging initiatives, such as a digital identity framework, to further streamline switching processes. Adatree encourages the acceptance of Recommendation 3.4 (identity verification assessments) in the *Review into Open Banking*, as this will further promote consumer benefits.
- It is vital that CDR Action Initiation allows for the ongoing sending of Action Initiation instructions under a **single consent and authorisation**. Though we appreciate that it is alluded to in the supporting material, this functionality will be fundamental to the system's success.

About Adatree

Adatree has been a pioneer in the Consumer Data Right (CDR) since June 2019 with its turnkey Software as a Service platform for Data Recipients. Adatree's platform removes technical complexities so companies can focus on leveraging data instead. Our platform enables companies across all industries to receive real-time consented banking data via API.

Adatree's award-winning platform simplifies the hardest part of the CDR – the technical connection and security standards – by providing connectivity to the CDR ecosystem through one API.

As a company, we have significant expertise operating within the CDR ecosystem and first-hand experience navigating its challenges. As first-movers in the CDR market, we understand the real-world challenges faced by startups and smaller companies who would rather participate in the CDR than rely on unregulated and unethical forms of data-sharing, like screen scraping.

Detailed Comments

Privacy Safeguards and the definition of 'CDR data'

Application of the proposed Action Initiation flow
We understand that at the heart of the Government's proposed model is the separation of the instruction layer - where the information necessary to authorise and request an action is transferred between action participants - from the action layer - where the ASP executes the action just like if it was received through any other channel.

We understand that the instruction layer operates as follows:

1. A consumer consents to an AAI sending instructions to an ASP on their behalf.
2. The AAI engages with the ASP to establish an authorisation in line with key requirements of the consent.
3. The ASP confirms with the consumer that they authorise specific actions to be taken, including key parameters.
4. The AAI then sends discrete write access requests to the ASP in relation to a specific consent requesting that a certain action be undertaken. This request will contain specific information necessary to progress the request - such as updating personal information, relevant details to make a payment, etc.
5. If the action request aligns with the authorisation, then the action is progressed by the ASP in line with its existing procedural requirements.
6. The ASP provides the AAI with confirmation as to whether the action has been undertaken (either 'the action was undertaken', or 'the action was not undertaken' and potentially a reason why). The AAI makes a record of this and may be required to update their consumer dashboard.

If a consumer wants to update their address details for example, then they would consent to the AAI sending requests under a specific 'update details' action, and their new address would be provided to the ASP in step 4. Upon receiving this information, the ASP will progress the specific action requested in the same way it would a request received through any other channel. It will then communicate the status of the action to the AAI in step 6.

CDR data sharing already features both an instruction layer and an action layer

The explanatory material seems to indicate that CDR data sharing currently operates exclusively within the instruction layer - including the disclosure of CDR consumer data. We disagree with this assertion. The instruction layer should only relate to the communication between the ADR and the DH to set up a consent and authorisation and to instigate a data sharing (or read access) request. The actual sharing of consumer CDR data is then a distinct action that is introduced and regulated by the CDR legislative framework.

1. A consumer consents to an Accredited Person requesting specific data sets from a Data Holder
2. The Accredited Person engages with the Data Holder to establish an authorisation in line with key requirements of the consent (duration and data clusters).
3. The Data Holder confirms with the consumer that they authorise their data to be shared (specifying the data clusters and duration) and allows the consumer to select the relevant accounts.
4. The Accredited Person can then send discrete requests to the Data Holder in relation to a specific consent requiring that data be shared (in this case through a token that represents authorisation to collect data endpoints relating to the token).
5. A Data Holder then progresses this action - however in this case, the process is prescribed by the CDR legislation. As the CDR is mandating how an action must be performed, the disclosure of CDR data to the Accredited Person falls within the action layer. Many of the CDR's existing protections - like the Privacy Safeguards - relate exclusively to the regulation of the action layer and not the instruction layer. This separation of regulatory obligations is appropriate and should be maintained.
6. The Data Holder then provides the Accredited Person with confirmation (yes or no) as to whether the action has been undertaken.

