IMPLICATIONS OF THE CONSUMER DATA RIGHT FRAMEWORK FOR TRUSTED ADVISERS

DR ANTON N DIDENKO

SENIOR LECTURER, UNIVERSITY OF NEW SOUTH WALES FACULTY OF LAW & JUSTICE

CPA AUSTRALIA

ISBN 978-1-922690-07-4

TABLE OF CONTENTS

AUTHOR

Dr Anton N Didenko

Anton is a Senior Lecturer at the Faculty of Law and Justice of the University of New South Wales (UNSW Sydney) specialising in banking and finance law, with a focus on FinTech, RegTech and cyber security.

Anton has over 10 years of experience in financial regulation. Prior to joining UNSW Sydney, he worked as head of legal support of international operations in major commercial banks in Russia, as a senior associate at a law firm in London and as a research fellow at the British Institute of International and Comparative Law.

He also specialises in the area of secured transactions law and transnational commercial law: he is the author of a monograph on the documentary history of the Cape Town Convention on International Interests in Mobile Equipment (Hart, 2021) and the general editor of the Cape Town Convention Journal. Anton holds several law degrees from Russia and the United Kingdom, including a DPhil (Doctor of Philosophy) from the University of Oxford.

At the time of writing, Anton's research at UNSW Sydney was funded by the Australian Government through the Australian Research Council (project FL200100007 'The Financial Data Revolution: Seizing the Benefits, Controlling the Risks').

1. INTRODUCTION

The recent introduction of the Consumer Data Right (CDR) in Australia represents a major change to how consumer data is transferred in designated sectors of the economy – starting with banking. The CDR is expected to promote competition by making it more convenient for customers to compare and select products and encourage innovation by enabling businesses to offer new products and services that are better adjusted to customers' needs.

The recent public inquiries and consultations have highlighted a number of issues associated with the rollout of the CDR, such as implementation and rollout of open banking; accreditation and access to CDR data; alternative means of accessing customer data; extending CDR to sectors beyond banking and; CDR governance.[1]

While much of the debate around the CDR has largely focused on 'accredited data recipients' (as defined in Part IVD of the *Competition and Consumer Act 2010* (Cth)), the impact of the CDR regime on professional advisers such as accountants or financial consultants and their customers has not been adequately analysed.

On the one hand, prior to the recent revisions to the CDR framework, non-accredited entities did not have access to a consumer's CDR data. On the other hand, professional advisers are often already subject to special requirements and standards existing outside the CDR framework. The desirability and practicality of separate accreditation for such advisers was challenged in the 2020 report on the future directions for the CDR.[2]

In response, a new revision of CDR rules was adopted in September 2021 to allow professional advisers to access CDR data.[3] This report analyses the implications of the CDR framework for the handling of CDR data by such advisers and their customers.

[1] See The Senate, 'Select Committee on Financial Technology and Regulatory Technology: Interim Report' (September 2020), chapter 5 <https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/024366/toc_pdf/SelectCommitteeonFinancialTechnologyandRegulatoryTechnology.pdf;fileType=application%2Fpdf>.

[2] 'Future Directions for the Consumer Data Right: Consumers; Choice; Convenience; Confidence (Report, October 2020) <https://treasury.gov.au/sites/default/files/2021-02/cdrinquiry-final.pdf>.

[3] *See Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021.*

2. OVERVIEW OF THE CDR FRAMEWORK

The roots of the CDR can be traced back to the Productivity Commission's report 'Data Availability and Use' published in May 2017, which recommended the creation of a new 'Comprehensive Right' to the use of digital data by consumers.[4] Rather than being a duplicate of privacy law provisions, this new Right was 'meant to lift up the opportunity for consumers and offer a genuine two-way street to support their continuing willingness to supply a crucial input to business, research and public policy – namely, their data'.[5]

Two important interlinked features of this originally proposed Comprehensive Right are worth noting: the perceived economic value of data and consumer centrality. On the one hand, the report recognised that vast amounts of data and data analytics capabilities can enable data holders 'to apply data-derived insights to deliver better and new products for consumers, and to improve their own competitiveness' – as a result of non-rivalrous nature of consumers' data, which 'can be reused over and over again without diminishing its value'.[6]

On the other hand, it sought to 'enable [consumers] to have more influence in how value is created and extracted from their data'.[7]

According to the initial proposal, the Comprehensive Right would comprise five separate rights to consumer data:

1. a right to access a copy of consumer data;
2. a right to request edits or corrections of consumer data for accuracy;
3. a right to direct holders of consumer data to copy it (in machine-readable form) either to the consumer, or to a nominated third party (the 'transfer right');
4. a right to be informed about the trade of any element of consumer data to third parties; and
5. a right to be advised of disclosures of consumer data to third parties.[8]

[4]Productivity Commission Inquiry Report, Data Availability and Use (March 2017) 15 <https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf>.
[5]Ibid (emphasis in the original).
[6]Ibid 192.
[7] Ibid.
[8]Ibid 197.

For the purposes of this report, two aspects of this proposed structure are important. First, the so-called 'transfer right' was expected to cover instances of sharing a copy of consumer data to 'another identified service provider or *advisory service*'.[9] Second, the report identified the possibility of sharing consumer data *across different industries* – and the resulting need to deal with inconsistencies in data formats and standards. In the latter case, it was argued that 'the recipient industry would need to adapt to the standard of the *original* data holder'.[10]

In November 2017, the Government announced the development of the CDR in Australia, to be launched initially in the banking sector.[11] The design of the CDR regulatory framework was largely inspired by the open banking report by Scott Farrell.[12] The original regulatory framework included the *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth), the *Competition and Consumer (Consumer Data Right) Rules 2020* ('CDR Rules') issued by the Australian Competition and Consumer Commission ('ACCC') and the standards made by the Data Standards Chair, who is assisted by the Data Standards Body.[13] Application of the CDR framework to authorised deposit-taking institutions (ADIs) was extended by the *Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019*, which specified classes of information falling within the CDR framework.[14]

In general terms, the operation of the CDR Rules involves interaction of a consumer with two CDR participants:[15] a 'data holder' and an 'accredited data recipient' (ADR).[16] Data holders include all ADIs authorised to conduct banking business in Australia under section 9 (3) of the *Banking Act 1959* (Cth).[17] An ADR is an 'accredited person' (i.e. a person accredited by the Data Recipient Accreditor)[18] who has received CDR data under the CDR Rules.[19]

Disclosure of CDR data occurs pursuant to a 'consumer data request', which can be made by a CDR consumer directly (for a disclosure to such consumer), or by an accredited person on behalf of a CDR consumer (for a disclosure to the accredited person). A consumer data request is addressed to a data holder or, in the case of requests made by accredited persons, also to an ADR. Prior to making the requested disclosure, the relevant party obtains authorisation from the consumer. The disclosure itself is made using the prescribed data transmission channels and in accordance with the relevant data standards. Upon disclosure of CDR data to an accredited person, the recipient of CDR data becomes an ADR.

[9]Ibid 211 (emphasis added).

[10]Ibid 212 (emphasis added).

[11]'Consumer Data Right (CDR)', Australian Competition & Consumer Commission (Web Page) <https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0>.

[12]Australian Treasury, 'Review into Open Banking: Giving Customers Choice, Convenience and Confidence' (December 2017).

[13]See ss 56FH, 56FK of the Competition and Consumer Act 2010 (Cth).

[14]*Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019.*

[15]'CDR participant' is a term defined in section 56AL of the Competition and Consumer Act 2010 (Cth).

[16]As defined in sections 56AJ and 56AK of the Competition and Consumer Act 2010 (Cth).

[17]The CDR initially commenced in July 2020 for the four major banks (known as 'initial data holders' in the CDR Rules) and any ADIs that opted to participate voluntarily, but was subsequently extended to cover non-major ADIs, in a phased rollout process.

[18]See section 56CA of the *Competition and Consumer Act 2010* (Cth). The ACCC is the Data Recipient Accreditor in the absence of a contrary designation: see section 56CG of the *Competition and Consumer Act 2010* (Cth).

[19]See s 56AK of the of the *Competition and Consumer Act 2010* (Cth).

3. CDR ACCREDITATION

In its CDR explanatory guide issued in May 2018, the Treasury envisaged a multi-tier accreditation framework offering a certain degree of flexibility for CDR participants:

'It is proposed that there will be *different levels of accreditation* to reflect the different risks associated with different data sets and data uses. For example, a third party which intends to hold banking transaction data sets for extended periods is likely to have to meet a higher level of accreditation.'[20]

The legislative framework reflected this view in section 56BH of the *Competition and Consumer Act 2010* (Cth), according to which the CDR Rules may include 'rules providing that accreditations may be granted at *different levels corresponding to different risks*' – whereby the different risks may be associated with:

- specified classes of CDR data,
- specified classes of activities or
- specified classes of applicants for accreditation.[21]

Although the amendments commencing in February 2022 envisage a new level of accreditation,[22] at the time of writing the CDR Rules provided for a single 'unrestricted' level of accreditation.[23] In practice, this translated into only 23 accredited providers in operation, according to the published data.

4. IMPLICATIONS OF THE CURRENT ACCREDITATION REGIME FOR PROFESSIONAL ADVISERS

The earlier discussion in section two suggests that the possibility of transferring CDR data to providers of advisory services to consumers was considered from the start. Yet, the lack of flexibility in the original regulatory framework created a conundrum for an entire group of *professionals* specialising in the provision of advisory services, such as qualified accountants, lawyers or tax agents. On the one hand, under the original CDR framework all non-accredited entities did not have access to CDR data.

On the other hand, many professional advisers are already subject to professional requirements and standards – regardless of their accreditation status within the CDR framework.

While a number of measures could be envisaged to deal with this conundrum, the discussion about possible solutions has predominantly focused on two alternatives:

- a separate (potentially light-touch) accreditation pathway for certain groups of regulated professionals, or
- an alternative (non-accreditation) pathway to CDR data for such professionals.

Let us now analyse these alternative approaches in sections five and six, respectively.

[20] Commonwealth Treasury, 'Consumer Data Right' (Explanatory Guide, 9 May 2018) 8 <https://treasury.gov.au/sites/default/files/2019-03/t286983_consumer-data-right-booklet.pdf> (emphasis added).

[21] *Competition and Consumer Act 2010* (Cth), s 56BH(1)(d) (emphasis added).

[22] See section five below. See also *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021, Schedule 1.*

[23] CDR Rules r 5.2.

