Summary of Recommendations

Commonwealth Bank is supportive of the principles that have been applied to developing the Consumer Data Standards (Standards).

Standards

With respect to the standards, Commonwealth Bank is broadly supportive of the recommendations associated with the versioning of APIs, HTTP response code definitions, and payload extensibility. Further clarity is required around the definition of fields marked as mandatory or optional.

We are partially supportive of the definition of API versions with a recommendation around standardising to HTTP header versioning only. Commonwealth Bank also has strong views around technical complications relating to pagination and recommends the use of cursor based pagination as an alternate approach. Lastly, Commonwealth Bank recommend Data61 revaluate ID permanence for its complexities.

Security

In relation to information security, Commonwealth Bank is concerned that important topics are yet to be addressed. Given the relationship between the API Standards and Security Standards, it is difficult for us to provide support around a number of topics until more clarity is provided on security.

There has been limited documentation available regarding the Information Security Standards and the lack of clarity around this is emerging as an implementation risk for the regime. Commonwealth Bank recommends that Data 61 devote additional resources towards developing standards in this area, provide additional time for review, and ensure that industry participants are able to submit separate feedback regarding the Standards for information security once they are released.

A key concern around information security is the ability for a consumer to provide fine grained consent to data being shared, and this has not been adequately reflected in the standards established to-date.

The regime should ensure that security standards define how to prevent known vulnerabilities associated with API implementations from being easily exploited through common attack vectors, such as phishing attacks. For this reason we continue to advocate for a decoupled authentication framework, as opposed to redirection frameworks from uncontrolled devices, to re-enforce safe practices and help protect consumers.

Banking APIs

Commonwealth Bank is broadly supportive of the majority of the API definitions relating to accounts. Our primary concerns are around the scope of included data. We believe the current coarse-grained approach may lead to unnecessary over-sharing of sensitive data. For particular aspects of the standard, such as the implementation of individualised account objects and bulk data, we have technical concerns around the complexity which will result in a protracted delivery timeline. As such we suggest that they are pushed to a further version of the standards to accommodate this.

The product reference data API requires further assessment. Commonwealth Bank recommends Data61 continue to work collaboratively with the industry to understand how to best represent product in the regime and refine this API.

We also re-iterate our concerns about the inclusion of a direct debit payload as this data is not held by the bank. Finally, we have concerns around the potential leakage of Personal Information which is included in the payee payload.

Common APIs

Commonwealth Bank are not supportive of the current definition of the customer payload. We believe description and use cases of this API are not fit for purpose and could again lead to inadvertent data leakage. We recommend the deprecation of this API in favour of an amendment to the accounts payload, and use of the OAuth 2.0 UserInfo service.

Additional Recommendations

- Testing
    - The Commonwealth Bank needs adequate testing standards to ensure we are building what is required for July. This must be included in version 1 of the Standards in December.
- Reporting
    - The administrative endpoint is still a pending decision proposal on GitHub (28th July 2018). Clarity on reporting requirements is necessary so we have time to build the required capability in time for 1 July 2019 compliance.
- Authorisation Flows
    - We understand that these proposals will be considered more fully in the information security working groups and welcome additional workshops to facilitate this discussion.

1.1 Standards

1.1.1 Principles

The principles defined as part of the setting of the Consumer Data Standards process reflect their intent. In particular Principle 1 states: "The API definitions will consider and incorporate the need for a high degree of security to protect customer data. This includes the risk of technical breach but also additional concerns of inadvertent data leakage through overly broad data payloads and scopes. The security of customer data is a first order outcome that the API standards must seek to deliver." Commonwealth Bank strongly supports this principle as a central requirement for building trust and transparency within the Consumer Data Right (CDR) regime.

It is important that the Consumer Data Standards find a balance that makes it simple and easy for consumers to share their data in a way that doesn't undermine their privacy and security. From our research we know that consumers have an expectation that the banks will keep their data secure without them needing to be concerned with unnecessary risks.

1.1.2 Versioning Methodology

Commonwealth Bank supports the implementation of versioning but seeks the following clarity surrounding the implementation:

- How long will participants be expected to supported and maintain previous versions?
- Will different lead time for implementation be available for major version vs minor changes?
- How many versions does a data holder need to support?
- Will data holders and recipients be expected to migrate consumers onto new versions?

Clear requirements regarding the process for either developing and implementing additional or amending existing standards is required. Commonwealth Bank expects that many of these issues will be addressed in the Consumer Data Right Rules as they have not been included in the Standards. Commonwealth Bank further recommends that data holders are consulted on the proposal surrounding timelines for implementation in regards to material changes to the standards. Consideration for analysis, build, testing and implementation of new mandatory fields will need to be completed before delivering any new version(s).

