

# INQUIRY INTO THE FUTURE DIRECTIONS FOR THE CONSUMER DATA RIGHT

RESPONSE TO ISSUES PAPER

May 2020

# CONTENTS

<b>Executive Summary</b>	<b>3</b>
<b>Write Access</b>	<b>5</b>
Introduction	5
Change data	6
Payments initiation	6
Account/product applications	6
Common issues of identification, authentication and authorisation	8
<b>Other Actions to aid the Digital Economy</b>	<b>11</b>
Digital signing and delivery	11

## EXECUTIVE SUMMARY

1. ANZ appreciates the opportunity to make a submission to the Inquiry into the Future Directions for the Consumer Data Right (**CDR**). ANZ has supported the introduction of the CDR and worked with the Treasury, the Australian Competition and Consumer Commission (**ACCC**) and Data61 towards providing 'read access' for our customers. We look forward to the commencement of consumer data sharing under the CDR.
2. At this stage, we do not have any further comments on enhanced functionality for CDR read access. We acknowledge the scale and significance of the Government's work currently underway as it continues to implement the CDR, including its plans to apply the CDR beyond the banking sector. We support the application of the CDR across the economy and believe steps in this direction are appropriate. We note that the 2017 *Review into Open Banking* recommended that a review should be conducted approximately 12 months after the CDR starts. We believe that such a review would provide useful information to the Government, industry participants and consumers about CDR's successes and opportunities for improvement. We would be happy to contribute to such a review.
3. The focus of this submission is on a potential next stage of the CDR once read access is appropriately established: 'write access'. Write access would allow consumers to not simply 'read' data held with a service provider but manipulate it, including by changing it, applying for products or initiating transactions. The key issues that arise in considering write access are identifying the possible use cases and then thinking about what issues need to be resolved to allow these use cases to be realised. We also think the Inquiry could usefully consider work already underway that may help to enable those use cases.
4. Looking at the elements necessary to realise possible write access uses cases would allow the Inquiry to consider what the next steps might be, including what aspects of the CDR's existing law, infrastructure and governance could usefully serve write access functionality. At this stage, we would note the following on these points. On governance, write access could involve additional considerations relative to read access given the functionality it offers may touch on existing regulatory mandates, including those of the Reserve Bank of Australia (payments) and the Australian Securities and Investments Commission (product applications). We would also be happy to consider issues such as what elements of the CDR's existing law and infrastructure can be repurposed or extended once the precise intended functionality of write access is identified.
5. At the moment, the key points we think the Inquiry should consider are:
  - The potential use cases within banking for write access, including payment initiation and product applications.
    - It could be useful to undertake research into consumer propensity to use these kinds of services. While consumer education may be necessary before these






services are understood and asked for, research today could help prioritise use cases and reforms in line with consumer demand.

- The potential requirements to enable write access, including adequate identification, authentication and authorisation to allow consumers to safely and securely manipulate their data held with one service provider via functionality offered by another service provider.
  - The existing initiatives that could interact with, or enable, write access use cases, such as the aim to give consumers the ability to initiate payments through the New Payments Platform (**NPP**).
6. We also note that establishing the CDR is one element of making Australia’s digital economy successful. Through COVID-19, the Government has taken steps to temporarily enable electronic corporate signing of contracts and deeds. We think these measures should be made permanent. Just as much as write access, these simple changes allow innovation in electronic commerce. There are similar opportunities available at the state level in respect of electronic execution of documents and conveyancing of property.
7. These points are set out in further detail below. We would welcome further discussions with the Inquiry as it progresses its thinking.

# WRITE ACCESS

## Introduction

8. The introduction of write access has the potential to provide consumers with a more seamless digital experience. It could enable a third party to facilitate an act on behalf of, or change or addition of data about, a customer, providing the customer has given a direction and their consent to the third party undertaking such an action. The Issues Paper has identified payment initiation as a specific example of a write access use case and other use cases relating to banking products could conceivably be pursued such as product applications.
9. In the banking sector, write access could conceivably consist of a broad range of use cases. The table below outlines some potential use cases in banking.