5. TIERED ACCREDITATION PATHWAY TO CDR DATA

The absence of flexibility across data recipients was identified as problematic in submissions to a number of public consultations, citing reasons such as disproportionate authorisation requirements (e.g. in the context of mortgage brokers, who usually operate as 'a small business or sole operator' and therefore are 'unlikely to be able to support the technology platforms and software services required to manage CDR data as specified in the CDR Rules').[25] To address this issue, some professional advisers expressed a strong preference for accreditation 'through a separate tier of accreditation'.[26]

Different criteria have been suggested for defining the lower tiers of accreditation. For example, Deloitte proposed tiering based on

- the attributes of CDR data being shared (where basic customer information is eligible to lower tier ADRs),
- the sensitivity of shared CDR data (where higher accreditation tiers are needed for more sensitive data, such as data from minors) and
- standardised and/or approved uses of CDR data (where 'lower tier participants may be eligible to receive CDR data for purposes such as proof of income / expenditure or to summarise monthly expenditure by merchant type').[27] The Financial Planning Association of Australia proposed revisions to the accreditation format taking into account the different sizes of professional advisers: 'Privacy and information security requirements should be designed in a manner that allows sole practitioners, not just large financial services firms, to become accredited.'[28]

It should be noted, however, that some industry participants expressed concerns about the potential dilution of consumer protections in a multi-tier CDR setting. For example, Westpac adopted a no-compromise stance in relation to some aspects of tiered accreditation framework, such as security and consent:

'We agree that different accreditation obligations may be useful to distinguish between the different risk profiles associated with different activities, however there should be no lesser obligations in terms of security, privacy or consent.'[29]

Despite these reservations, the final report of the Inquiry into Future Directions for the Consumer Data Right ('Future Directions Report') prepared by Scott Farrell proposed the establishment of lower tiers of accreditation 'where the risk of harm and potential levels of harm that given data sets or activities could cause is lower than others',[30] as reflected in Recommendations 6.12 and 6.13:

[25]Mortgage & Finance Association of Australia, 'Consumer Data Right – Inquiry into Future Directions for the Consumer Data Right' (18 May 2020) 3 <https://treasury.gov.au/sites/default/files/2020-07/mortgage-finance-association.pdf>.

[26]See, eg, Mortgage & Finance Association of Australia, 'Consumer Data Right – Inquiry into Future Directions for the Consumer Data Right' (18 May 2020) 1 <https://treasury.gov.au/sites/default/files/2020-07/mortgage-finance-association.pdf>.

[27]Deloitte, 'Shaping the Future: Consumer Data Right; Deloitte Submission on the Consumer Data Right Rules Framework' (12 October 2018) 9-10 <https://www.accc.gov.au/system/files/CDR%20-%20Rules%20-%20Submission%20to%20framework%20-%20Deloitte%20-%20PUBLIC%20VERSION.pdf>.

[28]Financial Planning Association of Australia, 'Inquiry into Future Directions for the Consumer Data Right' (21 May 2020) 1 <https://treasury.gov.au/sites/default/files/2020-07/fpa-australia.pdf>.

[29]Westpac, 'Re: Inquiry into the Future Directions for the Consumer Data Right' (25 May 2020) 8 <https://treasury.gov.au/sites/default/files/2020-07/Westpac-2020.pdf> (emphasis added).

[30]'Future Directions for the Consumer Data Right: Consumers; Choice; Convenience; Confidence (Report, October 2020) 118 <https://treasury.gov.au/sites/default/files/2021-02/cdrinquiry-final.pdf>.

'Recommendation 6.12 – Accreditation criteria. The accreditation criteria should not create an unnecessary barrier to entry by imposing prohibitive costs or otherwise discouraging suitable parties from participating in the Consumer Data Right. A tiered, risk-based accreditation model should be used to minimise costs for prospective participants.'[31]

'Recommendation 6.13 – Tiering of accreditation.

Regulation of the Consumer Data Right should be able to allow tiering of accreditation requirements based on factors, including the risks associated with the accessible CDR data and the activities that could be undertaken with it.'[32]

The changes to the CDR Rules adopted in September 2021 (and commencing in February 2022) envisage a new, 'sponsored' level of accreditation (bringing the total number of CDR accreditation tiers to two). This permits a person to seek accreditation at a new 'sponsored' level if they have arrangements with an accredited person with an unrestricted level of accreditation (a 'sponsor'). In turn, the sponsor is required to have in place a 'third-party management framework' – to ensure that the sponsored person (an 'affiliate') maintains appropriate information security capabilities – and has a duty to 'take reasonable steps to ensure that the affiliate … complies with its obligations' as an accredited person and 'provide the [affiliate] with any appropriate assistance or training in technical and compliance matters').[33]

While useful for some industry actors, this solution is hardly relevant for professional advisers. And so, we turn to the second option: an alternative (non-accreditation) pathway to CDR data for professional advisers.

[31]MIbid 119.

[32]Ibid 121.

[33]*Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021* para 34.

6. NON-ACCREDITATION PATHWAY TO CDR DATA

Interestingly, some of the submissions to the public consultations on the expansion of access to the CDR framework strongly opposed the idea of creating alternative pathways to CDR data for non-accredited entities. For example, the Australian Privacy Foundation argued:

> 'People need to be sure that when they use the CDR … all participants are fully accredited and a member of an external dispute resolution scheme (EDR). Any inclusion of non-accredited parties presents a risk for consumers using the system.'[34]

Equally, the Financial Rights Legal Centre firmly rejected the idea of sharing CDR data with non-accredited persons, including professional advisers:

> 'All handlers of CDR data – from banks and credit unions (data holders), FinTechs and software developers (data participants) to *accountants, financial advisors, mortgage brokers, insurance brokers,* landlords or any other entity with even a remote interest in gaining access to sensitive, personal financial data – should be accredited.'[35]

Some commentators, while generally disagreeing with the idea of sharing CDR data with non-accredited entities, called for additional protections to be put in place in case the CDR Rules are nonetheless amended to allow such sharing. For example, Cuscal proposed a number of 'strict requirements' to address the resulting risks:

- reliance on an *intermediary* 'to ensure consent, security, insurance and dispute obligations are met',
- reliance on o*utsourced service providers*,
- industry *licences* or
- restricted *use cases* and restrictions on the *types of data* shared with non-accredited parties (e.g. with no or limited access to raw data).[36] The Consumer Policy Research Centre referred to the sharing of CDR data with non-accredited entities as a 'back-door' that is not recommended 'in the absence of economy-wide data protection reform', but nonetheless suggested that – if accreditation is unreasonable – certain classes of potential data recipients should 'be provided an exemption framework to use the CDR data only for a *specific purpose* with appropriate privacy protections put in place'.[37]

The dilemma surrounding professional advisers was noted in the Future Directions Report, which argued against *any* separate form of accreditation for trusted professionals:

> 'Requiring entities, who are subject to existing regulations and accountable for the use of consumer's data under those regulations, to obtain *accreditation* (even at a lower tier) would be *disproportionate*.'[38]

Around the same time, the ACCC proposed corresponding revisions to the CDR Rules to incorporate disclosure to non-accredited advisers. The ACCC acknowledged the potential risks but nonetheless sought to focus on expanding participation in the CDR framework:

> 'While recognising these risks, we consider it is important to consult on measures that will *encourage participation* in the CDR and benefits for consumers, including through expanding the range of service offerings that CDR participants can provide.'[39]

[34]Australian Privacy Foundation, Submission to the Issues Paper: Inquiry into the Future Directions of the Consumer Data Right (6 May 2020) 2 <https://treasury.gov.au/sites/default/files/2020-07/australian-privacy-foundation.pdf> (emphasis added).

[35]Financial Rights Legal Centre, 'Submission by the Financial Rights Legal Centre: Inquiry into Future Directions for the Consumer Data Right (May 2020) 45 <https://treasury.gov.au/sites/default/files/2020-07/c2020-62639-financialrightslegalcentre.pdf> (emphasis added). See also Financial Rights Legal Centre, 'Submission by the Financial Rights Legal Centre: CDR Rules Expansion Amendments Consultation Paper (October 2020) 29 <https://financialrights.org.au/wp-content/uploads/2020/10/201029_ACCCCDRRulesexpansion_Sub_FINAL-1.pdf>.

[36]Cuscal, Inquiry into Future Directions for the Consumer Data Right (20 May 2020) 3 <https://treasury.gov.au/sites/default/files/2020-07/cuscal-limited.pdf>.

[37]Consumer Policy Research Centre, 'Submission by Consumer Policy Research Centre to ACCC-Consumer Data Right Rules Framework' (12 October 2018) 3-4 <https://www.accc.gov.au/system/files/CDR%20-%20Rules%20-%20Submission%20to%20framework%20-%20Consumer%20Policy%20Research%20Centre%20-%20PUBLIC%20VERSION.pdf>.

[38]'Future Directions for the Consumer Data Right: Consumers; Choice; Convenience; Confidence (Report, October 2020) 111 <https://treasury.gov.au/sites/default/files/2021-02/cdrinquiry-final.pdf> (emphasis added).

[39]Australian Government, 'CDR Rules Expansion Amendments: Consultation Paper' (September 2020) 28 <https://www.accc.gov.au/system/files/CDR%20rules%20expansion%20amendments%20-%20consultation%20paper%20-%2030%20September%202020.pdf> (emphasis added).

The Treasury supported this view in its July 2021 consultation on version three of the CDR Rules,[40] which was subsequently adopted (with several minor revisions) in September 2021 as *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021* ('2021 CDR Amendment Rules'). More specifically, Schedule 3 ('Amendments Relating to Trusted Advisers and Insights') of the 2021 CDR Amendment Rules introduced a new category of 'trusted advisers' and envisaged disclosure of CDR data to trusted advisers without requiring them to obtain any form of CDR accreditation.

The 'trusted advisers', according to the revised CDR Rules, include:

- **qualified accountants** within the meaning of the *Corporations Act 2001 (Cth)*;
- persons who are admitted to the **legal profession** (however described) and hold a current practising certificate under a law of a State or Territory that regulates the legal profession;
- registered **tax agents, BAS agents** and **tax (financial) advisers** within the meaning of the *Tax Agent Services Act 2009 (Cth)*;
- **financial counselling agencies** within the meaning of the *ASIC Corporations (Financial Counselling Agencies) Instrument 2017/792;*
- 'relevant providers' within the meaning of the Corporations Act 2001 (Cth) (i.e. individuals authorised to provide **personal advice to retail clients** in relation to relevant financial products), with the exception of 'provisional relevant providers' defined in section 910A and 'limited-service time-sharing advisers' defined in section 910A;[41] and
- **mortgage brokers** within the meaning of the *National Consumer Credit Protection Act 2009* (Cth).[42]

Unlike the earlier proposals made by the ACCC in 2020 (which, in addition to expressly listed classes of trusted advisers, also included the residual option of 'a class approved by the ACCC'),[43] the revisions set out a closed list of eligible classes of trusted advisers, and the descriptions of those eligible classes became more specific. In response to the relevant public consultation, CPA Australia et al. have called for an expansion of the list of trusted advisers to include 'bookkeepers who are members of a professional association'.[44]

[40]'Consumer Data Right Rules Amendments (Version 3)', Australian Treasury (Web Page) <https://treasury.gov.au/consultation/c2021-187223>.

[41]The latter two groups of 'relevant providers' have been excluded 'on the basis that the *Corporations Act 2001* does not allow them to refer to themselves as "financial advisers"'. See Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021: Explanatory Statement 19.

