# NEW WAYS TO REINFORCE CONSUMER TRUST IN AUSTRALIA'S CONSUMER DATA RIGHT

ANTON DIDENKO*

*While Australia's Consumer Data Right ('CDR') legal framework has been hailed as 'the biggest reform to consumer law in a generation', there is no accepted measure or benchmark against which its efficiency can be evaluated. This article builds on the analysis performed by the author in the companion article published in the same issue and argues that the concept of 'consumer trust' can be used as a signpost of the CDR's success. It establishes consumer trust as a key enabler of social change envisaged by the CDR, performs a retrospective analysis of the factors which inhibit consumer trust in the current CDR framework and proposes legal reforms that should help overcome them. This article argues that some of the underlying challenges can only be more effectively addressed via economy-wide legal reforms, including an introduction of prescribed data transmission channels for transfers of valuable data (except between individual consumers). It is hoped the proposals formulated in this article will inform future reform directions for the CDR and consumer policy more generally.*

> To remain faithful to its original intent of providing benefit to Australian consumers, the CDR will need to have the flexibility and adaptability to harness opportunities and manage the risks of an evolving data economy.[1]

## I INTRODUCTION

Australia's Consumer Data Right ('CDR') legal framework has been hailed as 'the biggest reform to consumer law in a generation'.[2] Over the period of just several years since its launch, the CDR regime became the subject of several consultations

* Senior Lecturer, Faculty of Law and Justice, UNSW Sydney, NSW, Australia. MJur (Oxford), DPhil (Oxford). Email: anton.didenko@unsw.edu.au; ORCID ID: 0000-0003-0320-3404.

This research was funded by the Australian government through the Australian Research Council Laureate Fellowship of Ross Buckley (FL200100007: 'The Financial Data Revolution: Seizing the Benefits, Controlling the Risks'). The views expressed herein are those of the author and are not necessarily those of the Australian government or Australian Research Council. I am grateful to Ross Buckley, Scott Farrell and the anonymous reviewers for their invaluable comments. All errors are mine alone.

1 Elizabeth Kelly, 'Statutory Review of the Consumer Data Right' (Issues Paper, March 2022) 11.

2 Angus Taylor, 'Australians to Own Their Own Banking, Energy, Phone and Internet Data' (Media Release, Parliament of Australia, 26 November 2017).

seeking to refine the framework.[3] The Australian government has responded to these inquiries with legal reform initiatives[4] and a statutory review of the CDR regime pursuant to s 56GH of the *Competition and Consumer Act 2010* (Cth) ('*CCA*').[5] These developments demonstrate that the CDR is supported by a legal scaffolding that is both flexible and dynamic: the CDR is subject to periodic reviews and amendments to better achieve its objectives.[6]

To date, these revisions have led to the expansion of the CDR framework, both horizontally (by extending the CDR beyond the banking sector)[7] and vertically (by establishing new accreditation tiers and allowing certain unaccredited persons to act as recipients of CDR data).[8] This status quo is understandable: greater access by businesses is expected to increase the supply of services utilising CDR data and promote competition among service providers.[9]

Despite the continuous expansion of the CDR ecosystem, there is considerable uncertainty regarding its overall performance. This uncertainty is underpinned by the low amounts of reliable statistical information about the level of consumer engagement and the fact that the government has not formulated clear, measurable success criteria against which the CDR could be evaluated. This is reflected in recommendation 1.5 of the *Statutory Review of the Consumer Data Right* ('*Statutory Review*'):

3 See, eg, Treasury (Cth), 'Inquiry into Future Directions for the Consumer Data Right' (Issues Paper, March 2020); Senate Select Committee on Financial Technology and Regulatory Technology, Parliament of Australia, *Interim Report* (Report, September 2020) ch 5 ('*Senate Select Committee Interim Report*'); Senate Select Committee on Australia as a Technology and Financial Centre, Parliament of Australia, *Second Interim Report* (Report, April 2021) ch 3.

4 Treasury (Cth), *Government Response to the Inquiry into Future Directions for the Consumer Data Right* (Report, December 2021); Treasury (Cth), *Australian Government Response to: the Review of the Australian Payments System and the Senate Committee on Australia as a Technology and Financial Centre: Final Report and the Parliamentary Joint Committee Corporations and Financial Services Report: Mobile Payment and Digital Wallet Financial Services* (Report, December 2021).

5 Elizabeth Kelly, *Statutory Review of the Consumer Data Right* (Report, 2022).

6 Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth) 38 [1.202] ('2019 Explanatory Memorandum').

7 *Consumer Data Right (Energy Sector) Designation 2020* (Cth) ('*CDR (Energy Sector) Designation*'); *Consumer Data Right (Telecommunications Sector) Designation 2022* (Cth) ('*CDR (Telecommunications Sector) Designation*'); *Consumer Data Right (Non-Bank Lenders) Designation 2022* (Cth) ('*CDR (Non-Bank Lenders) Designation*').

8 See *Competition and Consumer (Consumer Data Right) Amendment Rules (No 1) 2021* (Cth) schs 1–3 ('*2021 CDR Amendment Rules*'); *Competition and Consumer (Consumer Data Right) Amendment Rules (No 1) 2023* (Cth) sch 1 item 12 ('*2023 CDR Amendment Rules*'), inserting *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) rr 1.10A(9)–(11) ('*CDR Rules*').

9 See, eg, James Eyers, 'Extension to Open Banking Rules Will Boost Participation: CDR Players', *Australian Financial Review* (online, 8 October 2021) <https://www.afr.com/companies/financial-services/extension-to-open-banking-rules-will-boost-participation-cdr-players-20211008-p58ybm>.

> Greater visibility of success measures and system objectives will provide increased confidence and assurance to participants. Success measures should incorporate measures of system health and meaningful outcomes for consumers.[10]

A better understanding of the effects the CDR framework have had on service providers and consumers can help identify its deficiencies and inform future reform directions. Development of appropriate evaluation criteria is challenging since the stated objectives of the CDR are not sufficiently specific. This article argues that the concept of 'consumer trust', which was the focus of a separate article,[11] could serve as a useful signpost of the CDR's success and then proposes a range of reforms that should enable a more balanced CDR framework that treats consumer trust as a central element of its legal design.

## II METHODOLOGY AND STRUCTURE

Legislative legal reform is recognised in legal scholarship as an area particularly suited for multidisciplinary analysis, considering that the underlying problems 'have a practical as well as a theoretical dimension'.[12] The complex interplay of different elements of modern legislative studies is reflected in the concept of 'legisprudence', which 'aims at furthering the theoretical understanding as well as the technical handling of legislation'.[13] From this perspective, there is no single 'correct way' to study legislative reforms: legisprudence 'combines elements of science, art and craftsmanship [and] concerns both the content of legislation and its form'.[14]

This article focuses on the CDR as a complex legislative framework to reduce the uncertainty regarding its success metrics, as recently highlighted by the *Statutory Review*, which calls for '[g]reater visibility of *success measures*'[15] to boost confidence among the participants. In legal scholarship, this challenge is associated with *evaluation* — an 'essential part of legislative methodology' that is mostly concerned with the substantive (rather than formal) aspects of legal reforms and in particular its key analytical steps: (i) 'retrospective evaluation' and (ii) 'adaptation of legislation'.[16]

Evaluation is inherently pragmatic, as it is concerned with the *effects* of legal reforms. It seeks to 'produce more relevant and more accurate information about

10 Kelly (n 5) 29.

11 Anton Didenko, 'Australia's Consumer Data Right and Its Implications for Consumer Trust' (2024) 50(1) *Monash University Law Review* 61.

12 Luzius Mader, 'Evaluating the Effects: A Contribution to the Quality of Legislation' (2001) 22(2) *Statute Law Review* 119, 119.

13 Ibid.

14 Ibid.

15 Kelly (n 5) 28 (emphasis added).

16 Mader (n 12) 121–2.

the potential or actual causal relationships between legislative action and observable social attitude, behaviour or circumstance'.[17] At the same time, the *complexity* of social causality implies that '[i]n most cases, it cannot be proven in a strict sense'.[18] Hence, in the light of the inherent limitations of the method, its main focus is to ensure that the legislators' *assumptions about the causal relations* underlying the legislative frameworks 'are based on the best possible theoretical basis'.[19] In this article, the evaluation focuses on the theoretical basis for measuring the success of the CDR regime and seeks to 'improve the legislator's assumptions and knowledge about the effects of legislation'.[20]

The focus of this article will be on *efficacy* as the main evaluation criterion. I follow Mader's simple but elegant definition of efficacy, as 'the extent to which legislative action achieves its goal'.[21] This analysis is facilitated by the express formulations of the legislator's intent against which the CDR can be evaluated. At the same time, this article does not engage in evaluation of the CDR framework on a more technical level, such as by reference to the *efficiency* or *effectiveness* of legislation as separate evaluation criteria distinguished by scholars.[22] The article readily acknowledges that '[t]he achievement of a policy objective or purpose is not the sole task of the drafter'[23] but deems efficacy-focused analysis an appropriate starting point for defining the success metrics of the CDR framework, which hopefully will be supplemented by additional criteria developed by other authors. For this article, I accept the proposition that efficacy is the 'highest virtue in the policy process'[24] and argue it is a key factor in defining the measures of success for the CDR.

I start my analysis in Part III with a brief overview of the CDR framework and establish the assumptions underlying the expected change in the attitudes of consumers in response to the implementation of the CDR. I conclude that this change is predicated on the existence of consumer trust in the CDR legal framework. Part IV then outlines the key factors that inhibit consumer trust — and, by implication, impact the validity of the above assumptions. This discussion is informed by the more detailed analysis in a separate publication,[25] and constitutes

17 Ibid 123.

18 Ibid.

19 Ibid 124.

20 Ibid.

21 Ibid 126.

22 See, eg, Helen Xanthaki, 'On Transferability of Legislative Solutions: The Functionality Test' in Constantin Stefanou and Helen Xanthaki (eds), *Drafting Legislation: A Modern Approach* (Routledge, 2016) 1, 4–9. Xanthaki distinguishes several levels of the 'hierarchy of virtues served by the drafter' of legislation (from top to bottom): (i) efficacy, (ii) effectiveness, (iii) efficiency, clarity, precision, unambiguity and (iv) simplicity/plain language and gender-neutral language: at 17.

