TRUELAYER

TrueLayer response to Statutory Review of the Consumer Data Right

20 May 2022

Table of contents

About TrueLayer

TrueLayer is a global open banking platform that makes it easy for anyone to build better financial experiences. Businesses of every size use TrueLayer to power their payments, access financial data, and onboard customers across the UK, Europe, and Australia. Founded in 2016, TrueLayer is trusted by millions of consumers and businesses around the world.

TrueLayer is Europe's leading open banking platform. We were the first-mover in the UK with over 98% coverage of the market and 90%+ coverage across key European markets. We are headquartered in London, and route over half of all open banking traffic in the UK, Ireland, and Spain and provide API-only based technology with industry-leading conversion rates.

In Australia, TrueLayer is an active Accredited Data Recipient (ADR) and participates in the CDR ecosystem as an accredited intermediary providing 'B2B' data collection and aggregation services.

Executive summary

From a global perspective, there is much to praise in the design of the CDR regime and the way it has been implemented in the banking sector, but more needs to be done to make the CDR a success and enable the statutory objects of creating more choice and competition to be achieved.

A key emphasis of the Statutory Review should be on those aspects of the UK and EU regimes that have driven the success of Open Banking to date and which should inform adjustments to the current CDR regulatory regime. These success factors were a dedicated Open Banking implementation entity with a pro-competition remit, lower barriers to participation in the Open Banking ecosystem and a regulatory regime that discouraged continued reliance on screenscraping. These lessons form the basis of TrueLayer's key recommendations for the future evolution of the CDR regulatory regime:

- **Key recommendation (1): Consistent with the competition focus of other Open Banking regimes, minimise barriers to accreditation and ongoing compliance so that more firms are encouraged to enter the CDR ecosystem instead of operating outside it**

- **Key recommendation (2): To give participation in the CDR a decisive boost, policymakers should phase out screen scraping (as the UK and the EU have done) for data designated by the CDR, commencing with Open Banking**

- **Key recommendation (3): An independent authority should be nominated to be responsible for the development of the CDR ecosystem, with an initial focus on Open Banking implementation**

Introduction

The CDR vision

The original vision underpinning the CDR was an economy in which consumers were empowered - via secure data sharing - to access new and better-tailored products and services, and where consumers would see their everyday 'costs' reduced. More broadly, the CDR was intended to bring competition and innovation benefits.[1] Today, encouraging competition rightly remains one of the CDR's 'guiding principles'.[2] A successful CDR will not only increase competition between existing providers and lower barriers for new entrants, but it will also lay the foundations for future innovation that will enhance and expand the set of products and services from which consumers can choose.

The CDR's rollout started in the banking sector - as it holds significant amounts of data from which consumers can readily derive value. But the Government's ambition remains to achieve economy-wide expansion of the CDR.[3]

As a leading enabler of secure third-party data access in many countries, TrueLayer is excited to be part of this effort, leveraging the CDR to power a growing set of products and services for the benefit of Australian consumers and businesses. We are confident that Open Banking can be the CDR's first true success story - and a springboard for the CDR's economy-wide expansion. Achieving this will place Australia at the forefront of open data reforms happening around the world.

Ensuring success in CDR-enabled Open Banking

From a global perspective, there is much to praise in the design of the CDR regime and the way it has been implemented in the banking sector. Australia's CDR-enabled Open Banking covers a broader set of accounts and products than implementations in other countries, with richer datasets. In addition, Australia has learnt valuable lessons from Open Banking initiatives in the UK and EU - for instance, common consumer experience (CX) standards applied from the beginning for data holders[4] and users have not needed to frequently re-consent to data

---

[1] Australian Government, Data availability and use, Productivity Commission Inquiry Report (March 2017), p. 193. https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf

[2] Australian Government, Future directions for the Consumer Data Right, final report, p. 6. https://treasury.gov.au/sites/default/files/2021-02/cdrinquiry-final.pdf

[3] Australian Government, Response to the Inquiry into Future directions for the Consumer Data Right, p. 2. https://treasury.gov.au/sites/default/files/2021-12/p2021-225462.pdf

[4] The UK only imposed these in September 2018, nearly nine months after Open Banking launched.

sharing[5]. As of May 2022, 30 firms have become accredited data recipients (ADRs), of which 18 are 'active'.[6] In our experience, there is genuine and growing interest from consumer-facing businesses in the opportunities created through data access under the CDR.