[42]2021 CDR Amendment Rules, Schedule 3, para 5; CDR Rules r 1.10C(2).

[43]Competition and Consumer (Consumer Data Right) Rules 2020: Consultation Draft (2020) 16 <https://www.accc.gov.au/system/files/CDR%20Rules%20%28Exposure%20Draft%20for%203rd%20amendment%29%20-%2030%20September%202020.pdf>.

[44]CPA Australia, Chartered Accountants Australia and New Zealand, the Institute of Public Accountants and the Institute of Certified Bookkeepers, 'RE: Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021 (30 July 2021) 3 <https://www.cpaaustralia.com.au/-/media/project/cpa/corporate/documents/policy-and-advocacy/consultations-and-submissions/cross-policy/2021/joint-submission-amendments-to-cdr-rules.pdf?rev=7f15cbed9ffa4a1a88b2e708927aab09&download=true>.

7. CONSUMER PROTECTION MECHANISMS IN THE NEW FRAMEWORK FOR TRUSTED ADVISERS

The 2021 CDR Amendment Rules envisage that the sharing of CDR data with trusted advisers is possible only with a consumer's consent – and for this purpose introduce a new category of 'disclosure consent': *TA disclosure consent*.[45] To prevent conflicts of interest, accredited persons are prohibited to make supply of goods or services requested by the CDR consumer conditional on:

- the nomination of a trusted adviser; or
- the nomination of a particular person as a trusted adviser; or
- the giving of a TA disclosure consent.[46]

Despite the above provisions, the main consumer protection tool enshrined in the CDR framework – CDR accreditation – does not apply to trusted advisers (who are not required to become 'accredited persons' for the purposes of obtaining CDR data and therefore need not be recorded on the Register of Accredited Persons maintained under Division 5.3 of the CDR Rules). Instead, the 2021 CDR Amendment Rules envisage several additional consumer protection measures:

- *Professional status verification*: ADRs are encouraged to take 'reasonable steps to confirm that a person nominated as a trusted adviser was, and remains, a member of a class' of trusted advisers.[47]
- *Consumer dashboard maintenance*: An ADR must, as soon as practicable after disclosing CDR data to a trusted adviser, update each consumer dashboard that relates to the disclosure request, indicating what CDR data was disclosed, when the CDR data was disclosed and the trusted adviser to whom CDR data was disclosed.[48]
- *Bespoke CX data standards:* Disclosure of CDR data to trusted advisers is subject to bespoke consumer experience data standards[49] (also referred to as 'CX standards') (while the previous version of the CDR Rules only envisaged consumer experience data standards for disclosure to *accredited persons*). CX standards are made by the Data Standards Chair and include:
  - data language standards,
  - accessibility standards,
  - consent standards,
  - authentication standards,
  - authorisation standards,
  - amending authorisation standards and
  - withdrawal standards.[50]

At the time of writing, the CX data standards for trusted advisers were not publicly available. Nonetheless, it is expected that the new standards will ensure that the consumer is provided with crucial information concerning the implications of sharing the CDR data with trusted advisers, such as 'information that the use of the data by the recipient will not be covered by the CDR regime and the recipient may not have obligations under the Privacy Act 1988'.[51] Another underlying issue is the need to ensure consistency of the CX standards with any regulatory requirements applicable to trusted advisers, such as the ATO.[52]

- *CDR information security controls:* The sharing of CDR data with trusted advisers is covered by the information security controls in Schedule two of the CDR Rules.[53]

[45] 2021 CDR Amendment Rules, Schedule 3, paras 2-3; CDR Rules r 1.10A(1)(c)(iii).

[46] 2021 CDR Amendment Rules, Schedule 3, para 5; CDR Rules r 1.10C(4).

[47] 2021 CDR Amendment Rules, Schedule 3, para 5; CDR Rules r 1.10C(3). See section 8(d) below for a more detailed analysis of the verification processs.

[48] 2021 CDR Amendment Rules, Schedule 3, para 11; CDR Rules r 7.9(3).

[49] 2021 CDR Amendment Rules, Schedule 3, para 12; CDR Rules r 8.11(1)(c)(iv).

[50] See 'Consumer Experience', Consumer Data Standards (Web Page) <https://consumerdatastandardsaustralia.github.io/standards/#consumer-experience>.

[51] Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021: Explanatory Statement 20.

[52] CPA Australia, 'Consumer Data Right Rules Expansion Amendments Consultation Paper (29 October 2020) 3 <https://www.cpaaustralia.com.au/-/media/project/cpa/corporate/documents/policy-and-advocacy/consultations-and-submissions/digital-transformation/pre-2021/customer-data-rights-and-trusted-advisers-submission.pdf?rev=444554d41d6d42b2a71155c24b4cb2eb&download=true>.

[53] Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021: Explanatory Statement 20. See section 8(c) below for a more detailed analysis of the information security controls.

The amendments do not envisage any additional *record-keeping* or *reporting* duties for trusted advisers: the new reporting obligations apply to ADRs instead. First, the latter are required to keep and maintain *records* of:

- disclosures of CDR data to trusted advisers,
- trusted advisers to whom CDR data was disclosed and
- the steps taken to confirm that a trusted adviser is a member of one of the approved classes of trusted advisers.[54]

Second, ADRs must periodically report:

- the number of consents received from CDR consumers during the reporting period to disclose CDR data to trusted advisers and
- the number of trusted advisers to whom CDR data was disclosed during the reporting period (for each class of trusted advisers).[55]

8. ANALYSIS OF THE CDR REFORMS RELATING TO TRUSTED ADVISERS

The 2021 CDR Amendment Rules seek to enable consumers to use the CDR framework to share CDR data with their trusted advisers and are expected to 'encourage greater participation in the CDR by accommodating existing and new use cases which rely on the ability to disclose data to third parties'.[56] The reforms have generated polarised views, from clear support[57] to outright rejection and claims that '[d]isclosure to a "trusted adviser" is not just inherently risky but is contrary to the entire point of the CDR to provide a safe and secure data environment'.[58]

As with any data sharing framework for valuable data, the key component of success is end-users' trust – and, particularly in the CDR context, *consumers'* trust. The new framework for trusted advisers includes two main sources that should help generate such trust:

- First, a set of consumer protection mechanisms envisaged by the revised CDR Rules (as outlined in section seven above).
- Second, recognition that 'as members of a professional class, [trusted advisers] are subject to existing professional or regulatory oversight, including obligations to act in accordance with the consumer's interests (e.g. fiduciary or other duties to act in the best interests of their clients)'.[59]

The protections in the first group, which target mainly ADRs, largely apply *prior* to the disclosure of CDR data to the trusted adviser, or *during* such disclosure (except for the obligation to update consumer dashboards). At the same time, any professional duties or standards applicable to trusted advisers become crucial *after* such disclosure has taken place.

[54]2021 CDR Amendment Rules, Schedule 3, para 14; CDR Rules r 9.3(2)(eb)-(ec).

[55]2021 CDR Amendment Rules, Schedule 3, para 15; CDR Rules r 9.4(2)(f)(vi)-(vii).

[56]Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021: Explanatory Statement 18.

[57]CPA Australia, Chartered Accountants Australia and New Zealand, the Institute of Public Accountants and the Institute of Certified Bookkeepers, 'RE: Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021 (30 July 2021) <https://www.cpaaustralia.com.au/-/media/project/cpa/corporate/documents/policy-and-advocacy/consultations-and-submissions/cross-policy/2021/joint-submission-amendments-to-cdr-rules.pdf?rev=7f15cbed9ffa4a1a88b2e708927aab09&download=true>.

[58]Financial Rights Legal Centre et al, 'Consumer Data Right Rules Amendments (Version 3) (23 July 2021) 4 <https://financialrights.org.au/wp-content/uploads/2021/07/210723_TreasuryCDRRulesUpdate_FINAL.pdf>.

[59]Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021: Explanatory Statement 20.

This section will next consider the adequacy of the new CDR provisions aimed at trusted advisers from different perspectives.

a. Best interests duties of trusted advisers

A number of submissions have stressed the importance of professional rules, codes and standards trusted advisers may be subject to – as evidence of appropriate consumer protections afforded by professional advisers handling CDR data.[60]

At the same time, the degree of consumer comfort generated by a best interests duty has its limits, and in practice compliance with this duty has been fraught with challenges for some classes of trusted advisers.

For example, in a 2018 study focusing on the largest advice licensees (by number of advisers) owned or controlled by Australia's largest financial institutions the Australian Securities and Investments Commission ('ASIC') found that in 75 per cent of reviewed cases the adviser failed to demonstrate compliance with the duty imposed by section 961B of the *Corporations Act 2001* (Cth).[61]

In a subsequent study focusing on the superannuation sector, the number of noncompliant advice providers exceeded 50 per cent.[62]

In the light of these practices (as well as the Hayne Royal Commission findings), some commentators have questioned the wisdom of expanding access to CDR data by financial advisers[63] and some challenged the appropriateness of calling some types of professional advisers 'trusted' in the first place:

> 'Given the multiple inquiries and the recent royal commission into financial services the reputation of financial advisors and mortgage brokers is such that "trusted" advisor is particularly in-apt.'[64]

Furthermore, the imposition of the best interests duty has another implication: in addition to providing a certain degree of comfort to consumers, it may – as argued by some commentators – *encourage* trusted advisers to access CDR data (with the implication that such advisers should 'have access to as much information as possible').[65]

Indeed, as long as the CDR framework facilitates convenient and secure access to consumers' data, one might argue that this indirectly affects the scope of the best interests duty – primarily in terms of the types and volumes of information about consumers trusted advisers are expected to collect.

For example, under s 961B of the *Corporations Act 2001* (Cth) an advice provider who wishes to rely on the 'safe harbour' provision in subsection (2) must demonstrate that it has 'made reasonable inquiries to obtain complete and accurate information' in situations 'where it was reasonably apparent that information relating to the client's relevant circumstances was incomplete or inaccurate'.[66]

[60]For example, the Financial Planning Association of Australia emphasised the best interest duty of financial planners and their duty to adhere to a code of ethics. See Financial Planning Association of Australia, 'Inquiry into Future Directions for the Consumer Data Right' (21 May 2020) 3 <https://treasury.gov.au/sites/default/files/2020-07/fpa-australia.pdf>.

[61]ASIC, 'Financial Advice: Vertically Integrated Institutions and Conflicts of Interest' (Report 562, January 2018) 36 <https://download.asic.gov.au/media/4632718/rep-562-published-24-january-2018.pdf>.

[62]ASIC, 'Financial Advice by Superannuation Funds' (Report 639, December 2019) 30 <https://download.asic.gov.au/media/5395538/rep639-published-3-december-2019.pdf>.

[63]Super Consumers Australia, 'Submission to the Inquiry into Future Directions for the Consumer Data Right' (May 2020) 16-17 <https://treasury.gov.au/sites/default/files/2020-07/super-consumers-australia.pdf>.