23 Ibid 5.

24 Ibid.

25 Didenko (n 11).

'retrospective evaluation'. Part V sets out proposals to enable the CDR to address the above inefficiencies, as the final step of evaluation in legisprudence ('adaptation of legislation'). Part VI summarises the conclusions.

## III CONSUMER TRUST AS A CRITERION OF CDR SUCCESS

### A *An Outline of the CDR Framework*

The CDR framework focuses on expanding the circulation of a wide range of prescribed types of consumer data ('CDR data') in designated sectors of Australia's economy through specified data transmission pathways, subject to consumers' consent and under regulatory supervision.

The origins of the CDR in Australia can be traced back to the 2017 Productivity Commission report, *Data Availability and Use*, which proposed to empower consumers by establishing 'a new Comprehensive Right to the use of their digital data'.[26] The CDR was formally launched on 1 July 2020, following a detailed analysis of different design and policy options for Australia's open banking regime prepared by Scott Farrell.[27] The regulatory structure of the framework includes several instruments: (i) the *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth), (ii) the *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) ('*CDR Rules*') and (iii) the standards made by the Data Standards Chair (with assistance from the Data Standards Body).[28] From the start, the CDR was conceived as a multisectoral legal framework (as opposed to open banking regimes overseas) — and thus the implementation in the banking sector[29] was only the first step in its gradual rollout across the Australian economy, which followed shortly afterwards in the form of additional sectoral designations in 2020 and 2022.[30]

In general terms, the key aspect of the CDR framework is the interaction between two CDR participants,[31] namely (i) a 'data holder'[32] (such as a bank)[33] which holds CDR data and must transfer that data pursuant to a consumer's request and

26 Productivity Commission, *Data Availability and Use* (Report No 82, 31 March 2017) 15.

27 Scott Farrell, *Review into Open Banking: Giving Customers Choice, Convenience and Confidence* (Report, December 2017).

28 *Competition and Consumer Act 2010* (Cth) ss 56FH, 56FK ('*CCA*').

29 *Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019* (Cth).

30 *CDR (Energy Sector) Designation* (n 7); *CDR (Telecommunications Sector) Designation* (n 7); *CDR (Non-Bank Lenders) Designation* (n 7).

31 The term 'CDR participant' is defined in *CCA* (n 28) s 56AL(1).

32 As defined in ibid s 56AJ(1).

33 Within the banking sector, 'data holders' include all authorised deposit-taking institutions: *Banking Act 1959* (Cth) ss 5(1) (definition of 'authorised deposit-taking institution'), 9(3) ('*Banking Act*').

(ii) an 'accredited data recipient' ('ADR')[34] which receives CDR data and must be accredited for that purpose. Accreditation is performed by the Data Recipient Accreditor — the Australian Competition and Consumer Commission.[35]

## B *Centrality of Consumer Trust in the CDR Framework*

The goals of the CDR regime, like any other legal framework, could be evaluated by reference to its stated objectives. These are set out in s 56AA of the *CCA* as follows: (i) 'to enable consumers in certain sectors of the Australian economy to require information relating to themselves in those sectors to be disclosed safely, efficiently and conveniently' to themselves or to accredited persons, (ii) 'to enable any person to efficiently and conveniently access information in those sectors' about goods or services, and, on the basis of the first two enablers, (iii) 'to create more choice and competition, or to otherwise promote the public interest'.

These objectives helpfully articulate how the CDR legal framework is expected to generate social impact. First, its focus on *enabling* a shift in consumers' behaviour seeks to change how consumers treat their valuable (eg banking) data held by service providers in designated sectors. Since it does not force consumers to use the new system, consumers are expected to choose the CDR *voluntarily*. Second, in order to persuade consumers to choose the CDR framework, the latter introduces several features of CDR data transfer that seek to boost consumer trust (safety, efficiency and convenience).[36]

It follows that consumer trust is a key enabler of the social change envisaged by the CDR framework. This conclusion is supported by the analysis of other materials that may be used to establish the legislature's intent. The concept of consumer trust is at the centre of the CDR framework in Australia, considering its origins in open banking: 'In some respects, Open Banking is a simple concept — it is about giving customers the ability to instruct that their banking data be securely shared with *parties they trust* to unlock the value in that data.'[37] Furthermore, consumer trust is the centrepiece of one of the four guiding principles of Australia's open banking — namely its focus on consumers:

> An important component of this customer focus is that all participants feel justifiably confident in the system. Customers and other participants *will not engage* with a system that they *do not trust*. Trust includes knowing that customer data will remain protected, that any breach will be remedied, and that a system customers have integrated into their lives will remain stable and accessible.[38]

34 As defined in *CCA* (n 28) s 56AK.

35 'Consumer Data Right', *Treasury* (Web Page) <https://treasury.gov.au/policy-topics/economy/consumer-data-right>; 'The Consumer Data Right', *Australian Competition and Consumer Commission* (Web Page) <https://www.accc.gov.au/by-industry/banking-and-finance/the-consumer-data-right>; *CCA* (n 28) ss 56CA, 56CG.

36 See *CCA* (n 28) s 56AA.

37 Farrell (n 27) 8 (emphasis added).

38 Ibid (emphasis added).

The ubiquitous influence of consumer trust on the performance of the entire CDR ecosystem makes it a useful measure of success of the underlying legal framework. As a measure of success, consumer trust could helpfully address both priorities identified in recommendation 1.5 of the *Statutory Review*. On the one hand, it can be used as a 'measure[] of system health',[39] considering that consumer trust in the CDR framework has an 'institutional, impersonal nature'.[40] On the other hand, consumer trust reflects consumer perception of the CDR and thus can serve as an indicator of 'meaningful outcomes for consumers'.[41]

Several observations need to be made before proceeding further with the analysis.

As highlighted in the companion article,[42] the CDR framework applies to a broad range of 'CDR consumers'.[43] Some of them — in particular 'CDR business consumers' — are deemed more sophisticated and thus enjoy broader powers to share their CDR data with unaccredited persons.[44] Others — namely most individual consumers — are subject to additional restrictions and, importantly, are more likely to lack the capacity to manage their risks associated with the CDR framework and thus would benefit the most from additional legal protections.

Using consumer trust as a signpost of CDR's success invites a holistic approach and consideration of multiple factors. As an example, the use of empirical data to gauge the level of consumer engagement can help us understand how often and how many consumers have interacted with the CDR ecosystem — but does little to identify the underlying risks and complex interdependencies that affect consumer perception as *prerequisites* of consumer trust.[45] Raw empirical data is unlikely to be sufficient to establish the reasons for low levels of consumer engagement to plan future reform.

In addition, consumer trust is a dynamic concept,[46] and multiple factors may affect the degree of trust of consumers in the CDR framework, which may change over time.

*First*, there is a demonstrated trust crisis among consumers in Australia's economy. Major trust issues in Australia's financial system originate from (i) the global financial crisis, (ii) the Royal Commission into Misconduct in the Banking,

39 Kelly (n 5) 29.

40 Didenko (n 11) 72 (emphasis omitted).

41 Kelly (n 5) 29.

42 Didenko (n 11) 70–1.

43 Section 56AI(4) of the *CCA* (n 28) disapplies s 4B.

44 See *2023 CDR Amendment Rules* (n 8) sch 1 item 12, inserting *CDR Rules* (n 8) rr 1.10A(9)–(11). There is a caveat: CDR representatives are not permitted to deal with CDR business consumers under the *CDR Rules* (n 8) r 1.10AA.

45 Didenko (n 11) 72–3.

46 Denise M Rousseau et al, 'Not So Different after All: A Cross-Discipline View of Trust' (1998) 23(3) *Academy of Management Review* 393, 396.

Superannuation and Financial Services Industry,[47] and (iii) the problems in Australia's financial advice industry,[48] among other factors. The extraordinary string of high-profile cyber breaches across Australia in the second half of 2022 affecting, among others, some of the largest telecommunications operators (Optus),[49] private health insurers (Medibank)[50] and retail chains (Woolworths)[51] further undermined consumers' trust[52] in how their data is handled even by the largest, highly sophisticated *trusted* entities — pushing the government to propose urgent legislative changes dramatically increasing penalties for data breaches.[53]

*Second*, consumers in highly complex areas of financial regulation generally do not have the capacity to verify the trustworthiness of the product, service or their originator/provider. As a result, consumers may trust something that is not trustworthy (and vice versa).

*Third*, even where consumers know that a product or service (or their originator/provider) is not trustworthy, they may still knowingly continue to use it if (i) there is no meaningful alternative and/or (ii) the perceived benefits greatly outweigh the known risks.

These issues highlight the complex nature of consumer trust in the CDR framework but do not undermine its usefulness as a measure of CDR success. Having established the relevance of consumer trust, let us now turn to a retrospective analysis of the factors which inhibit consumer trust in the current CDR framework — before proposing reforms that should help overcome them.

47 *Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry* (Final Report, 1 February 2019).

48 See, eg, Australian Securities and Investments Commission, *Financial Advice: Vertically Integrated Institutions and Conflicts of Interest* (Report No 562, January 2018) 36 [137]–[141] ('*ASIC Report 562*'); Australian Securities and Investments Commission, *Financial Advice by Superannuation Funds* (Report No 639, December 2019) 30–1 [109]–[113] ('*ASIC Report 639*').