1.1.3 HTTP Versioning

Within the current proposal there is a potential for conflict between versions proposed in the HTTP header and URI version and this adds complexity for both the API provider and consumer. Commonwealth Bank proposes that we adhere to the UK standard of including version number only within the HTTP Header. Version numbers should be kept to a minimum and only be used when an interface breaking change is introduced.

Correlation-Id provides a reliable way to track any given transaction between consumer and data holder rather than a timestamp and is an important element for testing. This header field should be mandatory so that developers can ensure consistency for the consumer and reconcile the response on the developer end. Timestamp on its own is not a reliable way to track transactions because it can be out of sync between API data recipient and data holders.

1.1.4 HTTP Response Codes

Overall Commonwealth Bank is supportive of the response codes. We recommend Data61 ensure that all response codes are aligned with the expectations of the non-functional requirements as they are designed.

1.1.5 Payload Conventions

Greater clarity is required on the definitions of 'mandatory' and 'optional' fields. Commonwealth Bank considers that an appropriate approach would be to define 'mandatory' fields as referring to the core data fields requiring a response. Where a data holder does not hold that field, an empty string could be returned but a data holder must return a response.

'Optional' fields should refer to non-core data fields that a data holder may provide at their discretion. The latter category would extend in future versions to potentially chargeable data fields that may not be held by all data holders or standardised across the industry.

1.1.6 Pagination

Commonwealth Bank would like to recommend an alternate approach for pagination. The proposed solution does not take into account that adjustments may be made to payloads over a regular period due to new items being committed to ledgers. As a result, new data items will be introduced invalidating the page offset parameters. To ensure a performance and optimal response Commonwealth Bank agree there is a need to implement pagination, but we propose the use of cursor based pagination.

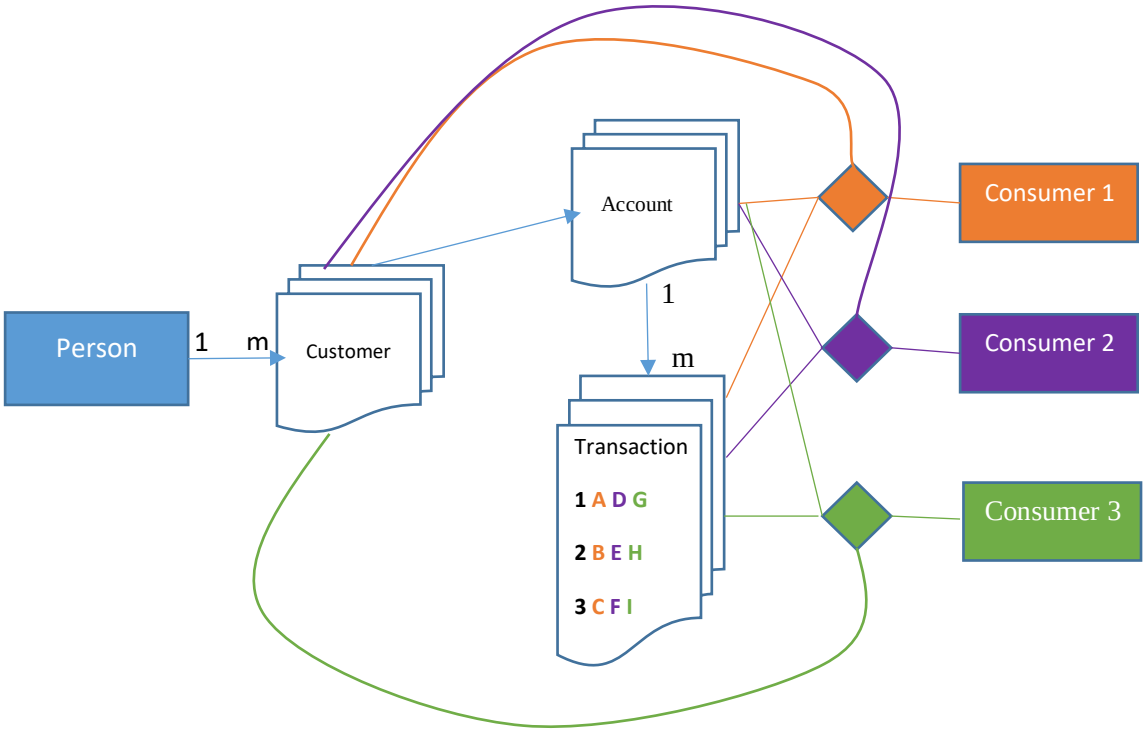
1.1.7 Extensibility

Commonwealth Bank supports the Extensibility Standards however requires greater clarity regarding the process for the creation of new API payloads as the CDR expands to industries beyond banking. Consideration should be given to issues concerning how the Data Standards are likely to iterate in line with the regimes extension to additional industries and banking products:

- The ownership of versioning and supporting new end points.
- The engagement process and sign off of new end points.
- Versioning catalogue of all the new and existing APIs.