[64]Financial Rights Legal Centre, 'Submission by the Financial Rights Legal Centre: CDR Rules Expansion Amendments Consultation Paper (October 2020) 31 <https://financialrights.org.au/wp-content/uploads/2020/10/201029_ACCCCDRRulesexpansion_Sub_FINAL-1.pdf>.

[65]See, eg, Mortgage & Finance Association of Australia, 'Consumer Data Right – Inquiry into Future Directions for the Consumer Data Right' (18 May 2020) 4 <https://treasury.gov.au/sites/default/files/2020-07/mortgage-finance-association.pdf>.

[66]Corporations Act 2001 (Cth) s 961B(2)(c).

With the expansion of the CDR framework, 'reasonable inquiries' in this context may end up being interpreted as implying that requests to access consumers' CDR data are not merely optional, but are, in fact, expected. In this context, a best interest duty may create an incentive for trusted advisers to collect more CDR data.

At the same time, this duty offers little in terms of ensuring that collected data (including CDR data) stays safe. Therefore, one needs to consider the relevant tools, such as privacy protections (subsection 8(b)) and information security controls (subsection 8(c)).

b. Limited reach of privacy protections

In 2018, a survey by Accenture identified security and privacy of financial data as 'Australian consumers' biggest concern with Open Banking', with 64 per cent of respondents citing it 'as the main obstacle to sharing their financial data with third parties'.[67] In the context of prospective sharing of CDR data with non-accredited entities, these issues become understandably more pronounced. On the one hand, the CDR privacy safeguards do not apply to such entities. On the other hand, some of the non-accredited recipients of CDR data (as discussed below) may not even be captured by the *Privacy Act 1988* (Cth). This can potentially degrade user experience and undermine consumer trust in the CDR framework.

In fact, the potential for degraded privacy protections has been identified as one of the key objections to allowing non-accredited entities access to CDR data:

> 'Any decision to allow non-accredited third parties to access sensitive CDR data is *incredibly dangerous*. It is dangerous because consumers are being led to assume their data will be protected under a "Consumer Data Right" but in fact it is facilitating the movement of this data to *lower privacy protections*.'[68]

In the view of the Office of the Australian Information Commissioner ('OAIC'), 'any … expansion of the CDR system should also maintain the strong privacy protections and safeguards that currently exist within the system'.[69] This view was shared by Visa, which argued that 'the paramount focus of any data-sharing should be on security, privacy, data protection, and consumer empowerment to manage their data'.[70] Furthermore, Westpac, while agreeing in principle to the idea of multi-tier CDR accreditation frameworks, firmly rejected the idea of compromising on matters of security or privacy at *any level*:

> 'Accreditation at any level – including for intermediaries and third parties – should at the very least meet the same high standards around security, privacy and the need for consumer consent as currently exist under the regime, with the expectation of additional more stringent requirements for those seeking write-access. Different accreditation obligations may be useful to distinguish between the different risk profiles associated with different activities, however, there should be *no relaxing of obligations concerning security, privacy* and consumer consent.'[71]

[67]Accenture, 'Tech Giants, Online Retailers Face Uphill Battle Pursuing Bank Market Share in Australia, But New "Open Banking" Rules Could Tilt the Landscape, Accenture Research Finds' (Media Release, 25 July 2018) <https://newsroom.accenture.com/news/tech-giants-online-retailers-face-uphill-battle-pursuing-bank-market-share-in-australia-but-new-open-banking-rules-could-tilt-the-landscape-accenture-research-finds.htm>.

[68]Financial Rights Legal Centre and Consumer Action Law Centre, 'Submission by the Financial Rights Legal Centre and Consumer Action Law Centre; Consumer Data Right: Consultation on How Best to Facilitate Participation of Third Party Service Providers, December 2019' (February 2020) 8 <https://www.accc.gov.au/system/files/CDR%20rules%20-%20intermediaries%20consultation%20submission%20-%20Financial%20Rights%20Legal%20Centre%20%28FRLC%29_Redacted.pdf> (emphasis added).

[69]Office of the Australian Information Commissioner, 'Inquiry into Future Directions for the Consumer Data Right – Issues Paper: Submission by the Office of the Australian Information Commissioner' (21 May 2020) 5 <https://treasury.gov.au/sites/default/files/2020-07/oaic.pdf>.

[70]Visa, Submission to the Inquiry into the Future Directions for the Consumer Data Right (19 May 2020) 5 <https://treasury.gov.au/sites/default/files/2020-07/visa.pdf>.

[71]Westpac, 'Re: Inquiry into the Future Directions for the Consumer Data Right' (25 May 2020) 8 <https://treasury.gov.au/sites/default/files/2020-07/Westpac-2020.pdf> (emphasis added).

Overall, the OAIC seemingly accepted the lowering of consumer protections to some extent, merely suggesting that 'CDR data provided to trusted advisors [sic] outside the CDR system should still be subject to a baseline level of protection, being the protections in the Privacy Act'.[72] The latter is only achievable, however, when all trusted advisers are considered 'APP entities' for the purposes of the Privacy Act 1988 (Cth). In practice that is not always the case due to the limited coverage of the Privacy Act 1988 (Cth), which does not apply to most small businesses (i.e. those with an annual turnover of $3 million or less, as per section 6D of the Act).

Prior to the transfer of the CDR rule-making function away from the ACCC, this issue was raised in an independent Privacy Impact Assessment of the proposed changes to CDR Rules (conducted by Maddocks)[73] and acknowledged by the ACCC,[74] as well as in other submissions[75] and remains outstanding at the time of writing but may be resolved if the proposed removal of the small business exemption (also proposed by the OAIC)[76] is eventually introduced into Australian law.

In the context of the ongoing (at the time of writing) review of the *Privacy Act 1988* (Cth), the 2021 CDR Amendment Rules may *serve as a catalyst for the adjustment (or complete elimination) of the small business exemption* – which would directly affect currently exempted advisers. It is noteworthy, however, that the October 2021 discussion paper[77] considers a number of alternative approaches to a complete removal of the exemption, such as:

- reduction of the annual turnover threshold,
- introduction of an employee number threshold,
- a requirement for small businesses to comply with some, but not all, Australian Privacy Principles or
- prescribing additional high risk acts and practices to be covered by the Privacy Act 1988 (Cth) regardless of turnover of the relevant business.[78]

[72]Office of the Australian Information Commissioner, 'OAIC Submission to the CDR Rules Expansion Amendments Consultation' (29 October 2020) <https://www.oaic.gov.au/engage-with-us/submissions/oaic-submission-to-the-cdr-rules-expansion-amendments-consultation/>.

[73]'We recommend that the ACCC consider only allowing CDR Data and CDR Insights to be disclosed outside of the CDR Regime to APP entities, or to entities who agree to comply with the APPs as if they were an APP entity.': Maddocks, 'Australian Competition and Consumer Commission: Consumer Data Right Regime; Update 2 to Privacy Impact Assessment' (8 February 2021) 14 <https://www.accc.gov.au/system/files/CDR%20v2%20Rules%20%E2%80%93%20Update%202%20to%20Privacy%20Impact%20Assessment.pdf>.

[74]Consumer Data Right, 'Consumer Data Right Rules: Update 2 to Privacy Impact Assessment; Agency Response (February 2021) 13 <https://www.accc.gov.au/system/files/Attachment%20B%20-%20ACCC%20response%20to%20update%202%20to%20Privacy%20Impact%20Assessment.pdf>.

[75]See, eg, Financial Rights Legal Centre, 'Submission by the Financial Rights Legal Centre: Inquiry into Future Directions for the Consumer Data Right (May 2020) 46-50 <https://treasury.gov.au/sites/default/files/2020-07/c2020-62639-financialrightslegalcentre.pdf>.

[76]'Recommendation 27 – Remove the small business exemption, subject to an appropriate transition period to aid with awareness of, and preparation for compliance with, the Privacy Act.': OAIC, 'Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner' (11 December 2020) 15 <https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission>.

[77]Attorney-General's Department, 'Privacy Act Review: Discussion Paper' (October 2021) https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/

[78]Ibid 45-48.

c. Information security controls of trusted advisers

Protections for consumers – particularly in the event of data breaches – are one of the key issues associated with the CDR regulatory framework. For example, according to the Australian Privacy Foundation, '[d]ata breaches are a near certainty' and the proper question 'is not if but when' – whereas the CDR regime is inadequate because (among other things) '[c]ompensation for loss is difficult to prove and obtain', '[t]here are no legislated or enforced security standards' and '[t]here is little or no enforcement or fines for data breaches which means there is little incentive for security by small intermediaries that hold data'.[79] If this status quo is accepted, further expansion of the CDR framework almost inevitably multiplies the risks of data breaches – which have recently been in ASIC's crosshairs, as the regulator initiated proceedings against RI Advice Group Pty Ltd over poor cyber security controls.[80]

Since trusted advisers do not require special accreditation to act as recipients of CDR data, the revised CDR Rules seemingly attempt to minimise their impact on the day-to-day operations of trusted advisers, stopping just short of attempting to impose explicit obligations on them. The 2021 CDR Amendment Rules do not prescribe bespoke information security requirements applicable to trusted advisers, which suggests that the CDR framework does not aim to interfere with any pre-existing information security obligations trusted advisers may already be subject to.

Two parallel information security regimes

Despite the above conclusion, an important practical question is whether the revised CDR framework *indirectly* encroaches on trusted advisers – and if so, to what extent. Notably, the Explanatory Statement emphasises that the 'disclosure of the CDR data from an accredited data recipient to a trusted adviser is covered by the information security controls in Schedule 2 to the CDR Rules' and, as a result, 'the minimum information security control of encrypting data in transit applies to the disclosure'.[81]

This conclusion appears to be based on paragraph 1.5(1)(a) of Schedule 2 of the CDR Rules, which requires accredited data recipients (among other things) to 'have and maintain an information security capability that … complies with the applicable information security controls' listed in the same Schedule. Importantly, however, Schedule 2 focuses on the obligations of *accredited data recipients*, rather than unaccredited parties. This is understandable, since originally within the CDR framework ADRs were not just one category of recipients of CDR data – they were *the only category* of recipients of CDR data (other than consumers themselves). From this perspective, the principal objective of the provisions in Schedule 2 was to enhance the information security environment at the level of ADRs (i.e. *recipients*) of CDR data (which is logical, considering that data holders were already covered by substantial information security obligations). As a result, the ongoing information security obligations of all ADRs helped preserve the overall security of data in the CDR ecosystem and ensure that data recipients would not act as its 'weakest link'.

[79]Australian Privacy Foundation, 'Submission to the Issues Paper: Inquiry into the Future Directions of the Consumer Data Right' (6 May 2020) 2 <https://treasury.gov.au/sites/default/files/2020-07/australian-privacy-foundation.pdf>.

[80]See *Australian Securities and Investments Commission v RI Advice Group PTY LTD (2020)* FCA File Number VID556/2020.

[81]Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021: Explanatory Statement 20.