It is our view that the distinction between these two layers is fundamental for Action Initiation to be successful. If there is not a recognition of this boundary, then there will be future difficulties faced when attempts are made to declare new action types, and CDR action participants will face significant challenges in understanding how they are required to treat data received and disclosed through the system.

Requesting a Quote

Example 8 of the Privacy Impact Assessment suggests that CDR Action Initiation could be used to request a quote. While we think that this is a beneficial use case that should be enabled, there are some issues around how this is presented. Specifically, the example seems to suggest that the ASP would create the quote and then disclose these details to the AAI directly within the instruction layer. This imposes obligations on the ASP to perform the action in a specific way, as it would normally not disclose the details of a quote directly with a third party - it is mandating new processes be undertaken in the action layer. This is against the underlying principle that Action Initiation should only mandate that an action must be undertaken, not how it must be performed. While we think this could be enabled through a combined CDR request (an Action Initiation request to create a quote and a Data Sharing request to disclose the outcome), this could not be enabled in the instruction layer alone. This would also require that quote outcomes be included as either mandatory or voluntary CDR data.

The reason why we see this distinction as important is because the Privacy Safeguards currently only apply in respect to CDR data - primarily being data shared in the action layer as there is currently no CDR data being shared in the instruction layer. The limitation of the Privacy Safeguards from being applied to the instruction layer is appropriate and should continue going forward.

The Privacy Safeguards should not apply to data shared through the instruction layer

As noted above, the instruction layer denotes the technical information that is required to be shared in order for an authorisation to be created and for an action to be successfully progressed. It should not be regulated by the Privacy Safeguards which were established to govern the increased access and usage of consumer data enabled through the new 'data sharing action' introduced under CDR.

> *The current Privacy Safeguards are crafted to provide protections to data being collected and used in the context of CDR data sharing. This limits the ease with which they can readily be adapted to provide equivalent or tailored protections for action initiation and, in particular, the instructions that an ADR sends to a data holder to initiate an action. Currently, the ACCC's general rulemaking power is more suited to crafting protections for other kinds of data collected or created through the use of the CDR regime.* - CDR Inquiry, p.177

While these safeguards may be appropriate for CDR data sharing, attempting to impose these protections on the instruction layer itself will unnecessarily increase complexity for those seeking to participate in the system.

We understand that the details shared in the instruction layer to create an Action Initiation authorisation or to initiate an action may include consumer information that is not currently required for a data sharing instruction - e.g. personal information to be updated, specific payment parameters, etc. We also understand that this information may include some details that have been collected through the CDR or otherwise designated as CDR data. Despite this, it is not appropriate to expand the Privacy Safeguards to the instruction layer itself as this is overlaying a strict privacy framework onto a purely technical process.

This is not to say that protections shouldn't be applied in relation to the CDR Action Initiation instruction layer - for instance, that you should need consumer consent to send Action Initiation instructions - merely that it is not functional to attempt to reuse the Privacy Safeguards to provide appropriate protections.

We agree that the Privacy Safeguard should also not apply to the action layer, other than in the CDR data sharing case.

Data collected by an Accredited Action Initiator directly from a consumer is not CDR data and must not be subject to the Privacy Safeguards

The Privacy Impact Assessment seems to imply that the Privacy Safeguards will apply to consumer data held by an Accredited Person even where this data was collected directly from the consumer. The basis for this interpretation is unclear, and this does not align with existing industry understanding or practices.

> 5.2.13 Importantly, it is understood that the Privacy Safeguards would be activated once CDR data is collected by an AAI. That is, any CDR data that an AAI collects from a consumer to carry out an instruction or any CDR data that is received by an AAI from a DH (ASP). This approach would ensure consistency with the treatment of data that moves through the data flows as discussed above.