49 'Optus Data Breach', *Cyber and Infrastructure Security Centre* (Web Page, 30 September 2022) <https://www.cisc.gov.au/news-media/archive/article?itemId=945>.

50 'Medibank Private Limited and AHM Cyber Incident', *Department of Home Affairs* (Web Page, 21 October 2022) <https://www.homeaffairs.gov.au/news-media/archive/article?itemId=961> ('Medibank Cyber Incident').

51 'OAIC Statement on MyDeal Data Breach', *Office of the Australian Information Commissioner*, (Web Page, 15 October 2022) <https://www.oaic.gov.au/newsroom/oaic-statement-on-mydeal-data-breach> ('MyDeal Data Breach').

52 One empirical study recorded a '10.5 per cent decline in the average trust in telecommunications companies between August and October 2022': Nicholas Biddle, Matthew Gray and Steven McEachern, 'Public Exposure and Responses to Data Breaches in Australia: October 2022' (Research Paper, Centre for Social Research and Methods, Australian National University, 8 November 2022) 8.

53 See *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Cth) sch 1 items 13–14.

## IV AN OVERVIEW OF THE INHIBITORS OF CONSUMER TRUST IN AUSTRALIA'S CDR REGIME[54]

The principal factors that might undermine consumer trust in Australia's CDR framework can be summarised as follows.

### A *Disclosure to 'Trusted Advisers'*

Contrary to the original design of the CDR, the 2021 expansion of the CDR framework enabled several groups of professional service providers called 'trusted advisers'[55] to receive CDR data *without obtaining CDR accreditation*. This change was based on an assumption that disclosure of CDR data to unaccredited recipients operating outside the CDR ecosystem should be acceptable as long as those recipients are members of 'professions that are considered to be appropriately regulated to receive CDR data, particularly due to consumer protection mechanisms that form part of their regulatory framework'.[56] In other words, the CDR framework treats all 'trusted advisers' as trustworthy by definition, by virtue of their professional status — regardless of their size or type of business.

This conclusion appears flawed for several reasons.

First, the effectiveness of consumer protections applied by different types of 'trusted advisers' cannot be taken for granted — as illustrated by major compliance failures recorded in recent years. As an example, the Australian Securities and Investments Commission's ('ASIC') 2018 study found that in 75% of reviewed cases the adviser failed to demonstrate compliance with the best interests duty.[57] In another study, the number of noncompliant advisers exceeded 50%.[58] Furthermore, the mere existence of professional rules, codes and standards that may apply to different types of 'trusted advisers' is not per se sufficient evidence of the effectiveness of these instruments. This was well illustrated by ASIC's first ever litigation against an Australian Financial Services ('AFS') licence holder, RI Advice Group Pty Ltd,[59] over poor cybersecurity controls that brought to light the

54 This discussion is based on a more detailed analysis in Didenko (n 11).

55 *2021 CDR Amendment Rules* (n 8) sch 3 item 5, inserting *CDR Rules* (n 8) r 1.10C. These include (i) *qualified accountants* within the meaning of the *Corporations Act 2001* (Cth) ('*Corporations Act*'), (ii) persons admitted to the *legal profession*, (iii) registered *tax agents*, *BAS agents* and *tax (financial) advisers* within the meaning of the *Tax Agent Services Act 2009* (Cth), (iv) *financial counselling agencies* within the meaning of the *ASIC Corporations (Financial Counselling Agencies) Instrument 2017/792* (11 February 2022), (v) 'relevant providers' within the meaning of the *Corporations Act* (n 55) and (vi) *mortgage brokers* within the meaning of the *National Consumer Credit Protection Act 2009* (Cth).

56 Explanatory Statement, Competition and Consumer (Consumer Data Right) Amendment Rules (No 1) 2021 (Cth) 18 ('2021 Explanatory Statement').

57 *ASIC Report 562* (n 48) 36 [137].

58 *ASIC Report 639* (n 48) 30 [110].

59 *Australian Securities and Investments Commission v RI Advice Group Pty Ltd* (2022) 160 ACSR 204.

limitations of the vaguely drafted statutory obligations found in s 912A(1)(a) of the *Corporations Act 2001* (Cth) (which requires AFS licensees to 'do all things necessary to ensure that the financial services covered by the licence are provided efficiently, honestly and fairly'). The provision was interpreted to include cybersecurity obligations, the scope of which, however, appeared rather difficult to ascertain *ex ante*.[60] The resulting uncertainty hardly reinforces the trustworthiness of 'trusted advisers' that require an AFS licence.

Second, consumers (in particular, individuals) generally do not (and arguably should not be expected to) possess sufficient technical knowledge to verify compliance of trusted advisers with the relevant rules, codes and standards.

Third, professional advisers are a source of *specialist knowledge and expertise*. As a result, some commentators have suggested 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'.[61] In other words, the fact that consumers routinely engage the services of 'trusted advisers' can be attributed to necessity (resulting from the lack of real choice), rather than genuine informed satisfaction with the consumer protections afforded by such professionals.

Fourth, the exclusivity of services offered by 'trusted advisers' creates a bigger systemic issue: the CDR framework does not create any incentives for trusted advisers to compete among themselves (eg, in terms of information security) — since the CDR regime adopts a hands-off approach to the consumer protections implemented by these professionals and consumers cannot rely on CDR accreditation as evidence of sufficient credibility of trusted advisers.

Finally, trusted advisers who receive CDR data remain untouchable by the CDR penalties applicable to CDR participants, since they do not require authorisation and therefore are not technically accredited persons for the purposes of the CDR. This status quo *obscures* one of the basic underlying elements of the CDR — accountability of the recipients of CDR data.[62]

## B *Information Security and Privacy Risks*

The absence of bespoke information security obligations for 'trusted advisers' tapping into the CDR data transmission channels has led the Australian Banking Association to conclude that '[w]ithin seconds … a customer's data will travel from *the most secure setting at the bank* to *no or uncertain security with Trusted Advisers*'.[63] A deeper analysis shows that this conclusion has merit. Indeed, the *CDR Rules* impose information security obligations on ADRs — but not on

60 Ibid 214–15 [46]–[47], 217 [65] (Rofe J).

61 Financial Rights Legal Centre, Submission to Australian Competition and Consumer Commission, *CDR Rules Expansion Amendments* (October 2020) 32.

62 2019 Explanatory Memorandum (n 6) 70 [1.414].

63 Australian Banking Association, Submission to Treasury (Cth), *Consumer Data Right Rules Amendments (Version 3)* (30 July 2021) 2 (emphasis added).

'trusted advisers'. As a result, different categories of trusted advisers are subject to their own information security rules — meaning that the *same CDR data is treated differently* depending on the type of recipient of such data (namely, ADRs, different groups of trusted advisers or unaccredited recipients of CDR data upon authorisation from CDR business consumers). This status quo, in turn, exposes the 'weakest link' problem whereby the entity with the lowest information security controls poses the greatest risks. On top of that, ADRs are not responsible for the actions or information systems of trusted advisers to whom they disclose CDR data. In the absence of formal CDR accreditation, this leaves consumers without an easily ascertainable signpost of the information security capabilities of the relevant trusted advisers.

Another important challenge in the area of information security is the continued reluctance of Australian lawmakers to abolish the practice of screen scraping. The latter is a process of gathering consumer data that involves inducing consumers to disclose their internet banking access credentials to a third party and is a source of major risks for consumers.

First, screen scraping is an inherently dangerous method of sharing consumer data that facilitates cyber breaches, regardless of the type of medium used and the types of precautions the consumer may implement[64] — while consumers resorting to screen scraping typically find themselves in breach of their financial institution's terms and conditions,[65] not to mention ASIC's *ePayments Code*, which states that users 'must not … voluntarily disclose one or more passcodes to *anyone*, including a family member or friend'.[66] In the absence of fixed standards of 'acceptable' screen scraping, consumers are essentially left to fend for themselves as financial institutions struggle to differentiate between consumer-authorised access to their banking details and illegal automation, considering the massive amounts of traffic generated by data aggregators that render standard fraud prevention measures ineffective.[67]

Second, even supporters of this practice acknowledge its fundamental deficiencies, while the seemingly neutral *Review into Open Banking: Giving Customers Choice, Convenience and Confidence* by Scott Farrell ultimately concluded that open banking 'should aim to make this practice redundant'[68] and the recent *Statutory*

64 See, eg, Jeffrey Voas et al, National Institute of Standards and Technology, *Cybersecurity Considerations for Open Banking Technology and Emerging Standards* (Draft Internal Report 8389, January 2022) 13.

65 Reserve Bank of Australia, Submission to Treasury (Cth), *Inquiry into Future Directions for the Consumer Data Right* (23 April 2020) 3.

66 Australian Securities and Investments Commission, *ePayments Code* (2 June 2022) cl 12.2(a) (emphasis added).

67 Olov Renberg, 'Fintech Aggregators and Open Banking: Service Enablers or an Unfortunate Backdoor for Fraud?', *BehavioSec* (Blog Post, 8 December 2021) (emphasis omitted), archived at <https://web.archive.org/web/20220811200827/https://www.behaviosec.com/fintech-aggregators-and-open-banking-service-enablers-or-an-unfortunate-backdoor-for-fraud/>.