Banking use case	Example
 <b>Change data concerning an account owner</b>	Changing email address, mobile phone number, or address
 <b>Payment initiation</b>	From within a third party app, direct your bank to make a payment
 <b>A persistent authorisation to administer an account</b>	Customer establishes a direct debit for a new service from within the service provider's website
 <b>Apply for product/account</b>	A comparison service allows a customer to compare product offerings and then apply for the selected product from within the comparison service
 <b>Close product/account</b>	Customer rationalises accounts

10. Obviously, these functions are all possible from within banks' apps and internet banking today. Write access would allow these use cases to be executed from within third party applications, including those provided by other banks and non-bank account aggregation services. One area of research that the Inquiry could usefully explore is consumer appetite to access these functions from within third party applications. We appreciate that there may be an issue with consumers not yet understanding this type of functionality (and thus, there may be a low indicated desire to use it), but the research may uncover areas of interest that could direct the next steps.
11. The sections below consider some issues for resolution in the use cases of 'change data', 'payment initiation' and 'product application'. We then consider the issues of identification, authentication and consent that are common to the use cases.

## Change data

12. The use case of changing data could intersect with the privacy principles under the *Privacy Act 1988* (Cth). For example, when a customer unilaterally 'writes' new data onto a bank's (or other service provider's) dataset, the bank will have 'collected' the data without any steps of its own. Presumably, it will then need to notify the customer that this collection has occurred. Further, consideration could usefully be given to the situation where the customer writes incorrect information onto the bank's system and how Australian Privacy Principle 10 concerning the quality of personal information applies. These issues are not insoluble but will need thought.

## Payments initiation

13. Payments initiation could allow customers to direct their bank to make a payment from within the service provided by another entity. As the Inquiry is likely aware, there is existing work underway within the NPP to provide this functionality. We would welcome an approach towards payments initiation that is cognisant of these existing steps.
14. We would also note that payments initiation raises special issues with respect to fraud. Each party participating in the payments system will have its own fraud risk appetite, and each party should manage their own fraud risks. However, a clear liability regime for third party payments initiation will require further thought, with consideration given to its interactions with the ePayments Code and the Australian Financial Complaints Authority, and how consumers are properly informed about the possible risks. As new tools and solutions are developed in the payments system, the nature of fraud will also change. This will require further monitoring and consideration of the sufficiency of technical security controls.

## Account/product applications

15. Allowing customers to open accounts or apply for products from within third party applications could help consumer outcomes and competition. Conceivably, a third party term deposit comparison tool could also include a write access function where a consumer can open a term deposit from within the same application. Such an application could also allow consumers to close another account after its funds have been transferred to the new term deposit. The same could theoretically apply for credit products, such as credit cards and home loans.
16. Opening an account for a new customer would involve the identification and know-your-customer (**KYC**) steps required under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**AML/CTF Act**). Similarly, there are existing and upcoming 'suitability' requirements that need to be met before banks (and others) can provide products. For example, for consumer credit products, the responsible lending obligations of the *National Consumer Credit Protection Act 2009* (Cth) (**Credit Act**) apply and for retail financial and credit products, there are the design and distribution obligations (**DDO**) in

*Corporations Act 2001* (Cth) (**Corporations Act**) that will apply from October 2021. Both of these regulatory overlays will be relevant to account and product applications.

