Chapter 4 - Part 2: The Saga Continues.

A Breakdown of the Inquiry into Future Directions for the Consumer Data Right - Final Report.

With 23 recommendations, numerous tables and examples provided, chapter 4 is by large one of the weighted chapters within this report. I had hoped to provide a more palatable explanation by breaking this chapter into two. However, I fear that this second part will end in tired eyes and a need to take several micro-breaks! As one can expect with the finer details of introduced legislation and accompanying policy, this is dry content but critical none-the-less if its introduction will be successful. I implore you to hang in there with your exploration of Scott's work, and please feel free to provide comments or your thoughts as we journey through this together.

THE ACTION INITIATION PROCESS

The process for Action Initiation must be consistent with the process of data-sharing.

Recommendation 4.5 – Action initiation process

Action initiation through the Consumer Data Right should be based on the existing consent, authentication and authorisation processes currently used for data sharing, with appropriate amendments.

ENGAGEMENT

SUPPORTED INSTRUCTIONS

In considering the inclusion of Action Initiation into the CDR, each sector must consider which data holders should be obliged to accept instructions and which classes of actions should be included. CDR Action Initiation should enable an accredited party to do something that the consumer can already do on their behalf. This excludes the accredited party forcing a data holder to perform an action that it does not offer or prohibited under other regulation.

Actions should be prioritised within each sector, allowing for those actions that best suit Action Initiations and will most likely drive consumer benefits to be introduced first. Ideally, this prioritisation should be given within the same sectoral assessment process that identifies potential data sets and data holders. More complex functionality is raised after the basic system is established.

The inquiry has found that both mandatory and voluntary actions should be initiated.

Recommendation 4.6 – Supported instructions for action initiation

Action initiation in the Consumer Data Right should only enable an accredited person to initiate actions which the consumer is already able to perform with a data holder. Action initiation should not be used to force data holders to perform actions which they would not otherwise offer, or which are prohibited under other regulation. This principle should be used to steer consideration of what actions are designated for action initiation.

The doesn't mean that all actions given by the consumer should be permitted due to security and privacy risks. These actions may vary from sector to sector and should be determined during the sectoral assessment or implementation phases. Actions such as enabling a third-party to update a consumer's information, such as their passwords, have been explicitly excluded from the CDR, including a voluntary data set.

Recommendation 4.7 – Exclusion from action initiation

Certain actions that are deemed to be of significant risk to consumers' security or privacy should be excluded from being able to be actioned through the Consumer Data Right. Such actions should be determined through consultation with industry and consumer representatives during the sectoral assessment and implementation within a sector. The updating of passwords is an example of one such excluded action.

The inquiry has identified some general classes of action that may be appropriate to designate within the CDR. These types of classes are generically related to customer relationship flow.

Table 4.1 – Potential supported actions

Customer relationship	Product or service	Communication
• Opening a customer relationship • Managing a customer relationship • Closing a customer relationship	• Applying for a product • Managing a product • Closing a product	• Notifications • Complaints

ESTABLISHING AND MANAGING A CUSTOMER RELATIONSHIP

ESTABLISHING A CUSTOMER RELATIONSHIP

To uniquely identify the customer, service providers commonly ask a consumer to establish a 'customer relationship'. This establishment allows the provider to create them within their system and allows them to clarify points of contact and authentication procedures.

The process of creating and establishing the customer relationship is different from most other actions under the CDR, as it requires the accredited person to send a CDR instruction to a data holder with whom the consumer may not have an existing relationship. In this situation, the data holder would not verify that the authentication has the consumer's consent in the same method that they would in data sharing applications or other Action Initiation where an existing relationship is held. The ability to establish the identity of the consumer, and the validity of the request is impeded.

The instance of Open Banking and Financial Services' practices may be deemed more complex than other sectors due to requirements such as Anti-Money Laundering/Counter-Terrorism Financing (AML/CTF) obligations. In this situation, the process of establishing this relationship would be significantly more complex than most other relationships

between the consumer and the service/product provider. It is, in part, for this reason, that Digital Identity solutions will play a role in enabling this in the future.

