

Director – Payments Strategy and Policy Unit  
Financial System Division  
The Treasury  
Langton Crescent  
PARKES ACT 2600  
By email: [paymentsconsultation@treasury.gov.au](mailto:paymentsconsultation@treasury.gov.au)

## **SUBMISSION TO THE CONSULTATION PROCESS ON THE AUSTRALIAN GOVERNMENT'S STRATEGIC PLAN FOR THE PAYMENTS SYSTEM**

Scientia Professor Ross P Buckley\*

Dr Anton Didenko\*\*

Dr Natalia Jevglevskaja\*\*\*

### **Summary**

This submission strongly welcomes the proposal to ground Australia's regulatory framework governing payments on the principles of efficiency, innovation, accessibility and trustworthiness. We equally welcome the inclusion in the future Strategic Plan of proposed key priorities to support and promote the said principles. In particular, for reasons outlined below,

1. we emphasise the importance of aligning regulatory payments architecture with developments in the broader data ecosystem, such as the Consumer Data Right (CDR); and
2. we welcome the proposal for the Strategic Plan to explore and / or articulate the policy rationale for introducing a central bank digital currency (CBDC) in Australia. In our view, CBDCs are likely to offer far more benefits in wholesale and cross-border applications in Australia and the Asia-Pacific region than in retail contexts. Specifically, CBDCs have the potential to revolutionise cross-border payments.

This submission briefly outlines our views. More comprehensive arguments are in our articles [here](#), [here](#), [here](#) and [here](#). We have explored the broader international aspects of CBDCs [here](#) and [here](#).

---

\* Ross P Buckley is the KPMG Law - King & Wood Mallesons Professor of Disruptive Innovation, an Australian Research Council Laureate Fellow, and a Scientia Professor at UNSW Sydney.

\*\* Anton Didenko is a Senior Lecturer at the Faculty of Law and Justice, UNSW Sydney.

\*\*\* Natalia Jevglevskaja is a Research Fellow on the ARC Laureate Project on the data revolution at UNSW Sydney.

The authors gratefully acknowledge the financial support of the ARC Laureate Fellowship on regulating the data revolution (FL200100007) – see <https://fintechrevn.org/>. The views herein are of the authors and not necessarily of the Australian government or Research Council.

## **Our Views on the Key Priority of ‘Aligning Payments System with the Broader Digital Economy Transformation’**

### **1. The Importance of Aligning Regulatory Payments Framework with the Developments in the CDR Regime**

Australia’s Digital Economy Strategy envisages Australia as being among the worlds’ top 10 digital economies and societies by 2030.<sup>1</sup> A safe, effective and efficient payments system is an essential building block of Australia’s digital economy as is the CDR – a regime which is intended to span the economy and to date has no analogues elsewhere making Australia the frontrunner among nations working on data-sharing systems. The successful development of the digital economy at home will be hugely boosted by Australia maintaining this lead.

As demand for data portability is projected to grow, aligning the payments regulation with the CDR regime is vital to enable both frameworks to operate efficiently. Specifically:

- (i) *The amount of data relating to payment transactions shared between participants in the payment ecosystem and beyond (for example, insurance) is poised to increase dramatically.*

As payments are increasingly made digitally, ‘many payments are now effectively data transfers, and the payments ecosystem is becoming a subset of the broader data ecosystem’.<sup>2</sup> With increasing digitisation, the demand for data portability – particularly of financial data – will only grow. The benefits to businesses and consumers flowing from data-sharing are plainly too good to forego: it spurs innovation, competition and efficiency across industries while consumers gain control over data that has previously been siloed within banks, insurance companies, energy and telecommunication providers, and other data holders. Data that has previously been used by businesses for self-serving purposes is ‘released’ to be used by consumers for their own purposes.

The CDR has been established to ensure that consumer data is shared safely, securely and efficiently. The drafters of the regime have rightly recognised that data is not just ‘new oil’. Data is much more vital – it is our water – and the CDR provides a sanitation system for Australia’s entire digital economy in that it keeps incoming data ‘reliable’ and ‘clean’, while ensuring the appropriate treatment of retained data. The CDR sets out a rigorous set of rules on data disclosure, collection, use, accuracy, storage, and deletion. If a data holder or an accredited data recipient (ADR)<sup>3</sup> are required or authorised under the CDR rules to disclose the CDR data they hold, they

---

<sup>1</sup> The Australian Government the Treasury, ‘Implementation of an Economy-wide Consumer Data Right: Strategic Assessment’ (Consultation Paper, July 2021) 7.