### AML/CTF Act

17. New to bank customers are required to have their identity verified before they can open an account. The AML/CTF Act requires banks to undertake KYC assessments. This requires collecting sufficient information about a customer, as well as verifying that customer's identification. This must be completed before a bank can establish a relationship with a customer or commence providing a regulated product or service. A number of issues emerge when considering the utility of the current AML/CTF regime in the digital economy.
18. We would anticipate that write access use cases of opening a new account or acquiring a new product would be expected to comply the AML/CTF Act. Such use cases could require both the third party provider and the product-owner bank to be compliant with KYC requirements. Issues that arise from such a scenario include:
  - Whether one party could rely on a KYC assertion from another party;
  - The type and extent of customer data shared between parties; and
  - An appropriate liability model.
19. A statutory review of the AML/CTF Act acknowledged that the ability of one party to rely on the identification undertaken by another party could deliver greater efficiencies to the current requirements under the Act.<sup>1</sup> The review recommended that an enhanced model should generally permit reporting entities to rely on identification procedures undertaken by a third party.
20. In October 2019 the Government introduced a bill to update provisions of the AML/CTF Act relating to reporting entities' customer due diligence obligations, including the circumstances under which they may rely on procedures undertaken by third parties. The bill requires reporting entities to form agreements with other entities before they can rely on that entity's procedures. The relying entity must also regularly assess the agreement or arrangement and terminate it if they do not have reasonable grounds to believe that each of the relevant requirements prescribed by the AML/CTF rules are being applied. Such arrangements will be subject to the individual risk and assurance approaches adopted by reporting entities, and the approaches taken by financial institutions to utilise these arrangements are likely to vary.

---

<sup>1</sup> Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations. Attorney-General's Department. 2016. <https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/report-on-the-statutory-review-of-the-anti-money-laundering.pdf>

21. The Inquiry may like to consider whether the bill will adequately facilitate write access. We would be happy to further consider this issue once precise use cases are defined.

### Suitability

22. An additional 'gate' that may apply before customers can acquire financial and credit products are various suitability obligations.
23. If the product is a credit facility, then the provider and any 'credit assistance provider' will need to comply with their responsible lending obligations under the Credit Act before the product is provided. Similarly, for all retail credit and financial products, the DDO will require issuers and distributors to take reasonable steps to align customers with target markets for products. These obligations will be relevant to both the actual issuer of the product (the entity whose systems are being 'written on') and the third party service provider who facilitates the 'writing' (ie the product application).
24. Any form of write access to facilitate product applications (for example, deposit account openings) will need to accommodate the steps that are required to meet these 'suitability' requirements. We would note that what steps are applied at the point of product application can vary from provider and product. For example, under the DDO, it is conceivable that different types of products would have different suitability 'gates' applied. This is because the law requires that 'reasonable steps' be taken. These will obviously vary with circumstances. As such, it may be difficult to design a universal product application mechanism that can be applied across products, issuers and distributors. The Inquiry may like to consider what aspects of product openings are capable of standardisation for the purposes of the write access mechanism.
25. Further, there may need to be contractual relations between the provider of the product and the provider of the 'write access' service. This is because, under the DDO for example, the product provider may need certain information from the write access service provider in order to meet their statutory obligations. As such, it may not be simply enough to allow API connectivity between parties; there may also need to contractual connectivity.

### Common issues of identification, authentication and authorisation

26. Common to all bank write access use cases will be the challenges of identification and verification of customers. Ensuring that the customer is who they say they are, and that the authority and consent to act on an account will be critical. There are three constituent functions that need to be addressed:
  - Identification (or Identity Verification) (as discussed above under 'AML/CTF Act')
  - Authentication
  - Authorisation (or Consent)



27. We note that market solutions to identification and verification solutions are emerging. International card schemes, industry bodies and Government enterprises are pursuing solutions, with varying degrees of functionality. The Inquiry may like to consider how these existing initiatives fit into any policy development. For example:
- There is currently work underway through the Australian Payments Network's (**AusPayNet**) TrustID framework to facilitate an industry approach to the sharing of personally identifiable information. The framework presents a series of rules and guidelines for organisations to adhere to in their design and build of products and services to ensure interoperability between different services.<sup>2</sup> This approach provides a competitively neutral ecosystem, which encourages continued innovation and customer choice.
  - The Digital Transformation Agency (**DTA**) has established a voluntary digital identity framework as an option for Australians to access Government services and to interact with the private sector. To date, the Government's 'myGovID' and Australia Post's accredited service provider 'Digital ID' interact as part of the Australian Government's Trusted Digital Identity Framework, with the DTA hopeful of an expansion of the ecosystem to include state and territory governments, local governments, banking and utilities.<sup>3</sup>