68 Farrell (n 27) x.

*Review* stated that '[s]creen scraping should be banned in the near future in sectors where the CDR is a viable alternative'.[69]

Finally, the retention of screen scraping creates perverse incentives for businesses offering data capture services, as it generates no stimuli to innovate or improve their information security practices. This is one of the reasons for the unfortunate status quo, whereby such businesses lobby ASIC to take no further action against screen scraping on the basis that the CDR

> is not yet at a stage where it is considered by the industry as a viable alternative offering to 'screen scraping' and other forms of digital data capture of such value as to outweigh the regulatory costs of participating in the CDR framework.[70]

## C *Limitations of Consumer Compensation Mechanism*

The CDR framework seeks to facilitate the sharing of valuable CDR data across a wider range of recipients. Despite the importance of *ex ante* protections aiming to prevent unauthorised access to such valuable data, it is no less important to consider the types of redress available to consumers *ex post* — ie after the incident, when those protections have already failed for one reason or another. The main consumer redress in this post-breach scenario is the *statutory right of action*: a person who suffers loss or damage by an act or omission of another person in contravention of the privacy safeguards established by the CDR or the consumer data rules 'may recover the amount of the loss or damage by action against that other person or against any person involved in the contravention'.[71] This type of redress appears poorly suited for individual consumers, considering major inequalities in bargaining power and information asymmetries between such consumers (who have very limited capacity to identify unreported data breaches and verify reported data breaches of ADRs) and other CDR participants. A framework that exists to induce consumers to share valuable data about themselves *more frequently* and *with more businesses* but does not propose a better solution than telling consumers to fend for themselves in court seemingly assumes that consumers impacted by the CDR will make the rational decision not to waste time, money and energy on obtaining compensation — which hardly makes for a defensible proposition to promote consumer trust.

In addition, consumers obtain only a limited benefit from the legal requirement for accredited persons to 'have adequate insurance, or a comparable guarantee, in light of the risk of CDR consumers not being properly compensated for any loss that might reasonably be expected to arise from a breach of obligations'[72] under the CDR framework. Indeed, unlike the financial claims scheme in banking, which guarantees that account-holders will recover their deposit (up to the maximum

69 Kelly (n 5) 12.

70 Australian Securities and Investments Commission, *Response to Submissions on CP 341 Review of the ePayments Code: Further Consultation* (Report No 718, March 2022) 34 [115].

71 *CCA* (n 28) ss 56EY(1), 82(1).

72 *CDR Rules* (n 8) r 5.12(2)(b).

statutory limit),[73] mandatory CDR insurance protects *ADRs themselves* by allowing them to claim under the insurance policy to increase the amount of funds available to the ADR to satisfy consumers' claims: 'Insurance will protect the financial position of the accredited person by preserving their ability to meet their liabilities and to *guard against their insolvency*.'[74] As the accredited person remains the beneficiary, the consumer cannot claim directly against the insurer.[75] As a result, to obtain compensation, consumers have to rely on the accredited person's ability to remain solvent — with seemingly no meaningful protections available in the event of bankruptcy.

## D *No Mechanism for Sharing CDR Data Directly with Consumers*

Despite the statutory objective to enable consumers to disclose data about themselves safely, efficiently and conveniently '*to themselves* for use as they see fit',[76] consumers cannot request and receive CDR data directly as the necessary standards have not been developed. In 2021, the Treasury announced a deferral of the 'direct to consumers' pathway for CDR data 'pending a future consultation process'.[77] Subsequently, the 2022 *Statutory Review* recognised that the framework remains insufficiently mature to permit direct disclosures to consumers: 'As the CDR matures, the risks associated with direct-to-consumer data sharing may decrease, at which point enabling data transfers should be reconsidered.'[78] This status quo is unfortunate, considering the resulting loss of opportunity to promote consumer trust (by enabling consumers to receive a copy of CDR data[79] and verify its accuracy).[80] However, perhaps more importantly, the resulting delay acts as clear evidence of the magnitude of the risks associated with enabling unsophisticated parties, such as individual consumers, to access CDR

73 See *Banking Act* (n 33) ss 16AF–16AG.

74 Australian Government, *Supplementary Accreditation Guidelines: Insurance* (Guidelines, December 2022) 2 (emphasis added).

75 Australian Securities and Investments Commission, *Compensation and Insurance Arrangements for AFS Licensees* (Regulatory Guide 126, July 2022) 9 [23].

76 *CCA* (n 28) s 56AA(a)(i) (emphasis added).

77 Treasury (Cth), 'Developments in Australia's Consumer Data Right in Response to Community Feedback' (Media Release, 30 April 2021).

78 Kelly (n 5) 7.

79 Once CDR data is shared with an ADR, the Australian Privacy Principles ('APPs') no longer apply and the consumer is unable to rely on APP 12. If the relevant data is held by the data holder and has not been shared, the consumer could, in principle, make use of APP 12 to access personal information — but that request will not be supported by the CDR ecosystem (including dedicated secure data transmission channels and machine-readable format of consumer data). On the interplay between the APPs and privacy safeguards under the CDR, see generally Mark Burdon and Tom Mackie, 'Australia's Consumer Data Right and the Uncertain Role of Information Privacy Law' (2020) 10(3) *International Data Privacy Law* 222.

80 The ability to control one's own information goes to the heart of the concept of 'privacy'. As an example, Altman defines privacy as 'selective control of access to the self or to one's group': Irwin Altman, 'Privacy: A Conceptual Analysis' (1976) 8(1) *Environment and Behavior* 7, 8.

data. Yet instead of addressing those risks, the relevant functionality of the CDR is simply disabled, seemingly indefinitely.

## E *Safe Harbours to Protect Service Providers*

In an attempt to offer additional legal certainty to service providers participating in the CDR framework, the latter incorporates 'safe harbour' provisions that grant immunity to any proceedings (whether civil or criminal) to any CDR entity, as long as such entity acts in good faith in compliance with the CDR legal framework.[81] While protection of service providers' interests is a valid regulatory objective, from a consumer perspective the key concern is who bears the risks whenever the relevant provider causes damage to consumers despite formally satisfying the 'safe harbour' criteria.[82] This issue is best illustrated by a fiction adopted in the *CDR Rules*:

> 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.[83]

The 'safe harbour' provides comfort to accredited persons, who may escape liability in the event of disclosure of CDR data to a wrong person simply by exercising reasonable efforts. The fact that despite those reasonable efforts valuable consumer data may end up in the hands of an unauthorised, even malicious, entity is of little relevance, meaning that in this case consumer interests end up subordinated to the interests of service providers. As a result, the *residual risks are borne by consumers* who have little capacity to verify compliance by accredited persons with their obligations and are 'unlikely to know whether a particular action by an entity breaches their privacy rights'.[84]

## F *Limited Consumer Awareness*

While the empirical evidence concerning the level of consumer participation in the CDR framework remains limited, publicly available data indicates low levels of consumer awareness.[85] This unfortunate result is likely caused by the substantial regulatory complexity of the CDR regime, which makes *genuinely informed* engagement with the framework seemingly out of reach of non-expert consumers for a number of reasons.

81 *CCA* (n 28) s 56GC(1).

82 For a more comprehensive analysis of the safe harbour provisions in the CDR framework, see Anton N Didenko, *Implications of the Consumer Data Right Framework for Trusted Advisers* (Report, 2022) 23–6.

83 *CDR Rules* (n 8) r 1.10C(3) (emphasis added).

84 Maddocks, 'Australian Competition and Consumer Commission: Consumer Data Right Regime' (Consultation Paper, October 2020) 45.

85 Natalia Jevglevskaja and Ross P Buckley, 'The Consumer Data Right: How to Realise This World-Leading Reform' (2022) 45(4) *University of New South Wales Law Journal* 1589, 1620.

First, consumers need to be aware of the 'boundary problem'. On the one hand, the differences in the regulation of consumer data within the CDR and outside this framework are significant. Therefore, consumers need to understand where the boundaries of the CDR lie. On the other hand, the boundaries of the CDR are not easily ascertainable: the *same* CDR data is regulated and protected *differently*, depending on whether the law treats it as being subject to the CDR regime or not. To be clear, the nature of CDR data transferred to trusted advisers does not change — the CDR framework simply stops operating once that data reaches the relevant adviser. Similar issues arise in the context of disclosures to unaccredited entities authorised by CDR business consumers.[86]

Second, as noted previously, the CDR regime uses complex and potentially misleading terminology — as illustrated by the recently added 'trusted adviser' concept, which is unhelpful due to its connotation that the relevant professional service providers are by definition trustworthy. Another example is the use of the word 'consumer' in the CDR framework to cover essentially all kinds of customers — which may be misinterpreted by stakeholders relying on the 'general' definition of 'consumer' found in the *CCA*.[87]

Third, consumer redress mechanisms exercisable following unauthorised access to CDR data remain time- and resource-intensive (considering the need to bring an action against the relevant business for every breach) and have limited usefulness for the consumer (considering the limitations of mandatory insurance).

Fourth, consumers (especially individuals) interacting with the CDR framework are likely to do so on the basis of very limited understanding of how the CDR regime may operate to the consumer's detriment — such as in the event 'safe harbour' provisions apply to the extent that CDR data may be lawfully misused without any liability to the consumer. This unfortunate status quo challenges the assumption that consumer consent under the CDR is 'informed'.[88]

The overall dynamic of the CDR framework seems to point towards increasing complexity (considering the post-launch reforms) — which is likely to continue to erode consumers' trust.

## V REFORM PROPOSALS TO BOOST CONSUMER TRUST

The focus on consumer trust adopted in this article — as opposed to other factors, such as economic interests of service providers — invites a consumer-focused approach to addressing the challenges identified in Part IV. Several key observations should be made upfront.

86 See *2023 CDR Amendment Rules* (n 8) sch 1 item 12, inserting *CDR Rules* (n 8) r 1.10A(11).

87 *CCA* (n 28) s 4B(1), sch 2 s 3.

88 *CDR Rules* (n 8) r 4.9(c).

*First*, the focus of the proposed reforms is on minimising the risks for consumers, without assessing the impact on other participants (such as the impact of proposed measures on the economic interests of providers of screen scraping services).

*Second*, considering that the CDR operates at the intersection of competition law, consumer (protection) law and data protection and privacy law, the analysis should — where workable — consider the feasibility of utilising other existing legal frameworks to address the relevant challenges. This is particularly important where the CDR creates implications that cannot be easily isolated and confined to the CDR alone (such as where CDR data is shared with unaccredited persons). This Part V acknowledges that — while the CDR might benefit from certain adjustments — a more efficient solution to the relevant challenges may require outside-the-box thinking and may need to *extend outside the CDR boundaries*.