<sup>2</sup> The Australian Government the Treasury, *Payments System Review* (June 2021) 79.

<sup>3</sup> An ADR is an ‘accredited person’ (ie a person accredited by the Data Recipient Accreditor) who has received CDR data under the CDR Rules, see s 56AK of the of the *Competition and Consumer Act 2010* (Cth) (‘CCA Act’). A ‘data holder’ is defined in *CCA Act*, s 56AJ. Broadly speaking, data holders are the holders of the original data to which the right to transfer under CDR applies.

must take reasonable steps to ensure that it is ‘accurate, up to date and complete’ for the purpose for which it is held.<sup>4</sup> When an ADR no longer needs redundant data and is not required to retain it, it must take one of two steps: delete it or de-identify it.<sup>5</sup> Notably, the CDR gives consumers *the right to instruct deletion* of their personal information.<sup>6</sup> Under the *Privacy Act 1988* – which provides the basis for nationally consistent regulation of privacy and the handling of personal information – no such right currently exists.

At the heart of data-sharing under the CDR lies consumer consent. Data holders must ask consumers to authorise disclosure of requested CDR data and keep records and explanations of authorisations provided by consumers.<sup>7</sup> ADRs, too, must have consumer consent to request consumer data. Consent cannot be ‘implied’ or ‘open ended’; consumers must understand what they are consenting to and be able to revoke their consent to data disclosure, collection or use at any time.<sup>8</sup>

Critically, the CDR imposes strict and detailed information security requirements, including an extensive set of minimum information security controls that an ADR should put in place to protect CDR data from misuse, interference and loss, and unauthorised access, modification or disclosure.<sup>9</sup> Multi-factor authentication or equivalent control is required for all access to CDR data.<sup>10</sup>

The recent large-scale attack on Optus – which some experts suggest may be the worst data breach in Australia’s history<sup>11</sup> – illustrates vividly how the CDR regime will help prevent unforgivable mishandling of consumer data. The security breach resulted in the unauthorised disclosure of personal information of up to 9.8 million Optus customers – about 40% of Australia’s population – and included ‘customers’ names, dates of birth, phone numbers, email addresses, and, for a subset of customers, addresses, and ID document numbers such as driver’s licence or passport numbers exposing affected consumers to a significant risk of identity theft and fraud.<sup>12</sup> Notably, the identity documents of some 900,000 customers had expired, and for all customers, once their

---

<sup>4</sup> See *CCA Act*, s 56EN(1) and (2).

<sup>5</sup> See *CCA Act*, s 56BAA(1) and rr. 1.17 and 1.18 of the *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) (*‘CDR Rules’*).

<sup>6</sup> See *CCA Act*, s 56BAA(1) and *CDR Rules*, r 4.16. See also Treasury (Cth), *Review into Open Banking: Giving Customers Choice, Convenience and Confidence* (Report, December 2017) 57.

<sup>7</sup> *CDR Rules*, r 9.3 (1).

<sup>8</sup> *CDR Rules*, rr. 4.9 and 4.11-12.

<sup>9</sup> See *CCA Act*, s 56EO(1) and *CDR Rules*, sch 2.

<sup>10</sup> *CDR Rules*, sch 2.

<sup>11</sup> Tiffanie Turnbull, ‘Optus: How a Massive Data Breach Has Exposed Australia’, *BBC News* (online, 29 September 2022) <<https://www.bbc.com/news/world-australia-63056838>>.