In addition to establishing a relationship, a data holder's ability to be assured that the customer has authorised the accredited party to request data or send Action Initiation instructions on their behalf. Depending on the complexity of the request/instruction, the sector that it occurs within and the type of customer, it is envisaged that differing assurance levels will need to be satisfied. For some data holders, the accredited party's mere assurance that the consumer initiated the request will suffice. For other use-cases, the data holder may need to engage directly with the customer to confirm the origin of the request and their authorisation of the third-party.

MANAGING A CUSTOMER RELATIONSHIP

The ability to correct and manage accurate customer records is critical to maintaining customer relationship. The inquiry considered that Action Initiation through CDR might be used for this purpose. CDR would allow a consumer to instruct a third-party to update these details on their behalf. Details could include personal information, product information and communication preferences.

"We believe that write access should extend to the ability to change customer identification details, as it is in the interest of consumers to find efficient and secure ways for them to update their details if required. This is also especially important if the CDR expands write access into more use cases, such as account opening and closing, or switching. Where write access is used to change identifying details, we would recommend that changing such details requires additional consent and authentication from the customer, for example two factor authentication." - TrueLayer

While there were submissions to the inquiry supporting Action Initiation for this purpose, other submissions were cautious, raising significant privacy risks associated with managing the customer relationship and records.

"[T]he expansion to write access may also raise new privacy and security implications, which will need to be appropriately addressed. In particular, as write access would allow third parties to modify a consumer's financial

information, it may increase the motivation for unauthorised actors to target an accredited data recipient's information system." – OAIC

The report raises the need for existing processes in confirming the accuracy and correctness of these details to be maintained. Given the sensitivity in updating personal information, data holders should take reasonable measures to mitigate perceived risks. The updating of passwords or mobile phone numbers are two examples that have been highlighted as posing significant risk and should not be updated, even with the consumer's consent. The information used for authentication purposes will vary across sectors and require explicit consideration as part of a sector assessment process.

CLOSING A CUSTOMER RELATIONSHIP

While Action Initiation could be deployed to close both a customer product and the closure of a customer relationship, there is a distinct difference between the two. The closing of a product may result in a customer relationship and associated details remaining in the system. The customer relationship's closure will require the customer to stop receiving all ongoing products, services, and communications provided by the service provider. The closing of the customer relationship via CDR should be no more complex than creating a customer relationship.

PRODUCT OR SERVICE PROCESS

APPLYING FOR A PRODUCT

The traditional application process requires the customer to complete an application form with personal details and existing service provider information. Action Initiation will allow an accredited party to complete this application form on behalf of the consumer and potentially acquire the majority of the information needed via the CDR process. In some cases, the consumer may still need to engage with the Data Holder to authorise or enter into contracts.

The steps involved in the application process may differ across various sectors, products and services. It is expected that the following steps may occur during a standard product application process:

• Quote – when specific details are provided to obtain the estimated price or benefit of a product

• Pre-approval – when initial details are provided ahead of a formal product application
• Validation – when certain details are checked for completeness before accepting an application
• Order – when the product specifications and quantity are confirmed or approved.

The CDR requires a data holder to receive authorisation to progress on the action before it can proceed. For this reason, establishing a new customer relationship may be difficult in the CDR framework due to the data holder, not knowing the customer. In this situation, a verification process will be conducted to grant assurance to the data holder of the customer's identity and consent.

MANAGING A PRODUCT

Differing products and services across various sectors may require a different management approach due to complexities and the transition to digital offerings. The inclusion of Action Initiation within the CDR for these purposes will allow easier and more convenient product management. It is deemed that digitally accessible products with varied functionality could be enabled through Action Initiation. Access would include online portals commonly utilised by banking products, payment initiation, and these would be considered primary functions.