*Third*, given the dynamic nature of consumer trust, legal reforms can take multiple stages, starting with the more easily achievable initiatives — and gradually proceeding towards more ambitious reforms. Accordingly, alternative approaches need to be considered, where relevant.

## A *Protect All Kinds of Consumer Data as Valuable Data*

The need to protect consumers' data had been acknowledged by scholars prior to the launch of the CDR in Australia: 'It is unsafe to promote a revolutionary increase in the exposure of the personal information of Australians without proportionate increases in the legal protection of that personal information.'[89] Furthermore, research indicates that individual data incidents could have negative implications on trust in the entire CDR ecosystem, since 'collectively very large data breaches have the potential to undermine trust in the system as a whole, rather than just individual companies'.[90]

The subsequent expansion of the CDR framework outside the banking sector, the 'trusted adviser' changes of 2021 and the introduction in 2023 of a permission to CDR business consumers to share their data with a wider range of unaccredited persons highlighted important vulnerabilities discussed in Parts IV(A)–(B). These vulnerabilities expose the need for more efficient information security controls applicable to consumer data. This article argues that attempts to resolve the information security challenge by focusing on the *CDR alone* are likely to have only limited success, in the light of the 'boundary problem' and the corresponding difficulties in determining when the relevant CDR protections apply.[91]

First, the current system of information security controls within the CDR framework is based on an intricate separation of different data protection regimes that operate simultaneously — which only increases overall complexity. As an

89 Katharine Kemp and David Vaile, Submission to Treasury (Cth), *Review into Open Banking in Australia* (23 March 2018) 12 [39] (emphasis omitted).

90 Biddle, Gray and McEachern (n 52) 13.

91 See above Part IV(F).

example, the suggestion in the Explanatory Statement to the Competition and Consumer (Consumer Data Right) Amendment Rules (No 1) 2021 (Cth) that 'the minimum information security control of encrypting data in transit applies to the disclosure'[92] to a trusted adviser essentially turns on a technicality: whether CDR data remains *at rest* or is *in transit*. More specifically, the relevant duties in sch 2 of the *CDR Rules* require ADRs to

> [i]mplement 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.[93]

As long as ADRs comply with their obligations, the *process* of transferring CDR data from them to trusted advisers is likely to remain secure. However, once the CDR data has reached such advisers (and remains *at rest*), the CDR information security controls cease to apply. A similar issue should arise in the context of disclosures to unaccredited entities authorised by CDR business consumers.[94]

## 1 *Looking beyond the CDR*

This status quo demands a response that looks beyond the CDR framework. That response lies in raising the protections of consumers' data *economy-wide* that can be achieved by targeting *all kinds of valuable consumer data*.

In finance, the notion that valuable data must be protected is axiomatic: if banks did not protect their bank account ledgers, they would be mostly redundant (since money nowadays largely exists in the form of digital data stored by banks). The point stands even outside the 'formal' financial system:[95] decentralised cryptocurrencies and other digital assets have no value to end users and intermediaries, such as digital currency exchanges and custodians, without robust built-in information security measures. Unlike fiat currency, digital assets do not have physical forms that could be valuable per se (ie without connection to a digital database).

While consumer data is noticeably different from bank account records (in the sense that it does not possess easily ascertainable monetary value), it clearly possesses economic value — as evidenced by the proliferation of open banking

92 2021 Explanatory Statement (n 56) 20.

93 *CDR Rules* (n 8) sch 2 cl 2.2(1)(i) (emphasis added).

94 See *2023 CDR Amendment Rules* (n 8) sch 1 item 12, inserting ibid r 1.10A(11).

95 See Anton N Didenko and Ross P Buckley, 'The Evolution of Currency: Cash to Cryptos to Sovereign Digital Currencies' (2019) 42(4) *Fordham International Law Journal* 1041, 1056–8.

frameworks across the globe.[96] In other words, *all consumer data (and not just CDR data selectively designated under the CDR framework) is valuable data*.[97]

As valuable data, consumer data is sought not only by law-abiding businesses, but also by criminals. Unlawful access to such valuable data can have *lifelong implications* for the consumer (as the same data can be copied and reused by different culprits).[98] Therefore, the security of such consumer data could be *more important and more valuable* to the consumer *than the security of their money*. It thus stands to reason that the law should seek to protect the process of sharing that data *at all times*, and not only when it is shared through the CDR ecosystem. In other words, this article argues that any valuable consumer data should be treated at least *as valuable as money* — and protected accordingly.

While there are various mechanisms facilitating the achievement of this goal (including general privacy legislation), this article proposes the introduction, through the law, of *prescribed data transmission channels* for transfers of valuable consumer data *to and from any entities (except between individual consumers)* — coupled with a prohibition on the use of other data transmission channels for such data. This change would restrict service providers (by prohibiting the use of unsecure data transmission channels when collecting valuable data from the consumer and exchanging that data among themselves) but would not impact individual consumers (who would still freely exchange valuable data among themselves as they like, and would not be impacted howsoever when transferring other types of data).

The second element of the proposed economy-wide reform concerns protecting valuable consumer data at rest: all holders of valuable consumer data (with the exception of the consumer in question) should be subject to a *minimum standard of information security* analogous to that applicable to ADRs. As a result, trusted advisers and unaccredited recipients of CDR data chosen by CDR business

96 Hayden Harrison, 'Mapping Out the World of Open Banking', *Mastercard Newsroom* (online, 22 September 2021) <https://www.mastercard.com/news/perspectives/2021/mapping-out-the-world-of-open-banking>.

97 For a more detailed analysis supporting this argument, see, eg, Scott Farrell, 'Banking on Data: A Comparative Critique of Common-Law Open Banking Frameworks' (PhD Thesis, University of New South Wales, 2022) 36–46.

98 Data breaches can expose consumers to the risk of identity fraud, particularly when stolen data cannot be changed (such as date of birth) or can be very difficult to change (such as address). Identity theft can have both direct and indirect impacts on affected consumers, including long-term repercussions, like general avoidance of online transactions or less inclination to apply for credit: Keith B Anderson, Erik Durbin and Michael A Salinger, 'Identity Theft' (2008) 22(2) *Journal of Economic Perspectives* 171, 181–2. This aspect highlights the limitations of data breach remediation programs based on replacement of some of the identity documents for the affected consumers, like the one implemented after the 2022 Optus breach: see Australian Communications and Media Authority, 'Optus Data Breach' (Web Page) <https://www.acma.gov.au/optus-data-breach>. The regulator noted that '[t]he government is looking at all possible solutions to protect and reissue victims' identity documents'.

consumers[99] will be incentivised to increase their information security level accordingly.[100]

In addition to raising the overall level of information security across the economy, this approach will generate important change to the CDR framework. First, data holders will only be able to collect valuable consumer data via secure channels (thus protecting the points through which consumer data *enters* the CDR ecosystem). Second, consumers will no longer need to be concerned about security of their CDR data whenever it *leaves* the CDR ecosystem — ie when shared with unaccredited persons (such as trusted advisers).

As an added benefit, this approach helps to mitigate the unnecessary complexity caused by the CDR intruding into the relationship between consumers and their 'trusted advisers'. The latter have previously sounded their objections to such intrusion: 'This is a relationship between the consumer and their trusted adviser, the CDR regime should not disrupt a relationship that has worked amongst the consumer and their trusted advisers for many decades.'[101]

This opposition — while understandable — is likely to be significantly less pronounced if it is part of an economy-wide initiative to scale up consumer protection standards (thus eliminating the first mover problem). Furthermore, if the relevant service providers already use secure data transfer channels (which is a reasonable expectation, given their role in routinely handling vast amounts of consumer data), then no change will be necessary. Others will need to step up.

The proposed approach also helps to address the strange status quo whereby the same entity may need to create separate silos for the *same* types of consumer data, depending on how that data was obtained: through the CDR or not.[102] It is also fully aligned with the strategic priority of the Australian government to enhance the level of cyber (and data) security nationwide — as evidenced by *Australia's Cyber Security Strategy 2020*[103] and the National Data Security Action Plan.[104]

99 See *2023 CDR Amendment Rules* (n 8) sch 1 item 12, inserting *CDR Rules* (n 8) r 1.10A(9).

100 Insufficient economic incentives to invest in information security represent a challenge that the law should address: see, eg, Vernon J Richardson, Rodney E Smith and Marcia Weidenmier Watson, 'Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches' (2019) 33(3) *Journal of Information Systems* 227.

101 Chartered Accountants Australia and New Zealand et al, Submission to Treasury (Cth), *Consumer Data Right Rules Amendments (Version 3)* (30 July 2021) 4.

102 See 'Guidance on Screen-Scraping', *Consumer Data Right Support Portal* (Web Page, 23 March 2021) <https://cdr-support.zendesk.com/hc/en-us/articles/900005316646-Guidance-on-screen-scraping>.