<sup>12</sup> ‘Optus Notifies Customers of Cyberattack Compromising Customer Information’ (22 September 2022) <<https://www.optus.com.au/about/media-centre/media-releases/2022/09/optus-notifies-customers-of-cyberattack>>.

identity had been verified, retaining the data of such documents was highly questionable practice.<sup>13</sup> It is also reported that Optus’s online channel for data access and transfer purposes – an application programming interface (API) – did not require authorisation or authentication to access customer data, meaning that anyone on the internet with knowledge of that API endpoint could use it.<sup>14</sup> Had Optus been accredited under the CDR, it – most likely – would have been in violation of its CDR obligations by holding on to out of date data<sup>15</sup> and certainly for failing to protect its customer data from unauthorised access – and potential subsequent misuse – by breaching the minimum information security controls. Still, the probability that these violations would have occurred at such scale in the first place would have been much diminished as a result of the corporate consciousness-raising exercise that the stringent CDR accreditation process invariably triggers.

(ii) *To ensure and then leverage efficient operation of both frameworks, alignment of data standards and accreditation requirements is necessary.*

The pipes through which CDR data flows are enabled by technical data standards that prescribe the format of data, method of transmission and security requirements. These data standards were envisaged to be ‘living documents’ subject to continual change, in order to adapt to changing demands for functionality and available technology solutions. Equally, the payments ecosystem would not be operative without industry standards that ensure that payments systems can be accessed safely and securely. To facilitate interoperability, transparency and predictability, and to reduce costs of accessing data and lower barriers to entry for data driven payment services providers (PSPs) into the future, it is therefore vital to ensure consistency between the standards created by the payment industry standard-setting bodies and the standards developed for CDR by the Data Standards Chair, assisted by the Data Standards Body.<sup>16</sup>

The stringent accreditation requirements under the CDR have been purposefully designed to ensure the pipelines that make up the CDR sanitation system are as robust as possible. To have CDR data disclosed to them, businesses must be accredited. An accredited data recipient must be a fit and proper person or organisation;<sup>17</sup> have processes in place to adequately protect data;<sup>18</sup> have

---

<sup>13</sup> ‘Optus CEO Kelly Bayer Rosmarin’s Video Statement About Data Leak’, *7NEWS* (online, October 2022) <<https://www.youtube.com/watch?v=0tSUDfrioZU>>.

<sup>14</sup> Josh Taylor, ‘Optus Data Breach: Everything We Know So Far About What Happened’, *The Guardian* (online, 29 September 2022) <<https://www.theguardian.com/business/2022/sep/29/optus-data-breach-everything-we-know-so-far-about-what-happened>>.

<sup>15</sup> Note that ADRs are not required to delete CDR data in certain circumstances, including where retention is required by law: *CCA Act*, s 56BAA(2) and *CDR Rules*, r. 1.17A.

<sup>16</sup> See also The Australian Government the Treasury, *Payments System Review* (June 2021) 71-72 and Recommendation 12.

<sup>17</sup> *CDR Rules*, rr 1.9 and 5.12 (2)(a).

<sup>18</sup> *Ibid* r 5.12(1)(a).

internal dispute resolution processes;<sup>19</sup> belong to a relevant external dispute resolution scheme;<sup>20</sup> hold adequate insurance due to the risk of CDR consumers not being properly compensated for losses that might reasonably be expected to arise from a breach of obligations under the CDR framework;<sup>21</sup> and have an Australian address for service.<sup>22</sup>

It is anticipated that accredited providers under the CDR may want to offer payment services.<sup>23</sup> The payment services licence to be introduced under the future payment services framework should therefore – where appropriate – align with the requirements under CDR accreditation. In particular, it should take account of the cyber security requirements that an ADR should satisfy to become accredited (see above).<sup>24</sup> PSPs should not have to re-establish that they fulfil cyber security requirements that they have already met as part of their CDR accreditation. Without such an alignment, the attractiveness of participation in the payment ecosystem in Australia will diminish, regulatory burdens will increase, and, ultimately, valuable resources of both the PSPs and the regulators will be wasted.

## **2. The Policy Rationale for Introducing a Central Bank Digital Currency in Australia**

The proposed Strategic Plan recognises modernisation of payments infrastructure as one of the four key priorities (p 10) and seeks to facilitate ‘transition to more modern infrastructure’ (p 12). We support this view and argue that the introduction of a central bank digital currency will facilitate such transformation. Such a CBDC could be dubbed the ‘e-AUD’, by analogy with China’s e-CNY.<sup>25</sup>

While both retail and wholesale forms of CBDC in Australia appear to be considered in the Strategic Plan, we argue that the short-term benefits of wholesale (particularly cross-border) applications are likely to be far more substantial for the reasons outlined below.