CLOSING A PRODUCT

Given the digital nature of the CDR, the closing of a product via Action Initiation is one convenient use case noted. Despite the incentive to data holders to maintain the customer product, CDR details that a customer should send specific instructions and complete any additional requirements of the data holder to close the product via CDR. This process should be no more difficult to navigate than the opening of a product or service.

COMMUNICATIONS

NOTIFICATIONS

A request for accredited parties to send notifications via push notification or similar technologies may be convenient to customers. The ability for accredited parties to survey consumers' interests and request their consent to receive personalised offers that align with their needs may be enacted via notifications. These types of actions will be purely voluntary in nature.

COMPLAINTS

Another convenience action may be the ability of a customer to complain about a product or service. However, some behavioural barriers to lodging complaints with data holders to be passed through to the accredited parties exist. Complaint actions may also be voluntary.

ACCREDITATION

It is deemed that those seeking to participate in CDR Action Initiation should be accredited. As per current CDR requirements, Action Initiation accreditation should also be tiered based on perceived risk layering or potential harm. Whilst this process should mirror the existing accreditation process, additional criteria may be needed to ensure the different safeguards are enacted.

Recommendation 4.8 – Accreditation for action initiation

The accreditation regime should be extended to include tiered accreditation for action initiation, with those actions posing greater potential risk to the consumer requiring higher tiers of accreditation.

By enabling Action Initiation, it may be easier for accredited parties to offer innovative services to consumers and SME's. This action mustn't circumvent existing protections and licensing requirements. The granting of accreditation will not negate the party's need to obtain any licenses such as those granted by regulatory services. There may be additional requirements and regulations in parallel to the CDR that accredited parties need to be aware of and satisfy at all times.

An example of this would be the need for parties previously offering general financial advice may need to apply for an Australian Financial Services Licence (AFSL) due to the specificity and tailored nature of advice possible under the CDR. Another example would be those accredited parties considering initiating payments on behalf of a consumer and the potential for adherence to all AML/CTF laws.

Recommendation 4.9 – Accredited persons' interactions with other regulatory regimes

As sectors are designated for action initiation, the relevant sectoral regulators should examine whether additional guidance or education material should be provided to assist persons seeking accreditation understand how the services they propose to provide using the Consumer Data Right could be treated under existing regulatory regimes. Prospective accredited parties should be encouraged to consider these issues.

CONSENT – GIVEN TO THE ACCREDITED PERSON

CONSENTS TO INITIATE ACTIONS FOR SPECIFIC PURPOSES

As with data sharing through the CDR, action initiation must also be enabled via a consumer consent model with accredited parties receiving consumer's active, informed consent to initiate on their behalf. The consent must include specific actions to be defined and their explicit agreements regarding the purposes for which these actions may be initiated. Action initiation consents should be voluntary, express, informed, purpose-specific, time-limited and easily withdrawn.

Table 4.2 – Equivalent data sharing and access initiation terminology

	Accredited Person		Data Holder
	Access Consents	Usage Consents	Authorisations
Data Sharing	Consents to collect CDR data	Consents to use data collected	Authorisation to disclose CDR data
Action Initiation	Consent to initiate CDR actions	Consent to purpose for which instructions may be sent	Authorisation to accept CDR instruction

The CDR will require both access consent and user consent for a consumer to engage an accredited party. The separation of these consents will grant consumers greater control over how the accredited party may act by adding additional usage consents if needed and the ability to revoke specific usage consents without terminating the entire arrangement.

Box 4.2 – Consents given to and revoked from an accredited person

Sim has signed up to a mobile provider that allows her to vary her call minutes and data amounts on a month-to-month basis. This mobile provider has also decided to voluntarily provide this service through CDR API. Rather than coordinate this herself, Sim subscribes to 'Tele-phorget-about-it' (TFAI), an accredited person who offers to coordinate this service for her. Sim provides TFAI, with an ongoing access consent to receive relevant data from her mobile provider for 6 months and to alter her plan once a month over this period. Sim also authorises her mobile provider to accept such instructions. Sim initially provides TFAI with a usage consent that allows them to edit her data amount each month.