This status quo changes substantially in one-way transfers of CDR data from ADRs (accredited recipients) to trusted advisers (unaccredited recipients). In this setting, accredited data recipients only act as transferors of data. Trusted advisers, on the other hand, only act as data recipients and are subject to their own information security rules (which may or may not be as strict as those found in Schedule 2 of the CDR Rules). In other words, instead of establishing a single information security framework for different recipients of CDR data, the reforms have made possible co-existence of two parallel regimes (with different requirements for data protection): one for ADRs and one for trusted advisers.

The 'weakest link' problem

This raises a logical question: might trusted advisers end up being the 'weakest link', since they are not subject to CDR-specific information security controls? The answer depends on the requirements that apply to trusted advisers by virtue of their legal/regulatory status (rather than their participation in the CDR framework). The scope and effectiveness of the relevant information security controls is of fundamental importance in the revised CDR Rules: if these controls are found lacking, the assumption that consumer data is held by trusted advisers *securely* falls off, which may negatively affect the credibility of the new rules in the eyes of consumers, as well as regulators.

While different classes of trusted advisers are subject to different legal frameworks, the relevant information security obligations often remain high-level and flexible in scope and typically require trusted advisers to 'have adequate risk management systems'[82] or to 'establish and maintain a Risk Management Framework'[83] to deal with different types of risks, including technology (e.g. cyber security) risks. The absence of detailed technical specifications can be explained by several factors, such as fear of over-regulation and the expectation that more flexible regulatory frameworks are better suited for dealing with dynamic and intelligent cyber threats.[84] Nonetheless, the effectiveness of high-level and abstract information security requirements is ultimately determined by the quality of their implementation – which can vary across different classes of trusted advisers. In practice, it is possible that while some trusted advisers may have in place complex cyber security systems and processes, others might struggle to deal with more sophisticated cyber-attacks due to the lack of relevant resources and expertise. Yet both groups need to be particularly mindful of their information security obligations.[85]

In the context of the CDR framework, it should be borne in mind that the party most vulnerable to the above-mentioned information security threats is the consumer whose CDR data leaves the CDR framework upon disclosure to a trusted adviser. Such consumer cannot be reasonably expected to possess the sophistication and expertise to conduct proper due diligence of the information security controls implemented by the selected trusted adviser and is, therefore, likely to *trust* their adviser without ascertaining whether the computer and risk management systems of its adviser are, in fact, *trustworthy*.

[82]See s 912A(1)(h) of the *Corporations Act 2001* (Cth); s 47(1)(l)(ii) of the *National Consumer Credit Protection Act 2009* (Cth).

[83]See paras 4.1-4.2 of the APES 325 'Risk Management for Firms' developed by the Accounting Professional & Ethical Standards Board.

[84]See, eg, Anton Didenko, 'Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonization in the European Union and Beyond' (2020) 25(1) Uniform Law Review 125, 138-139.

[85]See *Australian Securities and Investments Commission v RI Advice Group PTY LTD (2020)* FCA File Number VID556/2020.

The challenge of ensuring an effective minimum standard of information security is very complex[86] and is yet to be adequately resolved in many sectors (let alone on an economy-wide scale). Since trusted advisers do not need to incur the costs associated with bespoke CDR information security controls (which were custom-made for the CDR regime and are likely to be more expensive to implement),[87] some commentators have proposed to prescribe globally recognised information security standards for all entities participating in the CDR ecosystem (including trusted advisers). According to the Australian Banking Association, this approach would be both feasible and realistic in terms of the underlying costs:

'Whilst implementation costs of the information security standards will vary according to size and complexity of each entity, it is our understanding that accreditation with global technical standards bodies will cost circa $2,000-$3,000. This appears to be a modest amount to ensure uniform standards of information security implementation for consumers and participants of the ecosystem.'[88]

Regardless of any possible expansion of information security controls applicable to trusted advisers, the true implication of the 2021 CDR Amendment Rules for trusted advisers cannot be found in the rules themselves: on paper they are not subject to any additional bespoke CDR-related requirements of greater information security; in practice, the new regime merely turns on an assumption that data shared with any trusted adviser is safe. Should that assumption prove incorrect, this laissez-faire attitude is likely to be terminated or adjusted – given the real and immediate consequences of breaches of CDR data for consumers and considering that ASIC's recent proceedings against RI Advice Group Pty Ltd[89] may evidence a shift towards more active enforcement of information security obligations of licensees (in particular those engaged in providing advice to consumers).

Even though the information security obligations of trusted advisers may not necessarily match those applicable to ADRs, an important related question is whether the information security obligations of ADRs may create any spill-over implications for trusted advisers. To a certain extent, this may be true: after all, some of the duties in Schedule 2 of the CDR Rules require ADRs to focus on the data transfer processes (without specifying whether an ADR acts as a transferor or recipient of data). For example, ADRs must:

'Implement robust network security controls to help protect data in transit, including: encrypting data in transit and authenticating access to data in accordance with the data standards (if any) and industry best practice, implementing processes to audit data access and use, and implementing processes to verify the identity of communications.'[90]

On the other hand, most information security controls in the Schedule apply to data *at rest* (as opposed to *in transit*) – and, since they affect only ADRs, do not impact trusted advisers, which limits the spill-over effects of ADRs' mandatory minimum information security controls on trusted advisers. Furthermore, the rules for trusted advisers do not establish an unequal relationship (as observed, for example, in the case of sponsored accreditation):[91] ADRs are not responsible for the actions or information systems of trusted advisers.

[86]See ibid.

[87]Australian Banking Association, 'Consumer Data Right Rules Amendments (Version 3) Consultation' (30 July 2021) 7-8 https://treasury.gov.au/sites/default/files/2021-10/aba.pdf.

[88]Ibid 8.

[89]See *Australian Securities and Investments Commission v RI Advice Group PTY LTD (2020)* FCA File Number VID556/2020.

[90]See CDR Rules, Schedule 2, Part 2, r 2.2.

[91]See, eg, the obligations of the sponsor in relation to its affiliate at a sponsored tier of accreditation, as envisaged in 2021 CDR Amendment Rules, Schedule 1, para 34.

Is vetting allowed?

This raises another related issue concerning the ability of ADRs to assess the information security risks of CDR data transfers to trusted advisers. It should be noted that nomination of trusted advisers is made by a consumer, rather than by an accredited person.[92] In this context, is an ADR allowed to reject the nomination of a trusted adviser, if in the opinion of the ADR such trusted adviser appears to lack adequate information security controls, despite falling within one of the six approved classes? In other words, can an ADR sharing CDR data with a trusted adviser second-guess the non-accredited data recipient? Is any kind of vetting process by ADRs allowed? Several important observations can be made on the basis of the revised CDR Rules.

First, crucially, the 2021 CDR Amendment Rules do not *require* ADRs to offer the functionality of sharing CDR data with a trusted adviser ('An accredited person *may* invite a CDR consumer to nominate one or more persons as trusted advisers…').[93] Nor do the revised rules *require* ADRs to disclose CDR data once a TA disclosure consent has been given (a consent evidences permission, not compulsion). In fact, according to the ACCC, the disclosures of this kind are 'likely to occur in the context of an established commercial relationship between the ADR and the non-accredited person'.[94] Interestingly, however, this assumption does not appear to be fully aligned with the verification process (discussed in section 8(d) below), which, on its face, is more appropriate for a framework where ADRs and trusted advisers operate on an arm's length basis.

Second, even if any vetting by ADRs were expressly envisaged, it is likely it would be limited only to the *data transmission process* through which CDR data is transferred to a trusted adviser – not storage of that data at rest within that trusted adviser's systems. This conclusion is supported by the scope of the information security controls found in Part 2 of Schedule 2 of the CDR Rules, which are an element of an accredited data recipient's *own information security capability* (rather than the capability, and responsibility for the capability, of any other entity – such as trusted advisers).[95] In addition, according to the Explanatory Statement, the relevant controls apply to the '*disclosure* of the CDR data from an accredited data recipient to a trusted adviser'.[96]

Third, according to Part 2 of Schedule 2 of the CDR Rules, the minimum information security control of encrypting data in transit (which is expressly mentioned in the Explanatory Statement)[97] is meant to limit the risk of inappropriate or unauthorised access to an accredited data recipient's *own* 'CDR data environment'. Since accredited data recipients themselves are responsible for defining the boundaries of such environment,[98] it is not entirely clear whether and how these boundaries may overlap within the CDR framework. For example, on a narrow interpretation, the requirement of encrypting data in transit within an ADR's *own* CDR data environment may be interpreted as referring to transit of data between an accredited data recipient's *own* systems – rather than transfers of CDR data outside them, such as in the case of transfers of CDR data to a trusted adviser.

[92] See CDR Rules r 1.10C(1).

[93] 2021 CDR Amendment Rules, Schedule 3, para 5; CDR Rules r 1.10C(1).

[94] Australian Government, 'CDR Rules Expansion Amendments: Consultation Paper' (September 2020) 29 <https://www.accc.gov.au/system/files/CDR%20rules%20expansion%20amendments%20-%20consultation%20paper%20-%2030%20September%202020.pdf>.

[95] See CDR Rules, Schedule 2, r 1.5(1)(a).

[96] Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021: Explanatory Statement 20 (emphasis added).

[97] Ibid.

[98] See CDR Rules, Schedule 2, r 1.4(1).

However, the Explanatory Statement suggests this is not the case – and that disclosures to trusted advisers are also subject to the encryption requirement. The necessary implication of this statement appears to be that the 'CDR data environment' of an accredited data recipient encompasses all the data transmission channels an ADR may use to transfer CDR data to any non-accredited entity.

Fourth, although the CDR Rules do not directly regulate the information security controls implemented by trusted advisers and ADRs are not responsible for the information systems used by trusted advisers, accredited data recipients are free to choose the data transfer channels and encryption types used for sharing CDR data with trusted advisers.

As a result, on a literal interpretation of the new rules, ADRs remain in control of the CDR data that has been disclosed to them, as well as in control of the data channels they use to disclose CDR data to trusted advisers. In the absence of a clear legal compulsion to disclose CDR data pursuant to a valid TA disclosure consent, accredited data recipients are likely to err on the side of caution and offer the functionality to disclose CDR data only to those trusted advisers that they know and trust – as surmised by the ACCC.[99] If so, under the current CDR framework accredited data recipients end up as *de facto* gatekeepers of CDR data – as an alternative to the CDR regime attempting to regulate the information security controls of trusted advisers directly. Whether this is appropriate or not is ultimately a question of policy. A vetting process may be plausible from the point of view of *overall data security* – but any resulting benefits ought to be weighed carefully against the risks of ADRs imposing arbitrary requirements on trusted advisers on a case-by-case basis (which may limit the attractiveness of the new regime).[100] Ultimately, if such requirements imposed by ADRs appear too burdensome, a separate tier of accreditation for trusted advisers devoid of such added interference might be a more suitable alternative.

d. Verification process and allocation of liability

As discussed in the previous section, the 2021 CDR Amendment Rules introduce no additional information security protections once CDR data has been transferred from an ADR to a trusted adviser: essentially, the trusted adviser itself (or rather any associated professional duties and standards it may be subject to) is (are) expected to be the source of consumer confidence. Under this approach, the status and identity of a trusted adviser is of paramount importance, since transfers of CDR data to a wrong person would deprive the consumer of even the residual protections (in the absence of bespoke CDR-imposed duties) that trusted advisers are expected to provide by virtue of their professional status. Within such framework, the correct identification of the recipient should understandably be the responsibility of the disclosing entity, namely the ADR (for the consumer lacks the technical capacity to operate the CDR data channels and can always provide the relevant data directly to the trusted adviser outside the CDR regime if the latter becomes too cumbersome).