103 Department of Home Affairs (Cth), *Australia's Cyber Security Strategy 2020* (Report, 6 August 2020).

104 Department of Home Affairs (Cth), 'National Data Security Action Plan' (Discussion Paper).

The proposed economy-wide reform is more ambitious than expanding privacy protections to cover small businesses:[105] the latter idea, which was developed by the author in a recent submission,[106] merely plugs an important gap in the privacy regime whereby some recipients of CDR data (including some of the 'trusted advisers') must observe neither the Australian Privacy Principles ('APPs'), nor the CDR framework provisions. In contrast, prescribing permitted data transmission channels for *all* valuable consumer data will surpass the scope of the APP protections (particularly considering the broad definition of 'consumer' in the CDR framework).[107]

Arguably the biggest advantage of the proposed reform is its ability to mitigate the negative effects of regulatory complexity and limited consumer awareness of the relevant risks. Consumers who have not studied the CDR extensively and are overwhelmed with the consent requirements and on top of that lack the expertise to determine whether so-called 'trusted advisers' are trustworthy, will benefit from the reduced potential for interception and misuse of their valuable data. The complexity of competently navigating the CDR framework arguably already exceeds an average consumer's ability (in the sense that few consumers are fully informed of the relevant risks). Over time, with further expansions (whether to new sectors of the economy, or by allowing new types of unaccredited businesses to access CDR data), this complexity is only expected to increase. The recent amendments empowering CDR business consumers to share CDR data with a wider range of unaccredited persons are a perfect example.[108]

Importantly, the reform proposed in this section is not meant to replace the CDR regime: the latter is still necessary to ensure that data holders are obligated to share their CDR data in response to consumer instructions. Instead, it seeks to address the unfortunate effects of the ongoing CDR expansion, which creates a *patchwork of consumer data protection environments* in Australia's economy with unclear borders that are hard to navigate.

Lastly, it is worth mentioning that the proposed approach has spillover benefits for non-consumers. As an example, under the current legal framework, service providers that obtain consumer data through a combination of CDR and non-CDR mechanisms 'need to carefully design [their] consent flows and consider the impression [they] create in [their] interactions with consumers, to ensure [they] comply with the CDR framework and are not likely to mislead consumers'.[109] To avoid breaching their CDR obligations, including the prohibition on misleading and deceptive conduct,[110] businesses must either prevent commingling of CDR

105 As defined in *Privacy Act 1988* (Cth) ss 6D(1)–(2).

106 Lyria Bennett Moses et al, Submission No 290012370 to Attorney-General's Department (Cth), *Privacy Act Review* (10 January 2022) 5–7.

107 See above Part III(B).

108 See *CDR Amendment Rules 2023* (n 8) sch 1 item 12, inserting *CDR Rules* (n 8) rr 1.10A(9)–(11).

109 'Guidance on Screen-Scraping' (n 102).

110 *CCA* (n 28) s 56BN.

data with non-CDR data, or (if commingling cannot or is unlikely to be prevented) protect *all* consumer data to a CDR standard (since commingling 'will not excuse [such businesses] from applying the high standard of protection that applies to CDR data').[111] In this sense, the proposed approach essentially mirrors the latter option (which already applies to businesses that struggle with separating different types of consumer data, depending on its source).

## 2 *How to Introduce the Proposed Reforms*

The sweeping economy-wide nature of proposed reforms raises the question: which legal framework is best placed to incorporate them?

On the one hand, the *Privacy Act 1988* (Cth) ('*Privacy Act*') appears to be the natural choice — particularly in the light of the numerous reform proposals outlined in the *Privacy Act Review* published by the Attorney-General in February 2023.[112] In its response, the Australian government has agreed in principle with a number of the Attorney-General's recommendations that may, if implemented, help to align to a certain extent the general privacy protections with the protections available under the CDR framework. Examples include proposal 6.1, which envisages the conditional removal of the 'small business exemption',[113] and proposal 26.1, which would give individuals 'a direct right of action … to apply to the courts for relief in relation to an interference with privacy'.[114]

On the other hand, the CDR keeps expanding to additional sectors and is no longer confined to open banking alone and could, over time, become economy-wide. Furthermore, the CDR framework already overrides the *Privacy Act* by setting out the privacy safeguards that apply as an alternative to the APPs.[115] Overall, the CDR framework appears well-suited for introducing changes that extend beyond the existing privacy laws.

At the time of writing, the choice of either pathway for legal reform appears to be a matter of feasibility and practicality. While the *Privacy Act* could facilitate a stricter overall approach to consumer data envisaged in this section, this change would arguably detract from the principles-based nature of the Act.[116] At the same time, reliance on the CDR framework to bring about economy-wide data protection reforms could be beneficial if one considers the history of development of the CDR. The CDR regime was designed as a 'step up' in the level of protections for

111 'Guidance on Screen-Scraping' (n 102).

112 Attorney-General's Department (Cth), *Privacy Act Review* (Report, 2022).

113 Ibid 6; Australian Government, *Government Response: Privacy Act Review Report* (Report, 2023) 23 ('*Privacy Act Review Response*').

114 *Privacy Act Review* (n 112) 15; *Privacy Act Review Response* (n 113) 36.

115 For a more detailed analysis of the relationship between the APPs and the privacy safeguards, see, eg, Burdon and Mackie (n 79).

116 In the future, this could be less of an issue if the privacy regulation shifts away from the principles-based model, considering the more detailed prescriptions envisaged by the *Privacy Act Review* (n 112).

selected types of consumer data,[117] supported by explicit information security obligations and bespoke enforcement via the statutory right of action given to consumers.[118] In a similar manner, and considering the similarities between the CDR provisions and the recommendations of the Attorney-General discussed above, the CDR framework could be used as a *testing ground* for future revisions of the *Privacy Act*. More specifically, the CDR legislation could apply the economy-wide protections proposed in this section (using prescribed data transmission channels to transfer data, except transfers between individual consumers) *only to CDR data*. Once feasible, the *Privacy Act* could then be revised to cover *all valuable consumer data*.

This gradual approach has another added benefit: economy-wide security of CDR data is a prerequisite for *other* enablers of consumer trust — such as consumer empowerment via 'direct to consumer' sharing of CDR data (which remains disabled largely due to insufficient economy-wide protections for data disclosed to consumers). This is discussed in more detail in Part V(D) below.

## B *Ban Data Sharing Practices That Facilitate Security Breaches*

A framework that prescribes acceptable channels for transferring all valuable consumer data is the ultimate solution that requires substantial political will to be implemented (which can be expected, considering the government's strong push towards economy-wide expansion of the CDR). Absent such political will, however, a blacklisting regime might be a suitable alternative: consumer data sharing methods that facilitate breaches of security of consumer data *by design*, should be prohibited. Screen scraping is one such method — for the reasons given in Part IV(B).

As discussed previously, screen scraping facilitates cyber breaches *by design*, regardless of the type of medium used and regardless of the types of precautions the consumer may take. This is evidenced by the leading international guidance in cybersecurity, as well as Australia's own legal framework.

A decision to allow screen scraping ultimately pursues only short-term benefits — as clearly demonstrated in a report by the Senate Select Committee on Financial Technology and Regulatory Technology ('Senate Select Committee'):

> It is also clear that it will take some time for the Open Banking regime to provide a level of data quality and ubiquity that is currently available using digital data capture services. As such, the committee considers that an outright ban on screen scraping is

117 Treasury (Cth), *Consumer Data Right Privacy Protections* (Report, December 2018) 4:

> The Privacy Safeguards, while generally consistent with the APPs, are more restrictive and, in conjunction with supporting Rules, will be more detailed than their equivalent APPs. They will have broader application, to catch all designated data relating to identifiable natural and legal persons and to bind all accredited data recipients in respect of CDR data they've received.

118 Ibid 4, 8.

> not prudent at the present time, and that in many cases these practices are enabling companies to innovate and provide competition in the financial services sector.[119]

While the pro-business agenda permeating the Senate Select Committee's decision is laudable for many, there has been limited discussion of the long-term implications of this choice — particularly for consumers. The risks of screen scraping are well-documented and recognised outside Australia:

> The practice of using login credentials for screen-scraping poses significant security risks, which have been recognized for nearly two decades. Screen-scraping *increases cybersecurity and fraud risks* as consumers provide their login credentials to access fintech applications. During outreach meetings with Treasury, there was *universal agreement* among financial services companies, data aggregators, consumer fintech application providers, consumer advocates, and regulators *that the sharing of login credentials constitutes a highly risky practice*.[120]

Indecisiveness leaves consumers exposed to these risks — as recognised by the US Department of Treasury:

> As described by one observer, 'the U.S. debate seems stuck at the yet-to-be resolved issue of migrating account aggregators from screen scraping-based to more secure and efficient API-based data-sharing methodologies.' *As long as this impasse remains unresolved, consumers will be caught in the middle.*[121]

It is worth stressing that a breakdown of consumer trust in the CDR framework would cause the greatest detriment to consumers, rather than service providers. After all, incumbent data holders would continue enjoying the status quo, while prospective recipients of consumer data would continue using screen scraping to obtain it. It follows that a screen scraping ban would help align the interests of consumers and recipients of CDR data, and accordingly facilitate the CDR's harmonious development.

Against this background, the Senate Select Committee's deference to the needs of direct beneficiaries of screen scraping — data capture businesses — merely reinforces the perverse incentive to undermine the prospects of the CDR. After all, at the early stages of this framework, users of this business model arguably have the strongest bargaining power: as long as the CDR is not yet widely used, they can collectively bargain for a more favourable legal treatment. Maintaining a 'hands off' approach to screen scraping in these circumstances does a disservice to the CDR and its objectives. Hopefully, it will not be necessary to experience a major data breach for the law to intervene. Unfortunately, as discussed in Part V(C)(1) below, such breach is likely unavoidable.

119 *Senate Select Committee Interim Report* (n 3) [8.93]–[8.94].

120 Steven T Mnuchin and Craig S Phillips, US Department of the Treasury, *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation* (Report, July 2018) 34 (emphasis added) (citations omitted).

121 Ibid 27 (emphasis added), quoting Bob Hedges, 'Consumer Data in an API-Enabled World' (2017) 5(4) *Banking Perspectives* 45, 46.

## C *Establish an Efficient Compensation Regime*

A data protection framework is only useful to the consumer as long as it (i) keeps the data safe and (ii) provides adequate redress in case of breach. This section considers each of these elements and argues that the latter should lead to the development of a consumer-oriented compensation framework to facilitate consumer engagement with the CDR regime and build consumer trust.

