Submission to the consultation on:

Exposure draft legislation to enable action initiation in the Consumer Data Right

24 October 2022

Executive Summary

Introduction

Biza.io welcomes the opportunity to provide feedback on the proposed exposure draft legislation to enable Action Initiation (AI) in the Consumer Data Right (CDR) Rules.

Biza.io is an established Australian fintech and the market leading provider of cross-sector CDR Data Holder solutions. Founded by the former Engineering Lead of the Data Standards Body (DSB), Biza.io has been involved in the Data Standards creation process since the very beginning and its personnel remain the largest non-government contributors to the consultations.

In addition to participation within the CDR, Biza.io is also a contributing member of the Financial-grade API (FAPI) Working Group, a contributor to the FAPI 1.0 information security profile, and a co-author of the Grant Management for OAuth 2.0 specification.

Beyond just a contractual engagement, Biza.io considers all its customers as partners in the journey towards the shared vision of open data. At the date of this submission, Biza.io is responsible for delivery of CDR data for approximately 20 Banking and Energy Data Holders.

Format of this response

While developing a response to this consultation it became apparent that the number of items that could be commented on are significant and key points could be lost in the complexity of the topic. Biza.io has therefore chosen to make the following **6 sets of observations** that it believes to be of most relevance given Treasury's proposed direction.

1. Experimentation and activation phase
2. Instruction Layer and action complexity
3. Information security implications
4. Incentivising participation
5. Service provider compliance impact
6. General observations

The information provided is based upon a review of documents provided on the Australian Government's Treasury website at https://treasury.gov.au/consultation/c2022-317468

Experimentation and activation phase

Biza.io is highly encouraged by the movement of the CDR into AI. Enablement of actions has the potential to dramatically increase adoption. However, we are also wary of decisions made prior to validation and recommend that Treasury consider an experimentation phase for AI introduction.

Learning from prior CDR experience

Previous evolutions of the rules involving joint accounts and intermediaries provide a timely reminder of the difficulty in defining rules without proven technical and use case context. The subsequent need to adjust and retrospectively add rules was a slow and expensive process and we must avoid a repeat of this. While Biza.io recognises and applauds the urgency to progress AI, it will be a false economy to impose unproven legislation and related data standards upon participants.

Industry and consumer working groups

Treasury should consider creating and supporting dedicated working groups tasked with designing a set of robust rules and standards that are fit for purpose. These groups should include broad stakeholder participation but retain a hard outcome focus. This would reduce the likelihood of overlooking fundamental implementation issues. This approach is not dissimilar to CDR's original industry testing that took place between September 2019 and July 2020 involving the four major banks and a small number of prospective Accredited Data Recipients (ADRs).

Inclusion of Customer Experience (CX) design function

The working group composition should include representation from Data Standards CX teams to ensure proposed approaches have at least undergone rudimentary consumer testing. This will minimise risk of imposing unworkable obligations on consumers.

Contribution recognition

To date the private sector has significantly contributed to CDR without financial benefit and revenues remain minimal in line with adoption. Federal funding has supported the creation of CDR functions within government agencies, yet these bodies lack the practical experience of industry participants and the diversity of skills present within private industry. To attract the required specialist contributions necessary to develop robust and appropriate rules and standards, commercial reimbursement should be considered. Without such recognition in place the government may find itself competing with private industry equivalents operating outside the CDR framework.

Adjustments to rulemaking and standards setting processes

It is likely that enabling of AI will require multiple iterations and validation that the proposed approach delivers value to consumers. On this basis there is scope to alter the existing rules and standards setting processes to consider a period where actions intended for mandate operate within a proving phase to elicit live feedback from the ecosystem.

Instruction Layer and Action Complexity

There appears to be a general perception that actions are independent and atomic and that they can be issued by a consumer to an initiating third party via a simple instruction layer. Biza.io believes that many of the actions proposed to date do not fit this model as they are actually *groups of actions* requiring more complex arrangement and ongoing dialogue.

Actions may be bundles of actions

Example 1.2 within the Exposure Draft Explanatory Materials describes a consumer payment. It is suggested that, upon instruction, a bank would make such a payment using existing (non-CDR) infrastructure, rules and processes. Putting aside the need for an existing and active consent to be in place for data sharing (in order to support a balance check), the described payment 'action' would involve multiple steps. These steps might be:

1. Provision of target PayID or BSB/Account for recipient bank
2. Validation of recipient account details (PayID obligations exist here)
3. Confirmation of proposed transaction and payment method by consumer
4. Lodgement of AAI instruction with initiating bank
5. Return of unique identifier representing the instruction
6. AAI polling or checking payment status
7. ASP/AAI updates on reversals, network execution issues

Items 1-3 require the consumer to be present, interacting in turn with the AAI in response to the results of the AAI's interactions with the ASP – so this is not one single instruction.