Being happy with this service, Sim provides another usage consent to allow TFAI to also send instructions to edit her monthly call minutes. When 'Tele-me-something-I-don't-know', a competitor accredited person, offers Sim an even more convenient service, she revokes all of her consents with TFAI and terminates her arrangement with them. This prevents TFAI from initiating any further actions on her behalf.

Recommendation 4.10 – Consent to send instruction and consent to initiate action

Accredited persons should be required to obtain access and usage consents to initiate actions for consumers. These consents should be voluntary, express, informed, specific as to purpose, time-limited and easily withdrawn.

Aligned to the consent process for data sharing through the CDR, Action Initiation's consent process should be subject to the Data Standards Body's Consumer Experience (CX) Standards and Guidelines to ensure genuine consent is produced conveniently.

Recommendation 4.11 – Consent processes and consumer experience

Action initiation consent processes should be subject to Consumer Experience Standards and Guidelines to ensure that processes produce genuine consent. The Data Standards Chair should consider additional safeguards which balance the need for security with consumer experience where appropriate.

ONGOING CONSENT ARRANGEMENTS

Consumers should provide enduring access and usage consents, allowing for Action Initiation to occur on their behalf for the duration of the consent. It is considered that ongoing consent for Action Initiation may pose significantly more risk than the ongoing consent for data sharing arrangement depending on the action's nature. In maintaining the current limitations of consent and authorisation durations, Action Initiation should include the maximum 12-month duration for consents and authorisations and the 90-day notification requirement.

Recommendation 4.12 – Ongoing consent arrangements

Consumers should be able to provide consents to accredited persons to initiate actions on their behalf on an ongoing basis, within the consent's time limit. Additional safeguards should also be considered for inclusion in the Rules.

RESTRICTIONS ON UNNECESSARY ACTIONS

To provide consumer protections, accredited parties should only request access consents that are directly relevant to the provision of a specific product or service for that customer. This practice mirrors the current data minimisation principles within the CDR rules.

Accredited parties cannot request data that is not specific to the consented action. CDR data that is received that is either not relevant or no longer relevant to the provision of a service must be deleted or de-identified.

Recommendation 4.13 – Restrictions on unnecessary actions

The Rules should restrict accredited persons to only being able to request access consents for actions that are relevant to the provision of a service.

AUTHENTICATION

Customer Authentication in the CDR exists to provide data holders and accredited persons with sufficient confidence to deal with an existing customer. Any consents or authorisations received will be given by persons entitled to act on the consumer's request.

CUSTOMER AUTHENTICATION STANDARDS FOR DATA HOLDER

The current authentication method utilised by financial services and Open Banking for data sharing is a one-time password (OTP) authentication. Data holders adopted this method as it met the consumer data-sharing system's safety and customer experience needs and is utilised by the majority of banks and service providers. As the CDR expands, authentication requirements of both data holders and accredited parties must adapt to the perceived increased risks that the misuse of new data sets and the functionality for consumers may present. The needs for proportionate authentication methods are explored further in Chapter 8.

Recommendation 4.14 – Authentication requirements by data holders

Data holders should be obliged to authenticate consumers prior to requesting action initiation authorisations.

Authentication requirements should be reviewed by the Data Standards Body to ensure they reflect the risks associated with action initiation.

AUTHENTICATION REQUIREMENTS BY ACCREDITED PERSONS

The requirement for an accredited party to assume the responsibility to act on behalf of a consumer and access and use the consumer's data can carry a greater risk of fraud or misuse

than traditional CDR uses. This increased risk can expose the consumer to greater harm and the accredited party to greater potential liability if things go awry.

In line with traditional banking practices or proving authentication before acting on a customer's wishes, Action Initiation will require accredited parties and data holders to have in place a safe and convenient means of authenticating the consumer before acting on their instructions.