### 1 *Assume Breach*

Information security is a never-ending arms race between attackers and their prospective victims. Given their intelligent and evolving nature, cyber threats to information security demand a different attitude 'based on the realistic assumption that not all attacks can be prevented',[122] which implies greater emphasis on *responding* to breaches (including by providing compensation to affected persons) rather than attempting to build impenetrable cyber fortresses.

The inevitability of information security breaches has been acknowledged even in the most sophisticated industries in terms of data protection. For example, the severity and imminence of cyber risks in our banking system is emphasised by the Reserve Bank of Australia, which concluded in its October 2021 *Financial Stability Review* that 'a significant cyber event that has the potential for systemic implications is at some point *inevitable*'.[123] Similarly, in the context of the CDR, the Australian Privacy Foundation has argued that '[d]ata breaches are a near certainty' and the real question one should be concerned about 'is not if but when'.[124] As if to provide a sobering reminder of this simple conclusion, many of the largest Australian businesses experienced high profile cyber breaches in the second half of 2022.[125] Of particular relevance to this article are not just the magnitude and frequency of relevant cyber incidents (which are per se sufficient to paint Australian holders of consumer data as easy targets for cyber criminals), but the fact that these breaches affected the largest businesses in the two sectors recently designated under the CDR framework: telecommunications (Optus)[126] and energy (EnergyAustralia).[127]

122 Anton N Didenko, 'Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonization in the European Union and Beyond' (2020) 25(1) *Uniform Law Review* 125, 128.

123 Reserve Bank of Australia, *Financial Stability Review* (Report, October 2021) 38 (emphasis added).

124 Australian Privacy Foundation, Submission to Treasury (Cth), *Inquiry into Future Directions for the Consumer Data Right* (6 May 2020) 2.

125 See, eg, 'Optus Data Breach' (n 115); 'Medibank Cyber Incident' (n 50); 'MyDeal Data Breach' (n 51).

126 See 'Optus Data Breach' (n 115).

127 See Mostafa Rachwani, 'EnergyAustralia Latest to Be Hit by Cyber-Attack as Details of Hundreds of Customers Exposed', *The Guardian* (online, 21 October 2022) <https://www.theguardian.com/australia-news/2022/oct/21/energyaustralia-latest-to-be-hit-by-cyber-attack-as-details-of-hundreds-of-customers-exposed>.

The pragmatic 'assume breach' approach implies that the idea of building impenetrable cyber fortresses, while attractive in theory, is short-sighted in the long term. If applied in the context of the CDR, the 'assume breach' logic affects various elements of the framework, including security of fortified data transmission channels used by ADRs and information security of ADRs themselves recipients of CDR data, including trusted advisers and entities chosen by CDR business consumers.[128]

Conceptually, the 'assume breach' concept challenges the wisdom of CDR fundamentals: if every business — however advanced — will experience a successful cyber attack over time, then the idea of sharing *more data* with *more service providers* with *greater frequency* with the expectation that such data will be kept safe is, apparently, flawed. More importantly, it casts a new light on the enforcement challenges discussed in Part IV(C) above: the 'litigation quicksand' appears inescapable, making the limitations of mandatory insurance particularly dangerous. The protections employed by 'trusted advisers', from industry-specific data protection requirements to best interests duties, are similarly rendered meaningless in the long term.

If a successful cyber breach is only a matter of time — then the loss of one's CDR data at some point is also assured. This logic calls for a fundamental rethinking of the CDR's enforcement rules — by enabling consumers (particularly individuals) to obtain recourse more easily and cheaply. Ease of obtaining recourse is crucial, considering that litigation is likely to be uneconomical for many, due to the time and financial costs involved, the limitless potential for stolen data to be reused in subsequent criminal activities and difficulties in calculating the impact of CDR data loss.

### 2 *Compensation as Adequate Redress for Consumers*

If a cyber breach of CDR data is unavoidable in the long term (as discussed above), what types of recourse might be considered adequate? Returning lost data (unlike money) is essentially meaningless, as stolen data can be copied infinitely and cannot be 'unseen'. Furthermore, at the present level of technology, breached records can be stored by perpetrators indefinitely and shared with an indeterminate number of recipients. On top of that, databases storing unlawfully obtained data can be distributed — which effectively renders attempts to remedy the damage through database retrieval and destruction meaningless.

Considering the infinite sharing potential of breached data, every breach of CDR data may stalk the consumer for years (some for the entirety of their life),[129] making the current recourse envisioned by the CDR framework — litigation — unworkable:

128 See above Part III(B). See also *2023 CDR Amendment Rules* (n 8) sch 1 item 12, inserting *CDR Rules* (n 8) rr 1.10A(9)–(11).

129 See above n 98 and accompanying text.

> It is not realistic to expect consumers to detect data breaches or misuses of their personal information, or to pursue action against those who have exposed or misused their personal information. Consumers lack the resources, skills and powers necessary to discover most abuses or take effective action in response.[130]

Existing proposals to 'give teeth' to consumer protections, while useful, do not address the 'assume breach' conundrum. This applies equally to proposals to empower the responsible regulator[131] or to introduce

> liability which is sufficiently severe that firms do not simply price the contingency into their business model but instead take the utmost measures to protect consumer data, in line with consumer interests.[132]

The 'assume breach' approach does not render deterrence entirely meaningless but helpfully highlights its limitations: the consumer's data *will* be breached at some point — inevitably.

Safe harbours (discussed in Part IV(E) above) create another difficulty for consumers. Since consumer redress is based entirely on claims brought against the responsible CDR participant, safe harbours effectively create a gap in consumer protection by granting *immunity* to any proceedings (whether civil or criminal) to any CDR entity, as long as such entity acts in good faith in compliance with the CDR legal framework. As a result, consumers are unable to recover from service providers relying on safe harbour protections and must bear the loss, while those service providers remain protected.

As an illustration, consider the following example. A car engine is faulty, and the consumer returns it to the dealer for repairs — and, once the repairs are finished, finds out that the engine still does not work because the mechanic, despite trying really hard, could not identify the issue. In these circumstances the consumer should not be the party that bears the loss in the end: it does not matter how hard the mechanic tried, as the only thing that matters to the consumer is that the engine does not work. The same reasoning should apply to *safe harbours that directly impact consumers*, such as the one found in s 56GC of the *CCA*.

Finally, consumer redress options in relation to their CDR data are rather limited — since the concept of ownership does not generally apply to data.[133] In this context, it is worth noting the original, rather ambitious, plans to develop such an

130 Kemp and Vaile (n 89) 9 [29] (emphasis omitted).

131 Ibid 10 [30].

132 Ibid 17 [52] (emphasis omitted).

133 See, eg, World Bank Group, *Data for Better Lives* (Report, 2021) 224; HM Treasury, 'The Economic Value of Data' (Discussion Paper, August 2018) 8–9 [2.1]–[2.7]; *Data Ownership, Rights and Controls: Reaching a Common Understanding* (Report) 4–5; Select Committee on Artificial Intelligence, *AI in the UK: Ready, Willing and Able?* (House of Lords Paper No 100, Session 2017–19) 28 [62].

ownership model.[134] The reality, however, remains quite far from this ambitious goal: the CDR has not established separate ownership rights to CDR data, limiting the availability of redress options available to the consumer.

The resulting status quo calls for a form of recourse that is more easily accessible without significant resource costs to the most vulnerable groups of consumers, such as individuals. This article argues that a *compensation mechanism* triggered by breach or mismanagement of CDR data by a CDR participant could be such recourse. The key features of the proposed compensation mechanism can be summarised as follows.

*First*, it should not require the individual consumer to sue the CDR participant to obtain compensation, thus eliminating the upfront costs of securing redress (just as bank account holders do not need to sue to recover their balance under a deposit insurance scheme).

*Second*, this compensation mechanism should apply independently of regulatory penalties, as consumer compensation should not be affected by the regulator's ability to establish the grounds for liability or a decision not to pursue charges against the offender for whatever reason.

*Third*, a presumption that the 'CDR participant pays' should apply — with no safe harbours available to such a participant to avoid payment of compensation to the consumer. At the same time, the safe harbours could continue to operate as protection against regulatory penalties. As a result, the effects of safe harbours will be limited: they will no longer make consumers pick up the residual risks of CDR participants' business (as envisaged by the current CDR framework).[135]

This article argues that compensation obligations owed to consumers should not be viewed as an instrument intended to penalise CDR participants. A better view is to consider such compensation a reflection of fair allocation of liability between a service provider that seeks to benefit from valuable CDR data and its customer (the consumer) that enables such service provider to access such valuable data. A helpful illustration that can be used as a point of reference here is the allocation of liability between a bank and its customer upon presentation of a forged cheque for payment — which reflects the longstanding principles established in English and Australian case law.[136] There is considerable similarity between cyber breaches and forged cheques: just as CDR participants, faced with the inevitability of cyber incidents, would naturally seek to obtain protection from liability, so too banks did exactly the same due to the difficulties in identifying cheque fraud. Just as CDR participants cannot guarantee with 100% certainty that cyber incidents will be prevented, so too banks felt uncomfortable dealing with cheques knowing that their

134 Taylor (n 2) (emphasis added): 'Government is pursuing the very simple idea that the *customer should own their own data*. It is a powerful idea and a very important one.'