Items 6 and 7 introduce the need to monitor for state changes and protocols to support this. Actions may not complete, they may just reach a state that is usually permanent. Payments can be reversed so clarity on obligations and responsibilities here will be required.

It may be helpful to consider an action validation instruction prior to the action itself being submitted. This could improve likelihood of success but may also increase consumer burden. Biza.io flags the undesirable potential for exacerbating consumer consent fatigue through numerous independent related actions requiring multiple consent executions, potentially at the same time. This can be avoided through carefully considered experience design coupled with a deliberate acknowledgement that individual atomic actions are implicitly different from groups of actions to achieve a particular consumer outcome.

Instruction Layer interaction

Although it is proposed that ASPs make use of existing infrastructure and processes to carry out actions, the AAI-to-ASP interface through which these interactions must occur does not exist and must be built, yet the model for this is not defined.

Should AAIs interact directly with consumers, relaying requests from ASPs? Or is it assumed that, upon receipt of an action request, ASPs switch to alternate and direct channels of interaction with consumers? Perhaps it is implied, or perhaps it will vary based upon the type of action being performed, but *Diagram 1.1 – Participant Roles in CDR data sharing and action initiation* in Explanatory Materials does not provide any indication.

Actions are not always customer present

Broadly speaking the current proposal appears to focus its energy on a deliberately structured approach that assumes the consumer is continuously present and that actions will be conducted in a single "motion".

The reality is that for a significant, possibly a majority, of actions this is untrue. A consumer may *not* be present at the time of the submission of an action, instead receiving a notification to approve via a backchannel (such as an internet banking application).

Additionally, actions may take an extended period of time to complete. Simplistically this would apply to loan origination and actions which involve the use of "wet ink" contract signatures. In these cases, actions may persist, awaiting completion for days or weeks while external factors are resolved.

On this basis it seems logical to assume that actions can be synchronous *or* asynchronous as well as online, offline or both. By way of example the following simplistic table highlights some common use cases and the separation required:

	Online	**Offline**
Synchronous	Shopping Cart Checkout Payment Subscription Payment Initiation	High Value Payment requiring Mobile Banking approval Extension of Subscription In Store Purchases
Asynchronous	Identity Verification Setup Customer Detail Updates requiring internal approval Energy Account Churn Mobile Number Churn	Loan Contract Signing Nominated Representative Form Signing In Store Financing

Information Security Implications

Biza.io notes there are no changes to the Schedule 2 rules covering information security obligations on accredited persons. It is likely that these will need to be enhanced given the increased risk exposure associated with actions such as payment initiation.

Enhanced consumer authentication

Action initiation will require enhanced authentication and authorisation mechanisms between ASPs and their customers, most likely involving second or further factors. Within the banking sector this would align with existing risk-based access controls used by DHs.

Risk based ASP authentication

Not all actions carry the same risk and ASPs will have different positions based on the type(s) of action(s) they support and their own stated institutional risk appetite. This will also differ by sector. Finding consensus may be challenging. Banks already have a clear position on which actions can and cannot be undertaken without additional controls. Some banks may require a customer to call their contact centre and undergo verification in order to update their mobile phone number. Others may permit this within a digital channel following additional 2FA. Presenting a consistent consumer experience under CDR AI across all ASPs will be extremely challenging, even for what appear as simple actions.

Accreditation thresholds

Biza.io believes that there should be an accreditation review and uplift for AAIs, however the existing ADR requirements could well carry over without the need for wholesale change.

It may be appropriate to develop differing accreditation obligations for payments related AAIs whose actions are likely to be riskier in nature than those of ADRs whose accreditation is limited to the collection and use of consumer data.

Where such a distinction is made, further options could be considered. The ACCC may wish to take a highly prescriptive (and higher maintenance) approach, specifying actions an AAI is permitted to perform. Alternately, actions could be grouped into classes such as Financial Payment Instructions, Energy Account Instructions or Customer Detail Update Instructions.

Incentivising participation

Throughout the development of CDR, the government of the day has relied upon compliance and enforcement to increase participation of DHs. ADRs have been slow to participate due to existing, proven alternate data sharing methods. Biza.io believes a softer, incentives-based approach might be more effective for AI. A focus on encouraging participants to buy into a vision for CDR may reduce the likelihood of them seeking to achieve their business objectives outside the ecosystem.