### *(i) No convincing use case for a retail CBDC in the short term*

Despite significant interest among central banks around the world in the concept of central bank digital currencies, a convincing case for a *retail* CBDC in Australia is not apparent to us,

---

<sup>19</sup> Ibid r 5.12(1)(b).

<sup>20</sup> Ibid r 5.12(1)(c).

<sup>21</sup> Ibid r 5.12(2)(b).

<sup>22</sup> Ibid rr 1.7 (definition of ‘addresses for service’), 5.12(d), (e).

<sup>23</sup> The Australian Government the Treasury, *Payments System Review* (June 2021) 64.

<sup>24</sup> See *CDR Rules*, sch 2.

<sup>25</sup> Working Group on E-CNY Research and Development of the People’s Bank of China, *Progress of Research & Development of E-CNY in China* (Report, July 2021) <<http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf>>.

although of course this may well change with the current project by the Digital Finance CRC and the RBA to explore precisely such use cases.<sup>26</sup>

A CBDC is justified when it addresses an actual (rather than merely hypothetical) challenge that remains unresolved (for whatever reason) by the existing payment system. In this sense, most of the early CBDCs were designed to tackle the problem of financial inclusion, whereas Sweden's e-krona pilot<sup>27</sup> is a direct response to the significant reduction in the use of cash in the country (and the resulting risk that 'the public will, in future, no longer have access to, or be able to pay with, state-issued money'<sup>28</sup>). Overall, financial exclusion and cash phase-out appear to be the main drivers of retail CBDC development globally today.

In contrast, in a highly banked society such as Australia with widely available and free to use forms of state-issued legal tender (bank notes and coins), the need for a retail CBDC is less pronounced and the prospective benefits are likely to be minimal.

The drivers of a CBDC here are likely to be cross-border efficiencies and external geopolitical factors, including the risk of displacement of the domestic currency in international trade by a CBDC of another country or unmet demand for Australian currency overseas that cannot be easily satisfied by existing forms of the Australian dollar (eg the withdrawal of commercial banks offering Australian dollar accounts in some Pacific island nations). While China – the first major economy to pilot a retail CBDC on a massive scale – has spent years developing its central bank digital currency, the risks of displacement of the Australian dollar by the digital yuan currently appear to be remote (at least in the short term, in the absence of wide cross-border circulation of the e-CNY).

(ii) *CBDCs as enablers of cross-border payments*

A *wholesale* CBDC is likely to generate the most benefit in the short to medium term by improving the efficiency of cross-border payments.

The idea of cross-border integration of CBDCs is the result of the natural evolution of domestic CBDC studies. At the early stages of development of CBDC projects overseas, cross-border functionality was largely deferred for later consideration. For example, the Bank of Canada and the Monetary Authority of Singapore joined forces to work on a cross-border cross-currency DLT-based system combining the two domestic CBDC platforms only as the fourth stage of their

---

<sup>26</sup> Digital Finance Cooperative Research Centre and the Reserve Bank of Australia, *Australian CBDC Pilot for Digital Finance Innovation: White Paper* (26 September 2022) <<https://dfcrc.com.au/wp-content/uploads/2022/09/RBA-DFCRC-CBDC-Research-Project-Australian-CBDC-Pilot-for-Digital-Finance-Innovation-White-Paper.pdf>>.

<sup>27</sup> Sveriges Riksbank, 'The E-krona Pilot – Test of Technical Solution for the E-krona' (Web Page) <<https://www.riksbank.se/en-gb/payments--cash/e-krona/technical-solution-for-the-e-krona-pilot/>>.

<sup>28</sup> Sveriges Riksbank, 'E-krona' (Web Page) <<https://www.riksbank.se/en-gb/payments--cash/e-krona/>>.

respective research projects (Project Jasper<sup>29</sup> in Canada and Project Ubin<sup>30</sup> in Singapore), following years of experimentation in a purely domestic setting. The initial stages involved (i) investigating the use of DLT for high-value interbank settlement (phases 1 and 2 of Project Jasper and Project Ubin) and (ii) implementing CBDCs for delivery versus payment ('DvP') settlement of tokenised assets (phase 3 of both projects). A similar pattern was followed by the Bank of Thailand, which started investigating cross-border use cases of CBDCs<sup>31</sup> only after the successful completion of two domestic phases of Project Inthanon: phase I focusing on wholesale fund transfer<sup>32</sup> and phase II targeting DvP settlement.<sup>33</sup> In short, projects Jasper, Ubin and Inthanon began as domestic experiments and only much later proceeded to investigate cross-border functionality.