1.1.8 ID Permanence

Commonwealth Bank is not supportive of the current implementation requirements for ID permanence. As the regime is scaled out to include other industries limitations in storing and creating different permutations of the data become exposed. Creating unique IDs for each specific relationship is a significant amount of data for each provider to create and ingest. Furthermore when the unique IDs for each product are included in scope, applying the ID permanence standards would create a unique product ID for each relationship with a consumer, distinct from the product API identifiers. This would lead to infinite variations of IDs. As exampled below as each new relationship is created a new permutation of an ID is also rendered. The industry needs to address the issue and decide on an approach that would still create security for the consumer but allow the data holder the flexibility to limit the amount of permutations.



1.2 Security

1.2.1 High Level Profile

Commonwealth Bank is committed to protecting consumers' data. The success of a future Open Banking regime will rest heavily in the security of the data sharing framework.

There has been limited documentation available regarding the Information Security Standards and the workstream is far behind in establishing the standards needed to ensure that appropriate security safeguards will be in place by the commencement of the Open Banking regime. The lack of clarity around information security is emerging as an implementation risk for the regime. As a consequence, Commonwealth Bank recommends that Data 61 devote additional resources towards developing standards in this area, provide additional time for review and ensure that industry participants are able to submit separate feedback regarding the standards for information security, once they are released. The security implications of decisions require deep analysis and should therefore not be rushed.

1.2.2 Authorisation Framework

Commonwealth Bank support a decoupled authorisation approach, which is compatible with the FAPI Standard. The ACCC's 'Scamwatch' shows that phishing attacks are a significant economy-wide cost, with more than 19,000 phishing attacks reported and over $570,000 lost by consumers due to such attacks so far this year[1].

We believe that the proposed Redirect/Hybrid approach introduces significant weaknesses into the authorisation process and increased risk for consumers.

1.2.3 Additional Constraints

Commonwealth Bank supports the use of the financial-grade API Read/Write (FAPI R/W) profile. We also support the use of Mutually Authenticated TLS (MTLS) v1.2 and above to secure

[1] ACCC. 2018, "Scam Statistics: Phishing", accessed online at: https://www.scamwatch.gov.au/about-scamwatch/scam-statistics?scamid=31&date=2018

back channel communications between the data recipient and data holder. Lastly, we also support using certificate bound access token.

Standards and expectations for Key and Secrets management (for example granting and revoking accreditation to data recipients) must be addressed in the Standards. This includes expectations and agreed Certificate Authorities, and mechanisms for the issuance and revocation of Certificates to data recipients and data holders.

Data holders should be accountable for maintaining a Key Management Plan (KMP) for any cryptographic keys used by their services. The KMP should describe procedures to ensure keys are always kept secure and managed securely through their lifecycle.

1.2.4 Authorisation Scopes

We are concerned that consumers will not have enough control over information they consent to share with data recipients. Additionally, the unintended transfer of sensitive data means that consumers could be at greater risk from fraud or identity take-over.

The authorisation scopes described in the Draft Standards, which users consent to sharing, are bundled into large groupings. These large 'catch all' scopes need to be re-considered and consumers provided with the opportunity to provide more granular data at their discretion. Consumers also need to be informed about the specific data being shared in each instance.

The UK Standards are a useful case study as they separate Balance and account. While the UK has similar authorisation scopes in terms of the call, GET /accounts/{AccountId}, the information included is significantly different. This ensure that only the necessary data is shared in order to use a service.

The Commonwealth Bank also has concerns about consumers who hold authorisation over multi-party accounts, or accounts of another individual, such as child.

Current Data Scopes	**Commonwealth Bank Specific Comments**
Basic Bank Account Data	• Basic Account data should be separated out to give consumers greater control over data being shared. • Consumer to select specific accounts.
Detailed Bank Account Data	• Consumer needs to be aware of the extent of data that is being shared. • The UK model as an example separates balance and account data.
Bank Transaction Data	• The authorisation scope 'Includes all account transaction data.' The difference between the detailed and basic endpoints for transactions should be distinguished.
Bank Payee Data	• We support this being separated from a consumer and an account. The information would be considered personal information but we understand this will be addressed in the Rules.
Basic Customer Data	• We support the data scopes being separate however are concerned about the personal information being included in the payload.
Detailed Customer Data	

1.2.5 OIDC Scopes & Claims

The OIDC userinfo support decision proposal was closed during the release of the Draft Standards. However there had been discussion on the distinctions between customer and user by Data Action. Commonwealth Bank encourages Data61 to address this concern, which was also echoed through feedback in the GitHub forum.