The implications of this apparent decision are significant and risk destabilising the current practices of many operating within the CDR. For example, does this mean that consumer transaction data currently collected by an Accredited Person through screen scraping is also subject to the Privacy Safeguards? Does this mean that those Accredited Persons who use both screen scraping and the CDR to collect consumer data have Data Holder obligations in respect of any data

collected under screen scraping through reciprocity? If not, why not? It is very unclear on what basis the recommendation was made, as it decreases the viability of operating in a compliant manner within the CDR ecosystem and having a clear CDR data boundary. This brings more questions and complexity than benefits to consumers

The current definition and concept of 'CDR data' is poorly understood and insufficient information has been provided by Government agencies to assist industry in understanding where their CDR obligations begin and end. The proposed amendments to the legislation do not alter the definition of CDR data, so it is unclear how this apparent new interpretation in relation to instructions has been determined. Without a clearer delineation of when information is or is not 'CDR data' (and therefore subject to the heightened CDR obligations and bound within the CDR data boundary of the ADR or other CDR participant) it is not possible to operate effectively within the CDR system; participants will either operate without confidence that they are acting within the legislation or simply avoid the system entirely.

While we do think it is appropriate for stricter general protections to be put in place regarding how businesses are able to collect and use consumer data (including under screen scraping and other processes for harvesting personal information), we think that this is better addressed at an economy-wide level. We note that all Accredited Persons are already required to be bound by the APP in respect of any non-CDR personal data they hold, and that there is currently a review being undertaken as to the *Privacy Act 1988*'s ongoing appropriateness.

The proposed model will treat data shared in a CDR Action Initiation instruction inconsistently

Even if it is the case that data collected outside the CDR is deemed to be CDR data (due to it being deemed equivalent to data specified in a designated instrument), extending the Privacy Safeguards to also cover the instruction layer will result in CDR action participants needing to conform to dual privacy systems when engaging with a single instruction. For instance, date of birth is certainly not CDR data, but will likely need to be included in Action Initiation instructions - like when applying for a new product. This will mean that, under the current proposal, the Privacy Safeguards would not apply to this data but would apply to other data included in the same instruction. This inconsistency will result in the CDR becoming even more confusing for participants. This risk is noted in the CDR Inquiry and Privacy Impact Assessment, but no adequate solutions are included in the legislation to sufficiently address this complexity.

> *It is highly desirable for privacy and information security requirements to apply consistently to [action initiation instructions]. It will be important to address the issue that, to the extent that some action initiation instructions include data obtained or derived under CDR data sharing, different protections will apply potentially creating complexity for ADRs in managing their privacy and information security obligations.* - CDR Inquiry, p.178

A single set of consistent obligations should apply to the instruction layer
All information shared in the instruction layer should be subject to consistent protections. The instruction layer will contain discrete information required to initiate actions via an API. This will include limited and necessary factual information about the consumer which the consumer could themselves confirm and understand - similar to the data able to be disclosed as a CDR insight. The protections provided to this information should not be the same as those afforded to the extensive data sets able to be accessed and used through CDR data sharing.

Ensuring consistent consumer protections in relation to the instruction layer would be better accomplished by designing Action Initiation API standards to only include the minimum information needed to initiate a specific action and by continuing to require that any information transferred in the instruction layer is encrypted. This is the clearest way to ensure that consumer information is protected when being used to initiate actions.

Additionally, overarching obligations should be imposed on the information disclosed in this layer that do not need to rely on the extension of the Privacy Safeguards. For instance, the Data Minimisation Principle in the Rules could be extended to require that ASPs retain only the minimum information required to initiate an action received through a CDR Action Initiation instruction - regardless of whether this information is CDR data. Similarly aligned with the intentions of the Data Minimisation Principle, the Rules should also restrict Accredited Persons to only being able to request a consumer's consent to initiate an action where that action is relevant to the provision of a service, as set out in Recommendation 4.13 of the *CDR Inquiry*.

