BIZA·IO

Submission to the consultation for

Consumer Data Right rules amendments (version 3)

30 July 2021

Introduction

Biza.io welcomes the opportunity to present its thoughts and recommendations regarding the Consumer Data Right Rules v3.

Biza.io are the market leaders in Data Holder solutions to the Consumer Data Right and are the only pure-play CDR vendor in Australia. 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 its participation within the CDR, Biza.io is also a contributing member of the Financial-grade API (FAPI) Working Group, contributors to the FAPI 1.0 information security profile, and co-authors of the Grant Management for OAuth 2.0 specification.

As of July 2021, Biza.io is directly responsible for delivering, or heavily involved in the verification of, one in three of all active Data Holders. Beyond just a contractual engagement Biza.io considers all its customers partners in the journey towards open data. Our customers choose us to not only achieve compliance but to compete then command the consumer data ecosystem.

Overview

Biza is broadly in favour of the new amendments. We are strong proponents of increasing the number of participants in the CDR, *as long as the security of the ecosystem remains such that all consumers and all participants can trust the transmission, storage and usage of consumer data*.

The data transmitted, stored and consumed under the CDR is sensitive. On its own, banking data is highly personal. Taken in concert with data from other industries like energy, telecommunications, insurance and so on, it becomes even more revealing. Indeed, noted digital financial services and identity commentator David Birch has labelled personal data *"the new toxic waste"*[1].

Biza.io believes that all participants in the CDR, including the new categories proposed in the amendments to the Rules, should be protected by and subject to an equivalent information security (InfoSec) posture as that of the existing ecosystem participants. While we accept that contractual obligations provide significant protection, we feel that these should not diminish the InfoSec technology requirements as, in the event of a breach, data compromise is irreversible.

In this submission, we will detail some of the issues that are present in today's data sharing landscape that back up our position for strong InfoSec requirements across all new participant categories.

[1] https://blog.dgwbirch.com/?p=438

Data Sharing

APIs power the sharing of data across the internet. While current CDR Accredited Data Holders and Data Recipients operate under a strong InfoSec regime, this is not the case in many non-CDR API environments.

Yes, transport security is (mostly) always provided by TLS, which (mostly) prevents eavesdropping as data is transferred from holder to recipient. TLS guarantees the identity of the server to the client and provides a two-way encrypted channel between the server and the client.

However, the use of TLS does not validate that the recipient is who they say they are. In the CDR, this function is provided by Mutual TLS (MTLS) and constrained within a circle defined by the ACCC Certificate Authority. In many non-CDR environments, Mutual TLS, with its requirement for the recipient (client) to present a digital certificate, is not used. Instead, client authentication in many API-based environments still uses username/password authentication — so-called Basic Authentication.

By way of example, a new participant is Sponsored by an existing Unrestricted ADR. The Unrestricted ADR uses MTLS in its communications with Data Holders. But its communications with Sponsored participants may remain using legacy Basic Authentication. The Sponsored participants are therefore more vulnerable.

If Strong Authentication[2] is not mandated within the client security model for new CDR participants, then we consider this to be a major flaw. Indeed, one of the original intents of the CDR was to remove the need for screen scraping — the process whereby a Data Recipient requests a consumer's username and password, then replays it to the Data Holder. In effect, allowing Basic Authentication in downstream participants of the CDR would be a very minor uplift in security from screen scraping.

Biza.io believes that removing Strong Authentication should be avoided at all costs in the CDR ecosystem. We recommend that all new participants be required, at a minimum, to make use of MTLS to ensure conformity across the CDR, and to prevent them becoming the attack vector of choice by bad actors, due to their diminished levels of security.

By requiring all of the new participant categories to obtain and use a digital certificate created by the ACCC Certificate Authority, all communications (data sharing and future action initiation) will be secured at the same level. An additional benefit of this approach would be, in the event of a data breach at an individual downstream party, the regulator would retain the technical ability to halt data sharing of that particular downstream participant.

[2] https://en.wikipedia.org/wiki/Strong_authentication

Data Disclosure Traceability

Biza.io believes that the ability for a consumer to have traceability of their data disclosures, throughout the ecosystem, is a critical element of a successful and trustworthy data sharing ecosystem. While there have been changes made in the proposed rules with respect to the Data Recipient's dashboard, there does not appear to have been a similar change made for Data Holders.

Our concern is that a Data Holder's dashboard may show inconsistency with respect to the Consumer's perceived relationships with parties downstream from a Data Recipient. For example, Geoff may access their Big Bank dashboard and see that their data was disclosed to Mega Mortgage, when in reality, Geoff believed he disclosed data to Jane's Mortgage Broker. The lack of this visibility at the bank level could potentially breed distrust of the ecosystem.

Biza.io recommends that the rules incorporate a need for Data Holders to provide details of disclosure including downstream parties. As part of its ongoing work to innovate within the data sharing space Biza.io is continuing to develop solutions for this problem.

Action Initiation

The development of a framework for Action initiation was recommended by the *Inquiry into Future Directions for the Consumer Data Right* by Scott Farrell. Actions discussed in the recent Data61 Action Initiation Workshop include allowing accredited third parties to initiate payments, and simplify the decision making involved in and the process of switching accounts, amongst others.

The impact of fraud or malicious actions during action initiation have the potential to be as significant as data theft via CDR data sharing mechanisms. Beyond payment initiation, the enabling of actions such as closing a bank account or disconnecting an energy provider could have negative, irreversible and long-lasting effects on the impacted consumer.

For that reason, Biza.io recommends that the same information security controls and standards be used for action initiation ("write access") as used for data sharing ("read access").

Joint Accounts

On the amendment for Joint Accounts (4a), Biza does not have a strong opinion either way with respect to this amendment. As a technology provider, we are able to support either *pre-approval, co-approval or non-disclosure* options as set out in the proposed rules. We note that the pre-approval option is likely to have a lower friction and better customer experience than the original *co-approval* option.

We look forward to a future evaluation of these options in the context of multi-party accounts such as those commonly associated with business accounts.

Consistency

Consistent standards across all designated sectors of the CDR is also important. If data sharing and action initiation is to be broadly adopted by organisations in Australia, whether they are unrestricted or not, there must be consistency in the specifications. This will allow the implementation of each sector's specification to be possible without confusion or misunderstanding, both of which could lead to security flaws or costly interoperability problems.

Recommendations

Biza.io recommends:

1. Require the use of ACCC Certificate Authority MTLS for all participants in the CDR, including the new models proposed in the amendment
2. Incorporate rules for Data Holders to expose downstream parties within their Consumer dashboards
3. Mandate consistent information security controls for action initiation and data sharing
4. Mandate consistent information security standards across designated sectors