In recent years, the idea of cross-border integration of different central bank digital currencies has moved to the forefront of CBDC policy discussions, facilitated by the G20 Roadmap for Enhancing Cross-border Payments<sup>34</sup> and practical experiments conducted by the Bank for International Settlements (BIS) Innovation Hub that implement DLT (distributed ledger technology) to build cross-border payment platforms that enable 'multiple currencies within a single system'.<sup>35</sup>

Methods of cross-border integration among domestic CBDCs may differ and will determine the resulting benefits, which could be substantial and may include: (i) faster transaction processing on a 24/7 basis, (ii) improved transparency, or (iii) enhanced settlement mechanisms (eg 'atomic' settlement, which guarantees, in a bilateral settlement, that transfer of a currency in one direction occurs if and only if a corresponding transfer is made in the opposite direction). While CBDC interoperability could help facilitate both retail and wholesale payments, the latter are more likely to generate short-term impact for several reasons. First, most cross-border payments are processed on a wholesale basis, with several notable exceptions (regional single market areas, remittances

---

<sup>29</sup> Bank of Canada, 'Digital Currencies and Fintech: Projects' (Web Page) <<https://www.bankofcanada.ca/research/digital-currencies-and-fintech/projects/#project-jasper>>.

<sup>30</sup> Monetary Authority of Singapore, 'Project Ubin: Central Bank Digital Money Using Distributed Ledger Technology' (Web Page) <<https://www.mas.gov.sg/schemes-and-initiatives/project-ubin>>.

<sup>31</sup> Bank of Thailand and Hong Kong Monetary Authority, 'Inthanon – LionRock: Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments' (Report, 2020) <[https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Report\\_on\\_Project\\_Inthanon-LionRock.pdf](https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Report_on_Project_Inthanon-LionRock.pdf)>.

<sup>32</sup> Bank of Thailand, 'The Outcome and Findings of Project Inthanon Phase I and the Project's Next Steps' (Press Release No 5, 2019) <<https://www.bot.or.th/English/PressandSpeeches/Press/2019/Pages/n0562.aspx>>.

<sup>33</sup> Bank of Thailand, 'The Outcomes and Findings of Project Inthanon Phase II and the Project's Next Steps' (Press Release No 39, 2019) <<https://www.bot.or.th/English/PressandSpeeches/Press/2019/Pages/n3962.aspx>>.

<sup>34</sup> Financial Stability Board, *G20 Roadmap for Enhancing Cross-border Payments: Consolidated Progress Report for 2022* (Report, 10 October 2022) <<https://www.fsb.org/wp-content/uploads/P101022-1.pdf>>.

<sup>35</sup> BIS Innovation Hub, *Using CBDCs across Borders: Lessons from Practical Experiments* (Report, June 2022) 9 <<https://www.bis.org/publ/othp51.pdf>>.

and tourism).<sup>36</sup> Second, wholesale payments involve more sophisticated parties, which implies that the underlying rules and procedures can be less concerned with the difficult aspects of consumer protection.<sup>37</sup>

The need for cross-CBDC interoperability increases alongside the pace of international CBDC experimentation.<sup>38</sup> Due to the different stages of development of existing CBDC projects, it is unlikely that the rollout of CBDCs will occur in a coordinated fashion. It is equally unlikely that all CBDCs will implement the same technology or platform built by the same software developer. As a result, the risk of further international fragmentation of the international payments framework is very real – and calls for cross-border interoperability of different platforms.<sup>39</sup> Furthermore, many existing CBDC designs envisage public and private sector coordination, which creates additional pressure to ensure domestic interoperability across relevant jurisdictions.