[99] Australian Government, 'CDR Rules Expansion Amendments: Consultation Paper' (September 2020) 29 <https://www.accc.gov.au/system/files/CDR%20rules%20expansion%20amendments%20-%20consultation%20paper%20-%2030%20September%202020.pdf>.

[100] On the risks of requirements imposed by ADRs, see CPA Australia, 'Consumer Data Right Rules Expansion Amendments Consultation Paper' (29 October 2020) 2 <https://www.cpaaustralia.com.au/-/media/project/cpa/corporate/documents/policy-and-advocacy/consultations-and-submissions/digital-transformation/pre-2021/customer-data-rights-and-trusted-advisers-submission.pdf?rev=444554d41d6d42b2a71155c24b4cb2eb&download=true>.

The initial proposal published by the Treasury as part of the July 2021 public consultation envisaged a positive obligation for an accredited data recipient to take '*reasonable steps* to confirm that the trusted adviser is currently a member of a class of trusted advisers'[101] (since in the absence of such steps any disclosure to a trusted adviser would not be considered a 'permitted use or disclosure'). Unfortunately, the proposed rules did not specify what amounts to such 'reasonable steps' – although the explanatory materials clarified that these could include 'the ADR checking a register for the relevant class of trusted adviser' or 'seeking confirmation from the trusted adviser'.[102]

The 2021 CDR Amendment Rules follow a slightly different approach:

> 'Where the accredited person has taken reasonable steps to confirm that a person nominated as a trusted adviser was, and remains, a member of a [relevant] class …, the person is taken to be a member of that class for the purposes of this rule.'[103]

This provision serves as a safe harbour for the accredited person. Despite its perceived simplicity, the revised language raises several issues concerning its practical implementation.

What steps are required to constitute a 'permitted use or disclosure'?

According to rule 7.5(1)(ca) of the revised CDR Rules, disclosure of CDR data by an ADR is a 'permitted use or disclosure' if it is made 'in accordance with a current disclosure consent' (which includes a 'TA disclosure consent' – i.e. a consumer's consent to disclose such data to a trusted adviser). It follows that, in order to comply with this requirement, an ADR would need to verify that the nominated person is indeed a 'trusted adviser' and ensure that the CDR data actually reaches the nominated trusted adviser. The safe harbour in rule 1.10C(3) targets the first of these two steps – namely, verification of the 'trusted adviser' status of the nominee. It protects ADRs in cases where a consumer has nominated an ineligible person and, as a result, the recipient of the CDR data ended up being a non-trusted adviser, provided that the accredited person has demonstrated a certain minimal degree of diligence in response to a TA disclosure consent.

This safe harbour seemingly presumes that the consumer's nominee may be unknown to the accredited person – since otherwise (i.e. if ADRs only cooperated with trusted advisers they know) these added protections would be unnecessary. Perhaps more importantly, the accredited person remains at all times responsible for identifying what information channels the nominated person can utilise to receive CDR data and verifying whether these channels are controlled by such nominated person, so that CDR data disclosed through these channels reaches the correct recipient. A failure by an ADR to exercise due diligence resulting in a transfer of CDR data to anyone but the nominated person should not be captured by the safe harbour.

[101] Competition and Consumer (Consumer Data Right) Amendment (2021 Measures No. 1) Rules 2021 - Exposure Draft 2021 (Cth), Schedule 3, para 10 (emphasis added).
[102] Competition and Consumer (Consumer Data Right) Amendment (2021 Measures No. 1) Rules 2021: Exposure Draft Explanatory Materials (July 2021) 15.
[103] 2021 CDR Amendment Rules, Schedule 3, para 5; CDR Rules r 1.10C(3) (emphasis added).

Minimal degree of diligence required from an accredited person

The safe harbour in rule 1.10C(3) only requires the accredited person to take 'reasonable steps' to verify the status of the nominee. According to the Explanatory Statement, this requirement employs 'a *scalable standard* that will depend on the circumstances'.[104] However, since this 'scalable standard' comes without any specific criteria that could be applied ex ante, determination of what constitutes 'reasonable steps' will be made on a case-by-case basis, which generates uncertainty. Several observations can be made, however.

First, it appears from the Explanatory Statement that in certain circumstances the safe harbour may not be available to an accredited person, regardless of the steps taken to verify the nominee's eligibility. This would be the case 'where the accredited data recipient knew, or ought to have known that a person is not a trusted adviser'.[105]

Second, in the circumstances where the safe harbour is available, the 'reasonable steps' will depend on 'whether it is the consumer, or accredited data recipient, that has a closer relationship with the proposed trusted adviser when they are nominated by the consumer'.[106]

Third, according to the Explanatory Statement, the 'reasonable steps' test is not limited to conducting independent verification of the nominee's status: it is expected that accredited persons would be able to rely on the information provided by the nominees themselves (e.g. in the form of a 'contractual warranty' or an 'attestation or representation' by the nominee).[107]

This flexibility can be particularly detrimental to the consumer because the latter bears the risks of disclosures to a non-trusted adviser in cases where the nominee has provided false information – whereas the accredited person enjoys *multiple* protections (the safe harbour rule and the contractual claims arising from a breach of warranty or misrepresentation).

Fourth, the 2021 CDR Amendment Rules do not specify what information should be provided by a consumer in a nomination of a trusted adviser. This may lead to uncertainty in determining whether the resulting disclosure by an ADR is captured by the safe harbour provision. For example, if a consumer has only provided the name of the nominated person but failed to provide other details (e.g. the address) – and, as a result, the ADR disclosed the consumer's CDR data to a different person (with a very similar sounding name), has the ADR taken 'reasonable steps' in this case? A more complicated scenario would arise if a consumer has only provided an address of the nominated person (without specifying their name) – and the ADR discloses the consumer's CDR data to a trusted adviser operating at that address (without ascertaining that there are multiple trusted advisers at that same address, and it is unclear which one was nominated by the consumer).

[104]Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021: Explanatory Statement 19 (emphasis added).
[105]Ibid 20.
[106]Ibid 19.
[107]Ibid.

Fifth, it is plausible that the 'reasonableness' test and the associated uncertainty would not have been introduced in the first place in the absence of some perceived difficulty in confirming one's status as a trusted adviser (since otherwise the flexibility afforded to the accredited person would have been redundant). If that is the case, a better solution would be to address the source of the problem and improve the transparency, accuracy and completeness of public registries of trusted advisers – so that:

- ADRs were able to rely on those registries to confirm the current status of any nominee in real time and
- a failure to consult a corresponding registry would amount to a breach of the safe harbour rule.

The above issues create a number of challenges for trusted advisers. As a result of uncertainty generated by the 'reasonable steps' test, some accredited persons may prefer to err on the side of caution (as is not uncommon in commercial practice) and introduce extensive checks of consumers' nominees (including seeking direct confirmations from the relevant regulators and/or professional associations) and on top of that request contractual protections from those nominees (a measure that is expressly mentioned in the Explanatory Statement).[108]

Furthermore, the verification process in rule 1.10C(3) may generate delays (in addition to the process of nomination of trusted advisers and the duty to update consumer dashboard after disclosure of CDR data to trusted advisers).[109] According to CPA Australia et al. 'it could take days for an accredited person to confirm the class claimed by the trusted adviser'.[110]

The proposed measures to promote reliance on independent real-time verification of trusted adviser status (via public registries of trusted advisers with information that is conclusive, comprehensive and updated 24/7) would help mitigate this issue by reducing the time and cost of individual verifications.

Timing of verification actions

To comply with the safe harbour provisions of rule 1.10C(3), the accredited person needs to check that the consumer's nominee 'was, and remains' a member of a class of trusted advisers. The use of the words 'was' (in the past) and 'remains' (which implies an uninterrupted status) suggests that the verification should cover not just two separate points in time, but a continuous period beginning at some point in the past and continuing until the cut-off time in the present. While the text of the rules does not state this explicitly, the provision seemingly aims to cover the period between nomination by the consumer and the disclosure of CDR data to the nominated person. To eliminate uncertainty, the wording could be amended by specifying the relevant period more clearly, as follows:

> Where the accredited person has taken reasonable steps to confirm that a person nominated as a trusted adviser was, *at the time of nomination*, and remains, at *the time of disclosure*, a member of a class mentioned in subrule (2), the person is taken to be a member of that class for the purposes of this rule.

[108] Ibid.

[109] 2021 CDR Amendment Rules, Schedule 3, para 11; CDR Rules r 7.9(3).

[110] CPA Australia, Chartered Accountants Australia and New Zealand, the Institute of Public Accountants and the Institute of Certified Bookkeepers, 'RE: Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021 (30 July 2021) 4 <https://www.cpaaustralia.com.au/-/media/project/cpa/corporate/documents/policy-and-advocacy/consultations-and-submissions/cross-policy/2021/joint-submission-amendments-to-cdr-rules.pdf?rev=7f15cbed9ffa4a1a88b2e708927aab09&download=true>.

Another issue that is not expressly addressed in the 2021 CDR Amendment Rules concerns disclosures to trusted advisers made by an accredited person that does not intend to make use of the safe harbour in rule 1.10C(3) because the accredited person is confident that at the time of disclosure the consumer's nominee belongs to a class of trusted advisers (e.g. when the nominee is well known to it). In other words, can an accredited person rely on rule 7.5(1)(ca) alone and argue that, as long as it can establish that the nominee is a trusted adviser *at the time of disclosure only,* the disclosure is made 'in accordance with a current disclosure consent' and, therefore, is a 'permitted disclosure'?

Interestingly, rule 1.10C(3) does not state explicitly that the safe harbour is the only way to satisfy the requirement of nominee verification – and thus the suggested scenario appears plausible. However, if that is correct, then for an ADR that is confident that the nominee is a trusted adviser *at the time of disclosure of CDR data to such trusted adviser,* the safe harbour becomes unnecessarily cumbersome (since it requires the relevant 'reasonable steps' to confirm the status of the nominee to be taken both at the time of nomination and at the time of disclosure, as well as in-between those dates). Additional clarity as to whether (and how) an accredited person can avoid relying on the safe harbour in rule 1.10C(3) is needed to address this issue.

Allocation of liability

While the intention to provide some comfort to ADRs is understandable, the implications of disclosing CDR data to a wrong person are different compared to the sharing of CDR data with another accredited person (since the CDR data essentially leaves the CDR ecosystem and may end up in the hands of an unregulated entity). Who should be responsible if, despite checking with the potential data recipient (or taking other 'reasonable steps') the ADR nonetheless discloses CDR data to an entity that is not a 'trusted adviser'?