While CDR instructions will start to include more consumer data, the protections provided need to be considered in the context of existing data sharing practices. Sharing details around my name, address and date of birth through a secure API channel in a regulated ecosystem will be more secure than commonly used

alternatives, such as sharing photocopies of identity documents or relying on screen scraping.

If the Government is concerned that CDR action participants will use data provided in the instruction layer outside the context for which the consumer has provided it, then this indicates a broader issue around inappropriate data use. This will not be fixed by extending the Privacy Safeguards and should instead be addressed at a whole of economy level through either stricter regulation of service providers or a more robust general privacy framework. The CDR cannot and should not be a tool to address general deficiencies in how service providers handle data or systemic issues with Australia's overarching privacy framework. Attempting to do so will only serve to undermine the viability of the system.

'CDR data' needs to be redefined to have clear boundaries and limitations
As mentioned above, the other major issue contributing to the complexity in the proposed legislation is the overly broad and poorly defined concept of 'CDR data'. The current definition is not fit for purpose and should be amended to address both the issues facing Action Initiation and the more general issues being faced by current industry participants seeking to use the CDR.

The concept of 'CDR data' is fundamentally problematic as there are no boundaries around when data is to be treated as CDR data - if something is CDR data then it is CDR data forever and if it is not CDR data then it may still become CDR data in future. As the Privacy Safeguards hinge upon this definition, this means that a higher than appropriate degree of protection is frequently applied to data which is not sensitive, meaninglessly denying consumers autonomy over their information. This is paternalistic and inappropriate.

Currently, the only 'off ramps' for CDR data are when it is disclosed to a trusted adviser, when it qualifies as a CDR insight, or (soon) when it relates to a business consumer. These models need to be extended to further acknowledge the regulations of other entities (e.g. AFSL and ACL holders, ADIs, APRA-regulated general insurers) as well as to better facilitate data sharing with informed consumer consent.

Providing 'off ramps' that allow CDR data to be shared with those outside the system is not enough though, and the CDR Rules need to provide a process for data to lose the 'CDR data' tag where it is recognised that the heightened protections of the CDR are no longer appropriate. Clear instances include where the data constitutes a CDR insight, where it is disclosed to a Trusted Adviser,

where it has been received alongside a business consumer statement, and now where it is included in a CDR action instruction. All of these examples recognise that there are circumstances where the current level of protections provided by the Privacy Safeguards are inappropriate. However, due to the definition of CDR data in the overarching CDR legislation, the protections cannot be rolled back - so instead the Rules merely allow the data to be shared with those who are not governed by the act and who do not need to abide by these higher standards. This is inefficient and a clear double standard.

This results in ADRs, who would themselves be guaranteed to hold consumer data in line with the Australian Privacy Principles at minimum, being unable to offer consumers services that benefit from the increased flexibility associated with these disclosure models (e.g. CDR insights). We do not agree with this outcome. If it is determined that a lower level of protection is sufficient and appropriate for certain kinds of CDR data or CDR consumers, then all participants should be able to equally benefit from the increased flexibility associated with this. This is not an attempt to shirk appropriate CDR protections, but it is an appeal to ensure that both accredited and non-accredited participants are able to equally benefit from these different access models.

In the context of Action Initiation, the definition of CDR data will also make it very difficult to understand how an AAI and ASP would be able to interact with consumer data they have collected in relation to the system in a consistent way. As such, we recommend that any CDR data disclosed in an Action Initiation instruction lose the CDR data tag for the purposes of initiating the instruction, and instead be subject to consistent protections that are more appropriate for the information disclosed.

Importantly, any consumer data disclosed by a Data Holder under a CDR data sharing request would remain subject to the CDR protections.

General comments

Role of intermediaries

Adatree asks that the ability for intermediaries to effectively operate under the CDR Action Initiation framework be carefully considered at this early stage. Intermediaries perform a crucial role in increasing accessibility to the CDR system, and they must be able to engage with Action Initiation.