These new authentication formats must be flexible and appropriate for the action requested and, above all else, mirror international standards for assurance levels and the rigour of consent authentication mechanisms.

Recommendation 4.15 – More explicit requirements for accredited persons to authenticate customers

The Consumer Data Right should include explicit requirements for accredited persons offering action initiation enabled services to authenticate customers in circumstances where there is an ongoing provision of service to that customer. These requirements should be based on international standards on authentication processes.

AUTHORISATION – GIVEN TO DATA HOLDER

AUTHORISATION TO ACCEPT INSTRUCTIONS

As previously stated, to ensure consumer protection and the security of the CDR, a consumer should be required to give the data holder authorisation to accept their instructions sent via a third party before they action that instruction. This process aligns with the consumer giving the data holder authorisation to disclose their data to a nominated accredited third party under the initial data-sharing rules. Both authorisations are withdrawable.

The authorisation to the data holder must outline the class of action but does not need to disclose the purpose for the request. This is in keeping with the initial data-sharing rules of a need to know the dataset requests for sharing, but not the purpose of the accredited third-party requesting the data. A requirement to disclose the purpose and the request is thought to impinge on the consumer's privacy potentially but can be supplied voluntarily.

AUTHORISATION FOR TAKING A PARTICULAR ACTION

With not all requests for data sharing and Action Initiation being judged equally, for some actions, the data holder should be required to request specific authorisations to progress the request. This specificity should depend on the nature of the action requested and additional factors, such as the potential impact on the consumer, existing data practices and the overall processes of the sector. One example provided is that of updating a consumer's personal information. It may be appropriate for the consumer to review and authorise that specific action before it is completed.

Whilst there may be actions that ongoing authorisation can accompany; specific actions may require specific authorisation given the potential risk factor and established practices. This authorisation would be required at the point of request for the action initiation. This will allow the data holder to confirm the consumer's understanding of the request and ensure its consent. This is not designed to be an opportunity for the data holder to influence the consumer's decision-making process.

Box 4.3 – Specificity of Authorisations

An action where it may be appropriate to require a specific authorisation, due to its sensitivity, could be the updating of a consumer's personal details. A number of submissions noted the sensitivity of enabling such information to be updated by a third party. For this example, it would also be appropriate for a consumer to need to authorise a specific change to this information, rather than generally allow this information to be changed. To enable the consumer to review the proposed change, this would require them to grant authorisation at the time the action initiation instruction was sent to the data holder. As noted previously, the sensitivity of particular personal information will vary depending on the sector in question, and so consideration should be given during the sectoral assessment to which information should be subject to this requirement.

Another action which could require a specific authorisation, due to its substantial impact on a consumer's relationship with their data holder, may be a request to open certain kinds of new products or close a consumer's product or relationship. A customer may need to provide a specific authorisation to accept applications for new products that could impose substantial obligations or risks on the consumer, such as a share trading account, but may be able to give ongoing authorisations to accept applications for lower risk products, such as savings accounts.

Recommendation 4.16 – Authorisation to take a specific action

Whether the taking of a particular action should require a specific authorisation to be given to a data holder should depend upon the nature of the action requested and other factors, such as the value of the transaction and existing practices and processes in the sector. These requirements should be enabled in the Rules and specified through the Standards.

FINE-GRAINED AUTHORISATION

When it is not necessary for a consumer to authorise action in itself, a consumer may still impose restrictions when authorising the data holder to accept their Action Initiation instructions. One example aligns with the current financial services practice of imposing a maximum limit on transaction amounts that accredited parties can initiate. This process, known as fine-grain authorisation, enables consumers to have greater protections and embed greater consumer practices within the CDR.

Recommendation 4.17 – Data holders to require explicit consumer authorisation to accept instructions

Data holders should only progress actions initiated by accredited persons when they have received the consumer's explicit authorisation to do so. The Data Standards Body should investigate the benefits of enabling fine-grained authorisation for specific action classes, with recommendations being driven by consumer experience and security considerations.