Having said this, we stress that CBDC interoperability remains a vague concept: there are numerous ways to facilitate it in a cross-border setting. Interoperability could be limited to simplified access to the platform (eg via harmonised messaging standards), or it could go further than that and offer deeper integration through common business arrangements (such as a common counterparty) or even joint technical solutions connecting domestic platforms.<sup>40</sup> While the options are many, the importance of development of CBDCs with future interoperability in mind is acknowledged by major central banks (including the Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England and the Board of Governors of the Federal Reserve System):

‘The potential for *cross-border interoperability* should be considered by central banks from the outset of research on CBDC (focusing on broad harmonisation and compatibility between currencies to encourage safe and efficient transfers). The central banks in this group are therefore *committed to coordinating* as we move forward with our own domestic choices, exploring practical issues and challenges.’<sup>41</sup>

---

<sup>36</sup> Douglas Arner et al, *Building Regional Payment Areas: The Single Rule Book Approach* (Report, May 2022) 35-36 <<https://www.bis.org/publ/work1016.pdf>>.

<sup>37</sup> Ibid 36.

<sup>38</sup> Anneke Kosse and Ilaria Mattei, *Gaining Momentum – Results of the 2021 BIS Survey on Central Bank Digital Currencies* (Report, May 2022) <<https://www.bis.org/publ/bppdf/bispap125.pdf>>.

<sup>39</sup> See also Ghiath Shabsigh, Tanai Khiaonarong and Harry Leinonen, ‘Distributed Ledger Technology Experiments in Payments and Settlements’ (IMF FinTech Note, June 2020) 8 <<https://www.imf.org/~media/Files/Publications/FTN063/2020/English/FTNEA2020001.ashx>>.

<sup>40</sup> See Bank for International Settlements, ‘Central Bank Digital Currencies: Foundational Principles and Core Features’ (Report No 1, 2020) 7 <<https://www.bis.org/publ/othp33.pdf>>.

<sup>41</sup> Ibid 17 (emphasis added).

(iii) *Implications of competing non-interoperable CBDC platforms*

Failure to facilitate interoperability of potentially competing CBDC platforms at an early stage may well generate additional risks for Australians – if overseas CBDCs become widely accessible to businesses and individuals in Australia. While such risk may appear remote in the short-term, some of the CBDCs initially designed for domestic use are likely to operate across borders in the future. As an example, according to a recent BIS study, the People’s Bank of China is already ‘exploring the potential of the eCNY for cross-border payments’.<sup>42</sup> Substitution of the Australian dollar could therefore materialise, giving rise to a number of challenges.

Dominant foreign CBDC platforms are likely to become attractive targets for cyber attackers, with possible major systemic consequences resulting from successful breaches. Therefore, the rollout of CBDCs abroad raises important questions for the Australian government. Will it help to promote the safety of personal data of Australians if an overseas retail CBDC (such as e-CNY) becomes widely available to Australian citizens? Will any protective measures be implemented – and if so, which ones? It is highly probable that major economies (like China or the United States) will use CBDCs to both improve their *domestic* payment networks and project their economic power by controlling vast amounts of valuable transactional data about the Australian economy and personal data of Australians using such CBDCs. Major foreign economies have powerful tools to force Australian businesses to comply with their laws – as exemplified by the unprecedented extraterritorial reach of the US *Foreign Account Tax Compliance Act* (FATCA), which some scholars have dubbed ‘by far the most egregious example of extraterritorial overreach in history’.<sup>43</sup>

As major overseas CBDCs become widely available to Australian firms and individuals, large amounts of valuable data (including payment transactions information) will be controlled by foreign businesses and accessed by foreign regulators. Just like with FATCA, eventually Australia may be forced to negotiate some form of international (bilateral or multilateral) legal regime in response. However, to have any leverage in those negotiations, Australia likely needs to have its own CBDC in place.

---

<sup>42</sup> Douglas Arner et al, *Building Regional Payment Areas: The Single Rule Book Approach* (Report, May 2022) 23 <<https://www.bis.org/publ/work1016.pdf>>.

<sup>43</sup> Bruce W Bean and Abbey L Wright, ‘The US Foreign Account Tax Compliance Act: American Legal Imperialism?’ (2015) 21(2) *ILSA Journal of International and Comparative Law* 333, 367.