As Action Initiation is implemented, AAI participants must be able to send action initiation requests via third party OSPs who connect to the end ASPs. This is similar to the role currently played by collecting OSPs in facilitating CDR data sharing, which we note ran into difficulty due to how the legislation was drafted. Unlike with data sharing however, we consider it appropriate to limit Action Initiation OSPs to those who are Accredited Persons. This will be appropriate given the importance of restricting the ability to initiate actions to those who have been vetted by the CDR's accreditor.

Intermediaries, such as Adatree, must be able to be the poles and wires of Action Initiation. The Rules, Standards and CX Guidelines must also allow the consent process to focus on the end service provider and not simply the intermediary AAI. For example, if Adatree provides Action Initiation services for a comparison site, the authorisation consent must show the comparison site as requesting an action, not Adatree. The intermediary is not, by nature, consumer facing, and should not be present in the consent flow outside of the 'supporting parties' section, CDR Policy or equivalent. This should also be the case for intermediaries facilitating CDR data sharing.

Access Models

The legislation and supporting documents only mention how ADRs and AAIs will be able to engage with Action Initiation. However, it is also necessary to consider and be explicit as to how other access models, specifically Trusted Advisers, Affiliates and CDR Representatives, may or may not be able to interact with Action Initiation in future. These participants have already been integrated into CDR data sharing and would benefit from being able to initiate actions in some capacity. It is Adatree's opinion that the legislation must at a minimum leave the system open to allowing these participants to play a role, with more specific requirements to be determined through Rules. However, given the onus lies largely on an Accredited Person to ensure that those they bring into the system are appropriate, all AAIs seeking to partner with non-Accredited Persons should be required to have in place appropriate processes to mitigate risks to consumers,

codified in a third-party management framework. This should apply to CDR data sharing processes as well.

Reusing CDR infrastructure
We strongly support the Government's commitment to reusing as much of the CDR technical infrastructure as possible. This also extends to leveraging the existing consumer consent dashboard. We see significant capacity for existing government investment to be leveraged when delivering Action Initiation, and consider this as a sensible decision for promoting uptake across industry and increasing the speed with which Action Initiation can be implemented.

Action declaration approach
While we can see the appeal of declaring specific actions - rather than sectors - we consider that this may result in significant levels of complexity when different information is required for the same action to be initiated across different sectors. Based on the understanding that action instructions will be sent via API, it may be the case that distinct standards are required for the same action across multiple sectors (like opening an account). If not, an ASP risks receiving insufficient or excessive data to what is required. This may result in limited benefits of adopting an action based designation approach compared to continuing to use the existing sectoral approach. Additionally, this approach may mean that each time a new sector is added, all of the relevant existing action declarations will need to be amended.

Priority of action declaration
We recommend that the account application and management related actions be prioritised over payments related actions. This is because payments have existing certifications and processes in place, while the capability to manage the end-to-end account lifecycle is ripe for innovation and often the biggest barrier for consumers switching to more suitable and/or competitive products and services. This prioritsation would be in line with the principles of the CDR framework.

Payments related actions should not favour one payment channel over another. For example, limiting CDR payment initiation's scope to NPP and PayTo would be inappropriate as it would not cover the full product market, and these payment types are significantly more expensive than alternatives like BECS, BPAY or batch files.

Reciprocity

We do not fully support the idea that all those who voluntarily become ASPs should also be automatically made Data Holders through reciprocity. The more ASPs that join the system the more functionality will be provided to consumers and the better outcomes that can be achieved. If reciprocity is to be introduced in this way, there should be a clear de minimis threshold included in the Rules to ensure that those seeking to innovate and offer exciting new services are not unreasonably disadvantaged by additional regulatory obligations.