1.3 Banking APIs

1.3.1 Account

Commonwealth Bank is partially supportive of the proposed account payload but has concerns regarding the requirements for detailed personalised account parameters. Implementing individualised features, fees/discounts, depositRates and lendingRates on an account is challenging to deliver, specifically:

- Account level parameters is a calculation derived from multiple discrete components.
- A calculation must be performed at time of enquiry to produce accurate pricing and as a result a stored (cached) price would be inaccurate.
- The amount of workload this introduces creates risk of overloading core banking systems, putting the overall data ecosystem at risk

We would recommend that Data61 defers the mandatory detailed account endpoint to a later version of the Standards to ensure adequate time for data holders to enable this capability.

1.3.1.1 Bulk API Payloads Account & Transactions

Commonwealth Bank recommends changing bulk APIs to optional to be equivalent to the specifications within the UK Open Banking regime note. We also suggest optional Bulk APIs be removed from scope for the 1.0 deadlines to enable focus on a define MVP.

1.3.1.2 Balances

Commonwealth Bank is concerned around the mandatory inclusion of a balance payload for every request of an account (basic or detailed). We recommend that this information be included in a separate authorisation scope and URI. This would help prevent unnecessary data leakage in scenarios where account features are needed but balance are not required (such as product comparison).

1.3.2 Transaction Payload

Commonwealth Bank does not support the inclusion of search-based functionality (text, min-amount, and max-amount) as a method of filtering the transactions payload. This is a feature that should be constructed by the data recipient, to enable a consistent user experience across institutions.

Commonwealth Bank also recommends the inclusion of the following additional fields into the transaction payload:

- Merchant Category Code (MCC) a four-digit number listed in ISO 18245 for retail financial services.
- BPay biller code and the corresponding CRN (Customer Reference Number)
- The 6 digital APCA User ID

The inclusion of pending transactions creates complexity and data quality concerns around the treatment of expired pending transactions. Commonwealth Bank recommends that only reconciled transactions be included in the regime to ensure data quality.

1.3.3 Product

Commonwealth Bank does not support the current data model for version 1.0 of the Consumer Data Standards. We also request further guidance from Data61 as to how complex products will be represented in a way that provides value for consumers.

As referenced in section 1.3.1.4, account detailed payload, the product specific information needs to be assessed in detail by product experts. These fields will be subject to change as products are brought into scope. The Standards need to remain flexible to allow for version control as product mapping will likely vary amongst data holders.

For example, the concept of multiple features, fees, and bundling etc. attached to a single product reduces the usefulness for relevant product comparison due to the range and complexity of product offerings across data holders. For example, there is varied eligibility criteria which maps to different combinations of rates and fees. As it stands, the product API will be required to produce large data sets for every instance due to the numbers of possible permutations. These should instead be abstracted to a separate end point if the product reference data is at a detail line item level.

Additionally, Commonwealth Bank believes field such as the effectiveFrom and effectiveTo attributes are ambiguous and require additional clarity.

Commonwealth Bank requests further workshops on the product payload to ensure that proposed model is fit for purpose.

1.3.4 Payee

Commonwealth Bank is not supportive of the inclusion of a Payee payload in version 1.0 and recommends further review by the information security working group regarding the potential of personal information leakage.

Commonwealth Bank is required to mask credit card numbers to maintain compliance to the PCI-DSS industry standard. Currently within the wider banking section of the Consumer Data Standards, account number is masked by default, however the payee details payload returns full account details of individuals who have not explicitly provided consent in the regime. Data61 should investigate options to also mask account.

Inclusion of personal information is a privacy concern to the related consumer who has not expressly given consent to share their account information outside of the purpose it was originally designated for.

1.3.5 Direct Debit

Commonwealth Bank is not supportive of the inclusion of a direct debit payload in the regime as this information is not stored by banks, but rather by the organisation holding the debit authorisation.

1.4 Common APIs

1.4.1 Customer

Commonwealth Bank is not supportive of the inclusion of a 'customer' API. The main concern is the intent of the API, as there is no guarantee that the user requesting the data is a customer of the bank, as opposed to an authorised agent of a customer. In the event of the request coming from a non-customer operator there is potential leakage of personal customer information without express consent. In addition, the customer payload does not provide capability to determine ownership of the accounts being returned by the Account APIs. There is also

complexity if a customer of Commonwealth Bank has additional non-customer roles e.g., accountants, payroll clerks, or parents.

Commonwealth Bank recommends the deprecation of the Customer payload for the banking sector in favour of an increased usage of the UserInfo payload as specified by OAuth 2.0. We would also suggest an addition of a role and person payload to be added to the accounts to allow for this data to be returned in a manner that is representative of the ownership model associated with the more complex accounts in the banking sector.

Alternatively, Commonwealth Bank would suggest a fine-grained authorisation to apply to the data available within the Customer payload to avoid any unnecessary data leakage.