EXECUTION

OBLIGATIONS TO ACT ON INSTRUCTIONS RECEIVED THROUGH THE CONSUMER DATA RIGHT

A data holder should be obligated to act on a consumer's authorisation to initiate an action when received by an accredited party if the request is in line with the CDR parameters. The actions of the data holder should mirror that as if the request came directly from their customer.

This obligation is not exhaustive and will not be enforced if the data holder would not normally act due to legal limitations or suspicion of inappropriate actions. One example of this would be a potential or suspected breach of AML/CTF or in the instances of a potential fraud or abuse. This would include the prevention of physical and financial harm, and if it is reasonable, suspects that the request could threaten their information and

communication technology systems. This aligns with ordinary commercial and regulatory practices, and it is not desired that the CDR contradict these important practices.

Data holders are not permitted to discriminate against instructions sent through the CDR channel if they would not normally deny the action. Data holders should not obstruct the use of the CDR channels as;

• They will be obliged to invest in making the channel available for mandatory actions

• It will be possible for action initiation under the CDR to benefit consumers and data holders jointly, and

• The CDR will enable enhanced consumer experience, creating demand and support for the regime.

Data holders should make additional voluntary actions available to be initiated through the CDR in line with increased innovation and competition principles.

Recommendation 4.18 – Obligation to act

Data holders should be obliged to progress actions initiated by an accredited person for which the consumer has provided a valid authorisation to the same extent as they would otherwise be obliged to progress such an action were the request provided directly by the consumer through another channel. Data holders should not be able to discriminate based on the channel through which the instruction was received.

EXISTING DATA HOLDER LEGAL OBLIGATIONS AND COMMERCIAL IMPERATIVES

Within the CDR, data holders are still required to abide by all existing legal obligations placed on them by other regulatory regimes. The CDR is designed to offer an additional channel through which they can receive instructions from consumers, not replace the existing frameworks and obligations.

Given the need for data holders to maintain existing requirements and observe legal frameworks, measures will need to be built into the CDR environment to facilitate continuity. One measure explored is ensuring appropriate information is provided as part of the accredited party's instructions or enabling additional authentication processes (step-up authentication) to confirm the legitimacy of suspicious requests.

There are a variety of techniques currently employed by data holders when validating action requests. When Action Initiation by accredited parties is switched on, this may alter the methods in which these existing techniques are used. This may require data holders to exercise greater due diligence in processing these requests. The methods employed should be commensurate to the risks associated with the action that has been requested. Including additional information such as when and how the customer has directed the accredited party to take action may also help data holders perform a risk assessment process.

Recommendation 4.19 – Existing data holder obligations

Data holders should remain subject to any requirements imposed on them by other regulatory regimes and measures may need to be built into the Consumer Data Right to facilitate this. The Consumer Data Right should similarly contain provisions to assist data holders in managing commercial risks, such as fraud, when assessing actions initiated by accredited persons on the consumer's behalf. Data holders should remain capable of conducting reasonable step-up authentication measures to ensure the validity of any requests. The way in which these measures are conducted should be commensurate to the risk of the action being requested and not detract from the rights of access granted to accredited persons.

GENERAL LIABILITY AND RESPONSIBILITIES

The overarching Competitive and Consumer Act 2010 (CCA) protects data holders from liability when complying with data sharing requests within the CDR framework. The advent and inclusion of Action Initiation within the CDR framework and the related liabilities to participants may require further examination.

Currently, data holders are required to receive instructions to share data based on a principle-based approach that underpins the current provisions. These should be extended to Action Initiation instructions. This expansion will allow protections from potential liability as applied to the wider Action Initiation parameters, in line with the current data-sharing arrangements. If a data holder receives a request for Action Initiation from an accredited party, and they progress that request in a method consistent with the CDR requirements, the data holder should be protected from liability for doing so. If, however, a customer suffers a loss or breach for reasons other than compliance with the CDR, the CDR should not displace existing or ordinary rules for liability and loss allocation.