Ongoing consents and authorisations

As noted in recommendation 4.11 of the *CDR Inquiry,* Action Initiation should allow consumers to provide consents to Accredited Persons to initiate actions on their behalf on an ongoing basis, within the consent's time limit. The benefits of Action Initiation will largely be derived from the ability for processes to be automated and for consumer friction to be minimised, such as through services that seamlessly transfer money between a consumer's accounts or periodically assess the market and automate applications for better products. These services will be heavily reliant on such functionality. Though the summary of proposed changes, privacy impact assessment and explanatory materials indicate that this capability is intended to be enabled under the proposed amendments, we think it is necessary to reiterate its importance and encourage the Government to ensure that the legislation does not inadvertently restrict the ability for such services to be offered.

Additionally, though we agree that ASPs should be able to undertake appropriate due diligence when assessing whether to progress Action Initiation requests received through the CDR, it will be important that they do not unreasonably impede these actions or implement frictions that undermine the operation of the system. Any attempts to do so should be met with regulatory repercussions. We understand this to be the intent of the non-discrimination requirements and support their inclusion. ASPs should have clear service level agreement timelines for types of actions in their CDR Policy (e.g. one business day to open an account).

Initiating actions with new Action Service Providers

Unlike under the existing CDR data sharing processes, Action Initiation will require consumers to be able to engage with ASPs with whom they do not yet have an established relationship - such as when applying for a new product. Ensuring that this is facilitated in a way which is both secure and minimises consumer friction will be fundamentally important to the CDR delivering on its full potential in enabling switching use cases. Again, the supplementary

documents provided suggest that this is an issue which is being considered in significant detail, which we are encouraged to see.

Furthermore, we encourage the Government to consider how digital identity solutions could potentially be integrated into the CDR system to make the switching process easier for both consumers and service providers. Being able to easily confirm to an appropriate level that an action is being requested by a specific, identifiable consumer will assist in further removing the friction involved with switching providers, and will increase consumer confidence and convenience. It will also assist in reducing the amount of excessive personal information which is collected, shared and stored - such as through photocopies of identity documents, helping to mitigate against the risk of data breaches. Considering how these initiatives can be successfully integrated at this early stage will allow them to more successfully complement one another in future. This would align with Recommendation 3.4 (identity verification assessments) of the *Review into Open Banking*.

Disclosure of CDR data by Action Service Providers to Accredited Action Initiators

The legislation hints at the fact that CDR data may be disclosed to an AAI from an ASP through Action Initiation (rather than through CDR data sharing). It is not clear from the materials provided what this data would be, what circumstances would result in such a disclosure, and why it is appropriate for the Privacy Safeguards to be extended in this way. For instance - most of the examples in the PIA document list that an ASP would disclose confirmation to an AAI that an action has been taken, but this does not meet the definition of CDR data. Any detailed information shared about a consumer should be as a result of a data sharing action and would be covered by the existing application of the Privacy Safeguards.

Interaction with other systems - PayTo and Digital Identity

In order for the CDR to succeed it must work alongside other digital initiatives to promote a common goal and to ensure reuse and return on investment. We consider that there are substantial opportunities to explore how CDR can work alongside advancements currently being progressed by both industry and Government - like PayTo and digital identity frameworks - to ensure that they enable the best outcomes possible for consumers. For example, the accreditation processes for these different initiatives should be mutually recognisable and leverage existing processes wherever possible, and consideration should be given

to how the infrastructure required to be implemented for each system can be reused where appropriate.

The ADI designation instrument should also be expanded to include information about PayTo mandates. These mandates include details about the different kinds of payments that the consumer has authorised - similar to a direct debit. This is relevant information to be included under the CDR.

Charging for CDR Action Initiation

Careful consideration should be given before a determination is made as to whether an ASP should be able to charge to accept instructions under the CDR. This should take into account the existing products that are charged for in full. For instance, PayTo introduces proprietary channels offered by ADIs that can be used to send payment initiation instructions. This service is broader than just a payment API, as the ADI effectively operates as a single point of entry to the PayTo ecosystem which reduces the need for a user to connect to every different ADI. This service is therefore more akin to an Action Initiation OSP and should be considered as such when determining whether an ADI should be able to charge to receive CDR payment initiation instructions.