On the one hand, among the three key parties involved in the sharing of such data (an ADR, a trusted adviser and a consumer), it is conceivable that the consumer should *not* be the party that ends up being disadvantaged. After all, a consumer is likely to have a limited understanding of 'the implications of consenting to the disclosure of CDR Data … to non-accredited recipients'.[111] Furthermore, consumers have no direct involvement in the exercise of CDR information security controls by ADRs and trusted advisers and are 'unlikely to know whether a particular action by an entity breaches their privacy rights'.[112] And yet, the new rules seem to focus on providing comfort to an ADR (through the 'reasonable steps' safe harbour) – rather than the consumer, who would take the brunt of a disclosure to a non-trusted adviser. If this is an expected outcome, it should be clearly explained to the consumer.

Furthermore, if the revised CDR framework seeks to encourage consumers to take more responsibility and exercise more direct control, then the absence of a clear customer's authority to (unconditionally) nominate a trusted adviser (without waiting for an invitation from an accredited person)[113] is an omission – one that has been noted in a submission by CPA Australia et al.[114]

[111]Maddocks, 'Australian Competition and Consumer Commission: Consumer Data Right Regime; Update 2 to Privacy Impact Assessment' (8 February 2021) 7 <https://www.accc.gov.au/system/files/CDR%20v2%20Rules%20%E2%80%93%20Update%202%20to%20Privacy%20Impact%20Assessment.pdf>.

[112]Ibid 59.

[113]Competition and Consumer (Consumer Data Right)2021 CDR Amendment (2021 Measures No. 1) Rules 2021 - Exposure Draft 2021 (Cth), Schedule 3, para 5. (draft rules; CDR Rules r 1.10C(1).

[114]CPA Australia, Chartered Accountants Australia and New Zealand, the Institute of Public Accountants and the Institute of Certified Bookkeepers, 'RE: Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021 (30 July 2021) 3 <https://www.cpaaustralia.com.au/-/media/project/cpa/corporate/documents/policy-and-advocacy/consultations-and-submissions/cross-policy/2021/joint-submission-amendments-to-cdr-rules.pdf?rev=7f15cbed9ffa4a1a88b2e708927aab09&download=true>.

e. Concerns about consumer trust

Members of the relevant classes of professionals expressed their broad support of the flexibility afforded to trusted advisers. Some even went as far as to argue that 'a trusted advisor should be treated *more like the consumer* under the CDR rather than a large corporate third-party accredited data recipient'.[115] This approach follows the simple logic that 'consumers trust their advisor and want to provide them with all the relevant information necessary for them to provide their trusted advice service'[116] and was aptly summarised in a recent joint submission by CPA Australia, Chartered Accountants Australia and New Zealand, the Institute of Public Accountants and the Institute of Certified Bookkeepers:

> '…[W]e emphasise that trusted advisers are known to the consumer and nominated by the consumer. Trusted advisers do not elect to engage in the CDR regime but do so to obtain the data required to fulfil a service for a consumer. Being a known person to the consumer mitigates any risks that may arise in respect of the security and privacy of the data. Trusted advisers are a distinct and unique class of non-accredited person within the CDR regime eco-system.'[117]

Nevertheless, even though consumers do, as the ACCC notes, 'routinely share their banking data with…these professionals',[118] data risks persist, and it is unlikely that consumers routinely verify the information security controls of professional advisers they engage. Some commentators went as far as to suggest that '[i]n reality most people who rightly (or wrongly) trust their advisor will simply do what the so-called trusted advisor will ask of them to do'.[119]

Furthermore, it has been suggested that separate consents envisaged by the new framework, even if coupled with the right disclosures, would be akin to 'the iTunes Agreement process where the consumer is highly likely to not engage with the details and simply go through the motions at the request of the non-accredited party'.[120] While the comparison may not be entirely accurate (in the sense that the number of competing service providers is likely to be higher in the case of trusted advisers), for consumers professional advisers remain a source of *specialist knowledge and expertise* that cannot be easily (if at all) replaced.

Even if we consider that the number of different trusted advisers is substantial, does competition among them lead to genuinely different (and easily verifiable by the consumer) levels of protection of consumers' data? This seems unlikely – unless some members of the relevant (e.g. legal or accounting) profession start competing internally against others by obtaining CDR accreditation. After all, why would members of such professional groups wish to compete on the basis of data security in the first place – if they are trusted by definition?

Does the new framework for trusted advisers create meaningful incentives for such professionals to attain a higher level of data security? Again, the answer is unfortunately in the negative: even if certain advisers were to upgrade their systems, this would be hard for a consumer to verify – unless the adviser in question obtains CDR accreditation or some other independent confirmation of the quality of its risk management frameworks.

[115]SMSF Association, 'SMSF Association Submission on Consumer Data Right Expansion Amendments' (29 October 2020) 1 <https://www.accc.gov.au/system/files/SMSF%20Association%20%2829%20October%202020%29.pdf> (emphasis added).

[116]Ibid 2 (emphasis added).

[117]CPA Australia, Chartered Accountants Australia and New Zealand, the Institute of Public Accountants and the Institute of Certified Bookkeepers, 'RE: Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021 (30 July 2021) 2 <https://www.cpaaustralia.com.au/-/media/project/cpa/corporate/documents/policy-and-advocacy/consultations-and-submissions/cross-policy/2021/joint-submission-amendments-to-cdr-rules.pdf?rev=7f15cbed9ffa4a1a88b2e708927aab09&download=true> (emphasis added).

[118]Australian Government, 'CDR Rules Expansion Amendments: Consultation Paper' (September 2020) 30 <https://www.accc.gov.au/system/files/CDR%20rules%20expansion%20amendments%20-%20consultation%20paper%20-%2030%20September%202020.pdf>.

[119]Financial Rights Legal Centre, 'Submission by the Financial Rights Legal Centre: CDR Rules Expansion Amendments Consultation Paper (October 2020) 32 <https://financialrights.org.au/wp-content/uploads/2020/10/201029_ACCCCDRRulesexpansion_Sub_FINAL-1.pdf>.

[120]Ibid 33.

In the light of the above, a more plausible explanation of the need to provide access to CDR data to trusted advisers can be found if one considers the alternative where no such access is provided. In that hypothetical scenario, consumers engaging such professionals get to choose between agreeing to use non-CDR data transmission channels used by their advisers (such as screen-scraping or emailing sensitive information to a broker)[121] and getting no service at all. As a result, consumers are likely to continue to share their data with professional advisers outside the CDR framework. In other words, a rigid CDR framework may indeed help to keep CDR data very safe internally – but it would offer little benefit for those consumers who already share the same data with providers of unique or non-easily replaceable services. The new rules attempt to address the issue by allowing trusted advisers to tap into the CDR data channels without incurring the most onerous obligations associated with the CDR framework. This change has the potential to reduce the attractiveness of alternative pathways used for obtaining consumers' data – although the effects of the change can only be ascertained through empirical research following the implementation of the new rules.

f. The need for empirical research

The pragmatism of allowing trusted advisers to access CDR data without separate accreditation because 'this is happening already'[122] is hard to deny. Whether this pragmatism will translate into palpable benefit for consumers remains an open question in the absence of a corresponding cost-benefit analysis – a measure proposed by some commentators.[123]

In this context, empirical research would help ascertain whether consumers actually understand the risks and protections available when they share their data with trusted advisers; and more specifically – whether the new CX standards for disclosures to trusted advisers facilitate consumer comprehension of underlying risks.

Given the issues associated with some classes of professionals outlined above (see section 8(a)), it might be helpful to avoid a 'wholesale' approach to trusted advisers – and instead to assess the levels of consumer trust and understanding *separately for different types of trusted advisers.* After all, it is possible that the perceived dissatisfaction (currently or in the future) with one group of trusted advisers does not translate directly into consumer distrust of the other, simply as a result of different types of professionals being subsumed under the broad (and artificial) category of 'trusted advisers' in the revised CDR Rules. For example, past unsatisfactory practices of financial advisers may not necessarily impact the public perception of the privacy and security afforded by other groups, such as lawyers or accountants. If so, the latter should not be prejudiced. Furthermore, if necessary, the rollout of the changes could be staggered for different types of trusted advisers.

[121] Australian Finance Group, 'Consumer Data Right Rules consultation – CDR Rules expansion amendments Submission by Australian Finance Group Ltd ACN 066 385 822' (29 October 2020) 3 <https://www.accc.gov.au/system/files/Australian%20Finance%20Group%20Ltd%20%2829%20October%202020%29.pdf>.

[122] Consumer Policy Research Centre, 'Submission to Consumer Data Right Rules Amendments (Version 3) Exposure Draft (30 July 2021) 1

[123] Ibid 2.

It is also unclear whether the introduction of a data sharing framework directed *outside* the CDR ecosystem will, in practice, facilitate the use of CDR data – or whether the corresponding disclosures explaining the underlying risks will, on the contrary, have a cooling effect on consumer interest. The new reporting and record-keeping obligations of ADRs may offer some insights into the levels of sharing of CDR data with trusted advisers – but in the absence of corresponding ex ante data for comparison, the usefulness of that data will be limited.

Lastly, it is worth noting that possible responses to the challenges of the 'trusted adviser' model do not necessarily have to be limited to choosing between accreditation and non-accreditation of trusted advisers. In this context, data enclaves have been proposed as an alternative solution[124] – and could serve as a potential temporary measure pending the outcomes of more detailed empirical research into the impact of the new rules on consumers.

[124]Financial Rights Legal Centre et al, 'Consumer Data Right Rules Amendments (Version 3) (23 July 2021) 7 <https://financialrights.org.au/wp-content/uploads/2021/07/210723_TreasuryCDRRulesUpdate_FINAL.pdf>.

9. OVERSEAS EXPERIENCE: THE UNITED KINGDOM

Direct comparisons with overseas legal frameworks in the context of the CDR are problematic, since the CDR, as an economy-wide concept, remained unique at the time of writing. Nonetheless, the wide-scale expansion of the CDR beyond open banking remains a thing for the future (see section 10 below) – which makes it appropriate to compare the current CDR framework with overseas open banking regimes. In this context, the United Kingdom likely offers the most suitable open banking regulatory structure for comparison, as it is based on mandated participation – in contrast to most other jurisdictions (where participation remains voluntary)[125] and is widely considered to be one of the most developed open banking frameworks in the world.

Open banking in the UK commenced in January 2018. It was mandated by the Retail Banking Market Investigation Order 2017 issued by the Competition and Markets Authority. The order required the nine largest banks to make their customers' banking data available to authorised third parties through secure application programming interfaces (APIs). Another important element of the open banking regulatory framework in the UK is the Payment Services Regulations 2017, which transposed the European Union's Second Payment Services Directive[126] into domestic law.