Any instruction carried out by a data holder in good faith will continue to be subject to all existing regulatory requirements and obligations, i.e., compliance with AML/CTF sanctions

screening obligations. Further discussion on how and when liability may apply to payment initiation is included in Chapter 5.

Recommendation 4.20 – General liability for action initiation

For action initiation, the general liability framework should extend the principle underpinning the operation of section 56GC of the *Competition and Consumer Act 2010*. This will protect data holders from liability when acting in compliance with the Consumer Data Right regime in response to an action initiation instruction for which they have received the consumer's authorisation to accept. For the avoidance of doubt, the data holder continues to be subject to any regulatory or legal obligations that would otherwise apply if the instruction had come directly from the customer.

DUTIES WHEN SENDING INSTRUCTIONS

When sending instructions and the request's purposes, express consent must be received from the customer to act on their behalf. In addition to receiving customer consent, accredited parties should also be subject to specific obligations in fulfilling those functions. The obligations, such as the accredited party being obliged to act efficiently, honestly and fairly, ask discussed further in Chapter 7.

The duty and obligation should not apply solely in carrying out Action Initiation requests but to the entirety of services provided to the customer. Establishing a new level of service provision within the CDR should not be required as this is the role of sectoral regulatory frameworks and consumer law. Existing legal obligations that prevent accredited parties from engaging in misleading, deceptive or unconscionable conduct/additional restrictions will continue to apply.

ACTION STATUS AND REVERSALS

There must be an avenue for customers to monitor Action Initiations by accredited parties and what safeguards exist to reverse actions they did not intend to authorise. This will allow consumers to track actions that are performed on their behalf. Accredited parties should be required to keep a record of all actions they have initiated. This record should then be made available to the customer. In line with Privacy Safeguard 10, accredited parties should be required to notify consumers when an Action is initiated.

The inquiry notes that not all actions can be reversed when initiated through the CDR. In the instance where a customer agrees to have an account closed with a specific data holder, it may not be possible to reopen that account. The ability to reverse specific actions should

be assessed through the sectoral assessment process. Inclusion within the consent and authorisation process should be made to help prevent consumers from accidentally enabling actions.

- The ability for fine-grain authorisations
- The ability for data holders to have step-up authorisations
- The requirements for some actions to be specifically authorised at the time of Action Initiation.

Recommendation 4.21 – Notification of action initiation

In designing the Consumer Data Right framework, processes should be included to enable consumers to be notified when an action is initiated on their behalf by an accredited person.

CLOSURE

CESSATION OF AGREEMENTS

Accredited parties should only initiate actions when they have current consent from the consumer to do so. Once that consent expires or is revoked, all initiations must cease, and any CDR data must be deleted or de-identified that they have received about the consumer.

Recommendation 4.22 – Cessation

Accredited persons should be required to cease acting on the consumer's behalf through the Consumer Data Right when they no longer have a valid consent. Accredited persons should be required to communicate this cessation to the data holders to whom they could previously send actions.

ADDITIONAL CONSIDERATIONS

RECORD KEEPING

Once engaged by a consumer, the accredited party should be required to maintain ongoing records. These records should record the action initiated and the consents received from the consumer. These records should be used during any dispute resolution process, by inspection of regulators, or by the consumer themselves in determining if the accredited party acted within the scope of their remit. These records should be kept beyond the duration of the consent given. Records retention should be in line with the CDR's read-

access requirements and should similarly apply where there is a legal obligation, i.e., income tax purposes.

Recommendation 4.23 – Record keeping

Accredited persons and data holders should be required to keep records of the actions that were initiated through the Consumer Data Right, as well as records of the consumer's consents and authorisations.

DASHBOARDS

As per the data sharing rules, Action Initiation should also require the maintaining of customer dashboards from which consumers can easily track and manage their Action Initiation consents and full authorisations. The ability to revoke or amend consent and authorisations should also be possible through these dashboards. This would include;

- Revoking specific usage consents
- Withdrawing access consents for specific actions, or
- Withdrawing their consent altogether.