### Authentication

28. To reduce the chances of fraud and data loss, write access actions taken by existing customers of a financial institution should require a multifactor authentication process. Such an authentication process is known as 'strong customer authentication' (SCA).
29. SCA is an authentication process that validates the identity of the user of a payment service or transaction. SCA is a requirement of the European Union's (**EU**) second Payments System Directive (**PSD2**). It requires that payment service providers use SCA where a payer: accesses its payment account online; initiates an electronic payment transaction; or carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.<sup>4</sup> PSD2 defines SCA broadly as "an authentication based on the use of two or more elements categorised as knowledge (something only the user knows, such as a password), possession (something only the user possesses, such as a mobile phone) and inherence (something the user is, like the use of a fingerprint or voice recognition) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data."<sup>5</sup>

---

<sup>2</sup> See <https://www.auspaynet.com.au/insights/Trust-ID>

<sup>3</sup> See <https://www.dta.gov.au/our-projects/digital-identity/digital-identity-ecosystem>

<sup>4</sup> Second Payments System Directive, Article 97(1)

<sup>5</sup> Second Payments System Directive, Article 4(30)

30. SCA requirements should be specified using international standards to assist with international interoperability,<sup>6</sup> and the implementation of SCA should allow for innovation and competition to enable market solutions to be developed and refined. Different approaches to implementation are possible. For example:
- A third party provider could implement their own solution and provide the outcome to a bank
  - A third party provider could rely on a bank customer's existing authentication solution
  - A re-useable digital identity solution.
31. Whilst the risk of financial loss is greater in a banking context, use cases in other sectors could also be at risk of fraud or result in detrimental consequences for the customer. Further consideration should be given to the utility of authentication beyond banking sector use cases. Common SCA standards, based on international standards, would promote interoperability, including with the CDR.

#### **Authorisation and consents**

32. Ensuring a customer can grant and revoke their consents freely and clearly could give consumers confidence to participate in the CDR.
33. One way to promote strong consent mechanics that will promote interoperability between providers (eg the NPP and anything under the CDR) is a set of common consent definitions (ie a common consent taxonomy). It may be that identification and verification solutions could facilitate consent management over the longer term. Consideration should also be given to the architecture of consents storage, and whether write access arrangements should differ to current read access arrangements.
34. Further consideration will be required of how the CDR interacts where individuals are authorised to act on behalf of others (for example, a family member acting on behalf of a relative utilising a write access use case through the CDR). This should include consideration interactions between state and territory Power of Attorney arrangements and the CDR.

---

<sup>6</sup> International standards include NIST IAL, AAL, and FAL

## OTHER ACTIONS TO AID THE DIGITAL ECONOMY

35. The CDR is one part of Australia's digital economy. There are other actions that could be taken to help the digital economy to flourish. Some could be acted upon quickly, encouraging growth in Australia's digital economy in the short to medium term.
36. For example, there may be utility in assessing Australia's privacy regime, particularly the intersection between the privacy protections under the CDR and the general privacy protections; a greater exposure of state, territory and Commonwealth government data in the economy; and facilitating digital signing and delivery. A review of the operations of current legislation in the digital economy may reveal other simple reforms that would benefit the digital economy.
37. ANZ believes that if these actions were prioritised, they would help drive the expansion of the digital economy in the near term. Undertaking these reforms prior to the implementation of an expanded CDR would see benefits for both the digital and traditional economies, and ensure today's existing legislation is ready for the future development of the CDR.