135 See above Part IV(E).

136 *London Joint Stock Bank Ltd v Macmillan* [1918] AC 777; *Greenwood v Martins Bank Ltd* [1932] 1 KB 371; *Commonwealth Trading Bank of Australia v Sydney Wide Stores Pty Ltd* (1981) 148 CLR 304.

authenticity was not easily verifiable at all times. A balancing of competing interests of bankers and customers was needed — and was ultimately resolved in favour of customers, as the courts refused to expand the scope of the customer's implied duties towards the banker. Banks — as the more sophisticated businesses providing a service to their customers — were found to be the natural party to absorb the losses:

> If they pay out upon cheques which are not [the customer's], they are acting outside their mandate and cannot plead his authority in justification of their debit to his account. This is a *risk of the service which it is their business to offer*.[137]

This article argues that a similar reasoning should apply to CDR participants handling cyber incidents involving CDR data, considering that within the CDR framework an individual consumer is clearly the weaker and less sophisticated party. As the above comparison with the banker–customer relationship has its limitations (in the sense that ADRs do not have to be banks and therefore could be expected to be held to a lower standard), a limited exception can be made for circumstances where consumers, through their own actions, contributed to the breach of CDR data (similar to bank customers who may be able to prevent fraud by being more vigilant when executing cheques).[138] However, there appears to be no convincing policy reason to make consumers ultimately responsible for a CDR participant's *own failures* — and therefore 'safe harbours' (which protect service providers regardless of the consumer's role in breaches of CDR data) should not limit the obligation to compensate the consumer, subject only to the above qualification regarding consumers who have actively contributed to the breach.

*Fourth*, the amount of compensation should prevent businesses from viewing cyber breaches as a normal cost of doing business. Even if all cyber incidents cannot be prevented, cyber breaches should be an exception, rather than the norm.

The proposed approach offers several important advantages.

*First*, it recognises, and addresses the consumer implications of, the 'assume breach' approach to information security. Instead of reinforcing the illusion of safety, it focuses on dealing with the consequences for consumers. The latter should be made aware of the likely unavoidable risks of a cyber breach — to promote a more realistic understanding of CDR risks.

*Second*, the compensation obligation is well aligned with the requirement for all accredited persons to obtain mandatory insurance.[139] One may expect that the proposed compensation arrangements will lead insurers to rethink how they price the insurance premiums and, more generally, whether they wish to continue to

137 *Tai Hing Cotton Mill Ltd v Liu Chong Hing Bank Ltd* [1986] AC 80, 106 (Lord Scarman) (emphasis added).

138 The *ePayments Code* (n 66) developed by ASIC could be a helpful source of inspiration for outlining the circumstances where the consumer has contributed to the breach on an *electronic* data platform, as it was designed specifically for *electronic* payments.

139 See above Part IV(C).

provide more expanded coverage. However, this is hardly a convincing counterargument, as increased premiums in this scenario will be a direct reflection of the insurers' assessment of the likelihood that consumers would not sue the ADRs under the current CDR regime. If nothing else, the proposed change will make the insurance pricing more accurate by reflecting the obligation to compensate *all* affected consumers — rather than only those who have the resources and intention to seek compensation in court. Similarly, if insurers choose not to offer their services altogether, the absence of insurer appetite to provide such cover could indicate that the original pricing indeed assumed that many consumers would not claim what is due to them.[140]

## D *Enable Consumers to Receive CDR Data Directly*

The strong economy-wide protections for CDR data and the enhanced consumer enforcement process envisaged in Parts V(A)–(C) above should provide a solid foundation to enable the (currently non-operational) 'direct to consumer' pathway for CDR data. Furthermore, as discussed in the companion article,[141] the reasons for excluding business consumers from 'direct to consumer' CDR data sharing appear a lot less convincing, considering that CDR business consumers enjoy greater freedom in choosing the recipients of their CDR data and thus are deemed sophisticated enough to bear the associated risks.[142]

Nonetheless, despite the prospective benefits generated by the other proposed reforms, there remains a danger that individual consumers will remain the 'weakest link' jeopardising the security of CDR data: even if the disclosing entity implements secure data transmission channels, the security of such data at rest (ie when held by the consumer) may be at risk if the consumer does not implement adequate protections.[143] This article argues that these risks can be reduced if 'direct to consumer' disclosures are implemented as a two-step process: (i) copying CDR data to a secure controlled environment (rather than to consumers' own devices) and (ii) providing consumers with the necessary credentials to access such CDR data at their discretion. Conceptually, the proposed change resembles integrating central counterparties into derivative transactions: instead of multiple one-off exchanges of specific CDR data between a CDR participant and the consumer, that data is copied onto a separate storage (a 'direct to consumer' hub) that maintains custody and safety of that data.

140 It should be stressed that the author's compensation proposal is to simplify recovery in circumstances where consumers are *already entitled* to it but due to various difficulties may choose not to enforce their right to sue.

141 Didenko (n 11) 90–1.

142 See *2023 CDR Amendment Rules* (n 8) sch 1 item 12, inserting *CDR Rules* (n 8) rr 1.10A(9)–(11).

143 Empirical studies suggest that consumers often do not do enough to protect themselves against data breaches: see, eg, George R Milne, Andrew J Rohm and Shalini Bahl, 'Consumers' Protection of Online Privacy and Identity' (2004) 38(2) *Journal of Consumer Affairs* 217, 229–30.

The proposed approach seeks to ensure that the 'direct to consumer' pathway does not become yet another 'valve' through which CDR data leaves the CDR 'pipeline' to a location with unclear information security practices. It offers important advantages.

*First*, the proposed 'access' regime will allow consumers to retain access to their CDR data regardless of any limitations of consumers' own IT devices. In other words, consumers do not need to worry that the data on their hard disk becomes corrupted, as they could access the online storage at any time.

*Second*, an added benefit is the flexibility it offers to limit the information security risks on the consumer side to unauthorised *access* (which can be minimised via measures such as multifactor authentication), while also offering industrial-grade information security protection to CDR data stored on a dedicated platform.

*Third*, the proposed regime is vastly superior to screen scraping. Even if consumers, should they so desire, choose to share their login credentials to access certain CDR data with a data capture business, the latter will only obtain a limited set of consumer data, as opposed to virtually unlimited access to a consumer's bank account which screen scraping provides.

*Fourth*, the proposed data sharing mechanism mitigates the reciprocity problem, as consumers with access to centrally stored and protected CDR data will be able to share that data, via the CDR, without having to consider whether the relevant CDR participant that produced that data may not be legally obligated to share that data to a third party pursuant to a consumer's request: the consumer is empowered to decide for themselves where that data should go.

An obvious downside of designing the proposed 'direct to consumer' hub is the risk of data concentration. That hub's cyber protections are likely to be frequently tested by attackers and thus need to implement best in class financial institution-grade cybersecurity. This also means that the level of protection afforded by such a hub will not only be superior to the average level of protection among CDR participants, but also by far surpass the consumer level of cyber resilience. At the same time, the 'assume breach' principle will continue to apply — and thus compensation should equally be available for cyber incidents caused by the hub operator's action or inaction leading to unauthorised access to CDR data. The compensation arrangements, however, should not cover instances when the breach takes the form of unauthorised access to the hub's data resulting from a consumer's failure to maintain the safety of their login credentials (in the same way the *ePayments Code* lists the circumstances in which the user is liable for unauthorised transactions).[144]

Another important aspect to consider is the risk that the entity that serves as the 'direct to consumer' hub will abuse its control over the relevant data. This raises the question of which entity is best placed to provide this functionality, under strict regulatory control or oversight. While a detailed analysis of potential options and

144 See *ePayments Code* (n 66) cls 10–11.

their implementation is outside the scope of this article, this matter should be subject to extensive public consultation.

### E *Boost Consumer Awareness of the Underlying Issues*

The reforms proposed in this Part V can help boost consumer awareness of the relevant issues (eg a ban on screen scraping will draw the attention of consumers to the CDR as a safer and government-endorsed alternative) or reduce the underlying risks (eg the economy-wide protections for consumer data discussed in Part V(A) above). Nonetheless, some of these initiatives may take substantial time to implement. A short-term solution proposed in this article is to (i) draw the attention of consumers to the inhibitors of consumer trust discussed in Part IV and (ii) position consumer trust as a measure of CDR's success.

As discussed in greater detail in the companion article,[145] reliance on consumers' lack of awareness of the more obscure risks may have serious negative consequences in the long run, when the relevant risks materialise — potentially breeding *deeper distrust* in the entire CDR framework.[146] Earlier consumer awareness would enable consumer choice and consent to be truly informed, as required by the CDR framework.[147] As an added benefit, using consumer trust as a measure of success, will help guide future reform to address these issues more quickly or, alternatively, seek convincing reasons to justify to consumers the necessity of those risks.

## VI CONCLUSION

Redesigning different parts of the CDR regime has little meaning and brings few benefits, unless put into context of the *entire* framework, having at the centre its key user, source of data and beneficiary — the consumer. This is particularly important, considering that the expansion of the CDR framework to other sectors of the economy continues, despite a temporary pause announced for the telecommunications sector.[148]

In the absence of agreed measurable criteria to assess the efficiency of the CDR framework, this article has proposed that the concept of 'consumer trust' should become the signpost of the CDR's success. It has established consumer trust as a

145 Didenko (n 11) 91–5.

146 A delay in bringing the relevant issues to the attention of consumers can deepen consumer distrust. As an example, Muzatko and Bansal found that 'companies that delay the announcement of a data breach are likely to suffer a *larger drop in consumer trust* than those companies that immediately disclose the data breach': Steven Muzatko and Gaurav Bansal, 'It Pays to Be Forthcoming: Timing of Data Breach Announcement, Trust Violation, and Trust Restoration' *Internet Research* (advance) (emphasis added).

147 *CDR Rules* (n 8) r 4.9(c).

148 Expansion to the telecommunications sector was temporarily put on hold in mid-2023, to allow the regime to mature in other sectors first: 'Consumer Data Right Newsletter: 26 May 2023' (26 May 2023) *Consumer Data Right Updates*.

key enabler of social change envisaged by the CDR, performed a retrospective analysis of the factors which inhibit consumer trust in the current CDR framework — before proposing reforms that should help overcome them.

This article has demonstrated that some of the underlying challenges can only be meaningfully addressed via economy-wide legal reforms, including an introduction of prescribed data transmission channels for transfers of valuable data (except between individual consumers). It is hoped the proposals formulated in this article will inform future reform directions for the CDR and consumer policy more generally.