PRIVACY SAFEGUARDS

Consideration must be given to the adequacy of current CDR protections provided through the privacy safeguards. This is further discussed in Chapter 7.

CONSUMER DATA RIGHT AND THE ABILITY FOR AN ACCREDITED PERSON TO CONTRACT ON BEHALF OF A CONSUMER

Communication within the CDR is two-fold. An accredited party can send instructions to a data holder, and this channel establishes that this communication is with the consumer's authority.

The CDR was not designed to fulfil all legal requirements of entering a contract to provide consumer services. Ensuring this compliance is the accredited party's duty that is seeking to offer services to the consumer. The ability to enter into a contract with a third-party to act on their behalf already exists, i.e., an investment manager may buy or sell shares for a consumer with their ongoing participation in the process.

It may be possible for a consumer to enter into a contract with an accredited party outside of the CDR parameters to initiate a request within the regime then. For example, Tim agrees

to ComparisonServiceX acting as his agent to enter into a new internet service provider (ISP) contract. This occurs outside the CDR. Tim then allows ComparisonServiceX to lodge product applications on his behalf through the CDR. He allows them to communicate as part of those applications that they are legally binding offers to enter into a service contract on his behalf. This occurs through the CDR channels. The prospective ISP may voluntarily choose to accept that assertion that ComparisonServiceX has the capacity to enter into contracts on Tim's behalf.

Working together with existing legal frameworks, the CDR should support various products and services, such as more streamlined or automated switching. Box 4.4 provides an example of this switching.

Box 4.4 – Streamlined switching versus automated switching

[The Inquiry notes that the EIC requirements in the Energy Sector may mean that the following examples are currently not possible, however such services may become possible in future.]

D'Arcy signed up to 'Energ-Easy', a fee-free energy switching service that is accredited to use the CDR. Energ-Easy promises to swap D'Arcy between energy accounts to save him money on his energy bill. D'Arcy gives Energ-Easy consent to access his energy data and send applications to energy companies to give him a better deal through the CDR. D'Arcy also gives his current energy provider authorisation to share his energy usage data with Energ-Easy.

Energ-Easy assesses D'Arcy's energy bill and finds him a cheaper deal. Energ-Easy presents D'Arcy with this information and then sends an application to the potential new provider. On receiving this application, the new provider approaches D'Arcy to verify his identity and confirm that he agrees to sign up to their deal. D'Arcy agrees and also gives consent and authorisation to Energ-Easy accessing energy data from this new provider, allowing them to continue providing their service.

D'Arcy later decides, on the recommendation of a friend, that he would rather try a different service. He goes to 'Best Energy Deals' (BED), a CDR accredited person who charges a yearly fee. BED promises to assess all market options through analyses of CDR product reference data and only recommend the best deal for their clients. Additionally, BED offers a legal arrangement where they can cancel and enter into contracts on their clients' behalf. This authority to contract on the customer's behalf is facilitated externally to their capacity as a CDR accredited person.

D'Arcy agrees to sign up with BED, and opts into their additional arrangement. He gives BED consent to receive energy usage data from his current provider and gives his current energy provider authorisation to share data with BED. BED then goes looking for deals. As BED has an arrangement that allows them to enter into new contracts on D'Arcy's behalf providers no longer approach D'Arcy directly to sign him up. Additionally, as BED is an accredited person, they can send applications via the CDR rather than via email as they would have otherwise have done. D'Arcy now only needs to periodically go to the BED portal to allow them to access energy data from his latest provider.

Report this - Published by

Jamie K Leach
Data Champion | Digital Finance | Technologist | MAICD Published • 5mo

This article explores Chapter 3 of Scott Farrell's Future Directions for the Consumer Data Right report. From data-empowered consumers to an economy-wide foundation, an integrated data ecosystem, towards international digital opportunities. What is the future direction of the Consumer Data Right in Australia?