### Digital signing and delivery

38. Facilitating permanent reforms related to the electronic signing and delivery of documents and deeds under the Credit Act and the Corporations Act would benefit both financial institutions and consumers. Whilst such action would be of benefit to the digital economy, the recent COVID-19 pandemic has also demonstrated the benefit of such reforms to the traditional economy.

#### Digital Signing – Deeds

39. At general law, there remains a requirement that deeds must be written on 'paper, parchment or vellum'. A permanent amendment to section 127 of the Corporations Act could provide that a deed created by a corporation may be in electronic form and signed electronically.
40. The utility of the change to the Corporations Act has recently been demonstrated. As part of the Australian Government's response to the COVID-19 pandemic, the Treasurer announced on 5 May 2020 that the Government would allow company officers to sign a document (including deeds) electronically under the Corporations Act. The Treasurer made the change under the COVID-19 pandemic temporary instrument-making inserted into the Corporations Act. ANZ believes a permanent change to the Corporations Act would be of benefit to both the digital and traditional economies.
41. However, deeds signed by individuals, partnerships and other entities that are not corporations are governed by state and territory laws. Further, deeds signed by individuals (including attorneys under a power of attorney arrangement) need to be witnessed. The parliaments of New South Wales, Victoria, Queensland and the Australian Capital Territory recently passed legislation permitting the electronic execution of these types of documents

in response to issues encountered during the COVID-19 pandemic, however these changes are temporary only. States and territories would need to make permanent changes to land titles and electronic transactions legislation to provide the legal certainty required.

### Digital Delivery – Credit Act

42. Under the Credit Act credit providers are constrained from delivering documents required under the Act by electronic means. These documents include: credit contracts; notices of changes to existing credit contracts; credit guidelines; written unsuitability assessments; notices required by hardship provisions of the National Credit Code (**NCC**); and account statements.
43. The ASIC Corporations (Removing Barriers to Electronic Disclosure) Instrument 2015/647 granted relief to encourage and facilitate the use of digital disclosure for financial products. However, an equivalent position has not been reached for consumer credit facilities.
44. To remove these inconsistencies and facilitate digital disclosure, Part 3 of the Electronic Transactions Regulations could be amended to mirror the position under Instrument 2015/647. The Instrument permits a 'publish and notify' approach to electronic delivery of documents. Under this approach, disclosure is permitted digitally without consent, provided the customer is given 7 days to opt out of this method, and the providing entity notifies the client that the disclosure is available and how to access it.
45. Alternatively, the National Consumer Credit Protection Regulations 2010 could be amended. Such an amendment could, in addition introducing a publish and notify approach, permit digital delivery of required documents with consent. This would:
  - Remove the need to obtain prior written consent to electronic disclosures
  - Allow disclosures to be delivered digitally in full to an electronic address (e.g. an email address) if the customer has provided an electronic address as part of their contact details
  - Allow disclosures to be delivered using any digital method if the client has agreed, either orally or in writing, to this.
46. To best facilitate the delivery of documents by electronic means, these amendments could apply to all contracts, notices, statements of account and disclosure documents required to be provided to a consumer under the Credit Act.

### Digital Delivery – National Credit Code

47. Under the NCC an obligation is imposed on customers to provide to a credit provider their address in writing, potentially resulting in unintended consequences for the customer.
48. Section 195(1) of the NCC provides that the appropriate address to send a person a notice of other document required by the Code is an address nominated in *writing* by the person, or in the absence of such a nomination, the last known address of the person. Where a

person has nominated an address, section 195(2) provides that the person may change or cancel that address by notice in writing.

49. The effect of these provisions appears to be that where a customer changes their address and does not provide the updated details in writing, the credit provider would not be able to send documentation to the customer's new address. Section 195 requires a credit provider must send notices and other documents to the last address nominated in writing.

**ENDS**