In the context of sharing customers' data, the UK open banking framework includes two notable differences compared to the CDR regime in Australia. First, it does not envisage multiple tiers of accreditation for the purposes of sharing open banking data: the only level of accreditation is provided by the UK Financial Conduct Authority in the form of 'registration as an account information service provider'.[127] Second, there are fewer restrictions on the sharing of open banking data with unaccredited third parties: recipients of customers' data do not necessarily have to be registered as account information service providers. This follows from the definition of an 'account information service', which permits a customer's 'consolidated information on one or more payment accounts' to be provided 'to another person in accordance with the payment service user's instructions'.[128] Where customer information is provided to a third party that is not an account information service provider (e.g. for the purposes of credit scoring, mortgage or loan applications), this information must also be provided to the customer. A third party recipient can then pass the customer's account data to a fourth party (also not providing account information services) – in which case the transfer is not considered a 'payment service' for the purposes of the Payment Services Regulations 2017 (although the recipients would still be subject to the personal data protection rules).[129] Finally, there is no requirement in the UK open banking framework for the transferor of a customer's open banking data to a third party to notify the financial services regulator or to be responsible for those third parties.

The recent changes to the CDR Rules concerning trusted advisers take a step in a slightly different direction – while only a narrow group of professionals is eligible to obtain access to CDR data without separate accreditation, the new rules provide for a limited integration of those professionals into the CDR framework, through the record-keeping and reporting obligations of the ADRs and the relevant CX data standards.

[125] See, eg, Association of Banking in Singapore and Monetary Authority of Singapore, 'ABS-MAS Financial World: Finance-as-a-Service API Playbook', November 2016) <https://abs.org.sg/docs/library/abs-api-playbook.pdf>; Hong Kong Monetary Authority, 'Open API Framework for the Hong Kong Banking Sector', Hong Kong, 18 July 2018) <https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2018/20180718e5a2.pdf>; Japanese Bankers Association, 'Report of Review Committee on Open APIs: Promoting Open Innovation', 13 July 2017) <https://www.zenginkyo.or.jp/fileadmin/res/news/news290713_3.pdf>; Financial Services Commission, 'Open Banking' (Web Page) <https://www.fsc.go.kr/eng/po030101>; Bank Negara Malaysia, 'Policy Document on Publishing Open Data using Open API' (Policy Document, 7 January 2019) <https://www.bnm.gov.my/-/policy-document-on-publishing-open-data-using-open-api-1>; PaymentsNZ, 'PaymentsNZ API standards', March 2019) <https://paymentsdirection.atlassian.net/wiki/spaces/PaymentsNZAPIStandards/overview>.

[126] *Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC, and 2013/36/EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64/EC. OJ L 337.*

[127] *UK Payment Services Regulations 2017,* r 17.

[128] UK Payment Services Regulations 2017, r 2.

[129] Financial Conduct Authority, 'AISP Models under PSD2' (Web Page, 21 January 2020) <https://www.fca.org.uk/firms/agency-models-under-psd2>.

10. IMPLICATIONS FOR OTHER SECTORS OF AUSTRALIAN ECONOMY

The CDR is expected to expand to other sectors in the economy, through the application of section 56AC(2) of the Competition and Consumer Act 2010 (Cth) and development of corresponding CDR regulations. Following the designation of the energy sector in June 2020,[130] the fourth version of the CDR Rules was adopted in November 2021.[131] Telecommunications has been announced as the third sector covered by the CDR: a public consultation on a corresponding designation instrument remained ongoing at the time of writing.[132]

The expected effects of further expansion of the CDR regime are substantial due to multiplicative effects of different data streams:

> 'Aggregating and correlating multiple data streams can reveal more of a customer's preferences than any one data stream or multiple data streams taken separately, and the value of the whole may be greater than the sum of its parts.'[133]

Nevertheless, some representatives of the target industries have already raised objections that are similar to those discussed previously in the context of open banking – such as 'lesser regulatory obligations' of some classes of recipients of CDR data and 'reduced regulatory oversight' under a tiered accreditation model.[134] In addition, there have been proposals to extend the CDR framework even further, for example to the automotive industry.[135]

The expansion of the CDR beyond open banking will provide new opportunities for trusted advisers already recognised in the revised CDR Rules, such as the ability of financial planners to benefit from an extension of the CDR to superannuation products.[136] Furthermore, this expansion is likely to facilitate new use cases for CDR data from different sectors of the economy – creating, in turn, new opportunities for trusted advisers. For example, '[f]inancial counsellors for hardship customers, and financial advisors may find use cases which would assess the appropriateness of an energy plan'.[137]

At the time of writing, a more detailed discussion about the implications of the rollout of the CDR in other sectors appears premature – however, it is likely that the expansion of the CDR framework will raise issues that are similar to those discussed previously in this report. More specifically, despite any prospective benefits, the recent reforms for trusted advisers have highlighted an economy-wide issue that will remain relevant for any new sector covered by the CDR framework: the need to improve the baseline level of privacy and information security. The limitations of the *Privacy Act 1988* (Cth) discussed in section eight above have prompted proposals for 'urgent economy-wide reforms for outdated protection frameworks'.[138]

In the wider economy context, as the CDR extends outside open banking, the sharing of CDR data without clearly ascertainable benefits to privacy and information security is likely to face even stronger opposition, in the light of the recent studies suggesting that '94 per cent of Australian consumers are uncomfortable with how their personal information is collected and shared online' and '88 per cent of Australian consumers do not have a clear understanding of how their personal information is being collected and shared'.[139]

[130] *Consumer Data Right (Energy Sector) Designation 2020.*

[131] *See Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021.*

[132] See Australian Treasury, 'Consumer Data Right - Telecommunications Draft Designation Instrument' (Web Page) <https://treasury.gov.au/consultation/c2021-224994>.

[133] Public Interest Advocacy Centre, 'Submission to Inquiry into Future Directions for the Consumer Data Right' (21 May 2020) 1 <https://treasury.gov.au/sites/default/files/2020-07/public-interest-advocacy-centre.pdf>.

[134] Red Energy and Lumo Energy, 'Re: Inquiry into Future Directions for the Consumer Data Right (21 May 2020) 5 <https://treasury.gov.au/sites/default/files/2020-07/red-energy.pdf>.

[135] Victorian Automobile Chamber of Commerce, 'VACC Submission: Inquiry into Future Directions for the Consumer Data Right' (23 April 2020) <https://treasury.gov.au/sites/default/files/2020-07/vacc.pdf>.

[136] Financial Planning Association of Australia, 'Inquiry into Future Directions for the Consumer Data Right' (21 May 2020) 2 <https://treasury.gov.au/sites/default/files/2020-07/fpa-australia.pdf>.

[137] EnergyAustralia, 'Inquiry into Future Directions for the Consumer Data Right' (21 May 2020) 9 <https://treasury.gov.au/sites/default/files/2020-07/energy-australia.pdf>.

[138] Consumer Policy Research Centre, 'Submission to Consumer Data Right Rules Amendments (Version 3) Exposure Draft (30 July 2021) 2 <https://cprc.org.au/publications/submission-for-consumer-data-right-amendments-version-3/>.

[139] Consumer Policy Research Centre, 'CPRC 2020 Data and Technology Consumer Survey (Web Page, 7 December 2020) <https://cprc.org.au/publications/cprc-2020-data-and-technology-consumer-survey/>.

11. CONCLUSION

Although the possibility of transferring CDR data to professional providers of advisory services to consumers was considered from the start, the early CDR designs did not permit disclosure of CDR data to non-accredited entities (other than the consumer). Nonetheless, at the time of writing the pressure to extend participation in the CDR framework remains acute, with only 23 accredited providers in operation. The 2021 CDR Amendment Rules seek to facilitate the circulation of CDR data, albeit with minimum interference with the operations of trusted advisers – by imposing most of the relevant controls on accredited data recipients instead. Despite the proposals from some groups of trusted advisers to implement a separate accreditation tier for them, the revised CDR rules established an alternative, non-accreditation pathway for trusted advisers to access CDR data.

This report has identified several practical challenges that directly or indirectly relate to trusted advisers, but several of them are particularly noteworthy.

First, the 2021 CDR Amendment Rules bring into focus the question of security of CDR data disclosed to trusted advisers and may serve as a catalyst for the adjustment (or complete elimination) of the small business exemption under the *Privacy Act 1988* (Cth) as part of the ongoing review of Australian privacy legislation (see section 8(b)).

Second, while the revised CDR framework does not establish bespoke information security controls for trusted advisers, the recent proceedings initiated by ASIC against RI Advice Group Pty Ltd over poor cyber security controls may evidence a shift towards more active enforcement of information security obligations of licensees (in particular those engaged in providing advice to consumers).[140]

Furthermore, accredited data recipients continue to serve as gatekeepers of CDR data: ADRs remain in control of the data channels they use to disclose CDR data to trusted advisers and, in the absence of a clear legal compulsion to disclose CDR data pursuant to a valid TA disclosure consent, they are likely to err on the side of caution and offer the functionality to disclose CDR data only to a limited number of trusted advisers known to them (see section 8(c)).

Third, the safe harbour provisions in rule 1.10C(3) generate uncertainty. Among other things, it is unclear whether an ADR could rely on rule 7.5(1)(ca) and argue that, as long as it can establish that the nominee is a trusted adviser *at the time of disclosure only,* the disclosure is made 'in accordance with a current disclosure consent' and, therefore, is a 'permitted disclosure'. Furthermore, the safe harbour provision is built around a 'scalable standard' that implies that verification requirements applicable to trusted advisers will be determined on a case-by-case basis, which is likely to facilitate not only an overly cautious approach by ADRs, but also delays caused by verification checks (see section 8(d)).

The recent CDR reforms targeting trusted advisers have generated opposing views from different stakeholders, from clear support to outright rejection. Regardless of any commercial and professional interests involved, however, there appears to be no meaningful opposition to the presumption that the consumer should *not* suffer any negative consequences resulting from a disclosure of CDR data to a non-accredited adviser by an ADR such as in the case of a cyber breach during the transfer of CDR data to the trusted adviser or in the event of a data incident within the trusted adviser storing the received CDR data at rest.

[140] See *Australian Securities and Investments Commission v RI Advice Group PTY LTD* (2020) FCA File Number VID556/2020.

Empirical research is needed to ascertain whether consumers understand the risks and protections available when they share their data with trusted advisers; and more specifically – whether the new CX standards for disclosures to trusted advisers facilitate consumer comprehension of the underlying risks. It is suggested that such research should avoid a 'wholesale' approach to trusted advisers (which, in itself, is an artificial category) and treat each class of trusted advisers separately to acknowledge their unique features and challenges – and to prevent unwarranted association of issues affecting only one class of trusted advisers with the remaining classes.

While the overseas open banking experiences are not illustrative (as very few jurisdictions have implemented mandated open banking in the first place) and the CDR framework remains unique, Australia has little overseas evidence to rely on when choosing the way forward in shaping its economy-wide CDR. Nonetheless, it is conceivable that some of the challenges associated with the sharing of data with unaccredited third parties will remain relevant in other sectors – in particular the need to promote privacy and information security regardless of the type of recipient of CDR data.