Cost of compliance for ASPs

We should recognise that DHs have effectively funded the CDR data publication regime themselves as required by legislation. Consumer data sharing was (and still is) a compliance obligation for banks under CDR. There has been no opportunity for DHs to monetise their services and this has resulted in quality and performance that at best meets a stated requirement. This has played out to the detriment of consumers and ADRs.

Requiring ASPs to similarly expose services to AAIs without a commercial incentive is likely to result in further frustration for existing DHs and unlikely to result in committed participation at scale from new ASPs.

We have an opportunity to change this with AI.

We should consider how CDR AI can provide ASPs with better reasons to invest in CDR, stimulate innovation and unlock potential for consumers.

Learn from the UK's open banking payments experience

The UK's open banking regime experienced this same issue where the 9 major banks were required to expose single instant payment services without charge. Implementations were protracted and lengthy and while the UK enjoys both data and payments capability today, the scope of both sets of services remains limited. Only recently with Variable Recurring Payments, are banks finally able to monetise some of their services.

Service provider compliance impact

Many banks failed to meet their initial compliance obligations for the publication of consumer data in 2021 and this situation has continued into 2022 with joint accounts and business accounts. While there are many reasons for this, a large contributing factor was the reliance of ADIs on third party technology providers. We anticipate a similar outcome with AI and potentially a situation where some providers do not offer such services.

Core banking vendor engagement

A large number of the prospective ASPs within financial services employ the services of third-party vendors and white label platforms for core banking functionality. This functionality encompasses many of the proposed AI actions.

While DHs were able to explore a range of options to meet their data publication obligations in the first phases of CDR, 'write access' is an entirely different proposition. Legacy core banking systems do not offer integration capabilities appropriate for the emerging requirements of AI under CDR. This presents a considerable issue for ASPs that will be obliged to meet coming legislation. While exemptions may provide short-term reprieve, these institutions ultimately risk non-compliance and enforcement action from the ACCC.

It may not be possible for a regulator to compel technology service providers to provide compliant solutions to their clients in a timely manner, but perhaps these providers could be required to support integration work that creates other options for ASPs.

ASP processes, fraud management systems and appetite to risk vary

Even when integration with banking platforms is possible, compliance with prescriptive rules and standards may present challenges for Australian institutions.

Unlike consumer data sharing, more rigorous controls are required when carrying out payment instructions in the banking sector. ADIs and therefore ASPs will have differing operating models. Some will require a second factor of authentication (2FA) for particular types of payment transaction, perhaps to a new payee or if the instruction came from an unfamiliar device. The 2FA may require input of a One Time Password (OTP) provided through an independent process such as an authenticator app, a physical token or push notification from a mobile application. Even when the payment is submitted to the ASP, internal fraud monitoring systems may trigger alerts and potentially hold payments pending further consumer interaction.

This independence and variability of approach will also change over time based on market and environmental factors. If CDR payment AI is to operate consistently and successfully across all ASPs, these factors will need to be accommodated and managed through predefined and standardised responses, messaging and CX.

General observations

The following additional matters came to light as part of Biza.io's review of consultation materials and are included here for completeness.

Environmental factors outside CDR

Biza.io notes there are existing restrictions associated with services in scope for the proposed Action Initiation framework. For example, many banks place an arbitrary daily limit (as low as $1,000) on the value of PayID transaction values which may result in an AAI being unable to complete certain actions. This issue has impacted open banking use cases such as online car purchasing in the UK and remains unresolved.

Rather than wait for CDR to encounter and then attempt to remedy these types of issues, it would be advantageous to surface them during the proposed proving phase and commence the inevitably lengthy corrective action earlier.

The role of intermediaries in Action Initiation

Should we consider intermediaries as part of AI? Rather than AAIs communicating directly with ASPs, some companies may prefer to use an OSP for this purpose. This could be particularly effective if proprietary integrations are required between the instruction layer and ASP systems. Intermediaries may offer an advantage here in being able to invest in the design and development of individual bilateral arrangements that can then be offered as an outsourced service to AAIs.

However, the use of intermediaries may significantly increase the risk profile of actions. If they are to be included, there should be traceability through multiple parties, and this must be exposed to holders and ASPs. Recent privacy act proposals serve to highlight increased exposure of holders to such risks outside their control.

Consistent notifications experience

To date, CDR has included a range of imposed and optional notification arrangements for consumers. With the broadening of scope into AI, a well-structured technical solution to notifications is becoming an imperative. This should cascade through both consumer and accredited person levels to be consistent throughout the ecosystem.