But more needs to be done. To be truly successful, the CDR must attract a *significant and growing user base* that values the products and services built on the regime's foundations. This will be a dynamic process, involving not just measures to ensure the CDR is rolled out and available but ongoing engagement to make sure it is attractive to consumers and other ecosystem participants. This Statutory Review offers a timely opportunity for Australian policymakers to consider changes to the CDR regime that will put it on a path to success in banking, the first CDR designated sector. By making Open Banking a true CDR success story, policymakers will create a strong springboard for continued expansion of the CDR into energy, telecommunications, Open Finance, and beyond to the wider economy.

While Australia's vision for an economy-wide CDR is unique, other jurisdictions are further along in their Open Banking rollout, having launched before the CDR went live for banking in July 2020. The UK's Open Banking experience since 2017 shows what can be achieved in terms of ecosystem participation and take-up (5 million users at last count[7]) with a regulatory framework that is centred on encouraging competition and which has an ongoing and dedicated focus on ensuring implementation in line with that objective (**Chart 1**). The EU experience offers a similar lesson.

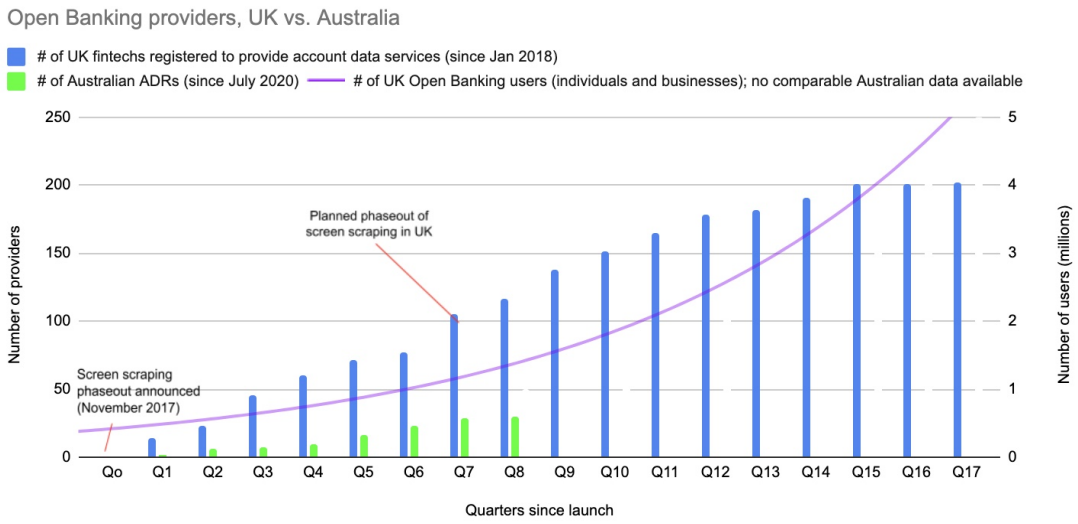
---

[5] The UK initially required consent to be refreshed every 90 days, it later extended this to 12 months - the period chosen in Australia. The European Banking Authority has also recently proposed extending its 90 days to 180 days minimum.

[6] https://www.cdr.gov.au/find-a-provider?page=2&providerType=Data%2520Recipient&status=ACTIVE

[7] https://www.openbanking.org.uk/news/open-banking-passes-the-5-million-users-milestone/

Chart 1: Growth of Open Banking: UK and Australia



Notes: The registered UK fintech figures include only account information service providers (AISPs) to facilitate comparison with Australia, where payment initiation is not yet part of the CDR regime. The Australian figures include banks among accredited data recipients - in addition to fintechs. The UK user numbers are for all of UK Open Banking (i.e. account information services and payment initiation services) - no data is available that just covers usage of account information services.[8] The UK screen scraping phaseout was originally set to take effect on 14 September 2019, but in recognition that certain bank accounts were not accessible via APIs on that date, the FCA announced an initial adjustment period running up to March 2020.

While recognising Australia's more ambitious vision for the CDR, a key emphasis of the Statutory Review should be on those aspects of the UK and EU regimes that have driven their success in Open Banking to date and which should inform adjustments to the current CDR regulatory regime. These include:[9]

- A stronger emphasis on promoting competition, with lower barriers to accreditation and ongoing compliance, so that more firms are encouraged to enter the CDR ecosystem instead of operating outside it.

- Phasing out 'screen scraping' as an alternative method of accessing consumers' banking data.[10]

---

[8] Source for UK AISPs: https://register.fca.org.uk/s/search?predefined=AIPISP. Source for Australian ADRs: https://www.cdr.gov.au/find-a-provider. Source for user growth data extrapolation: https://www.openbanking.org.uk/news/open-banking-passes-the-5-million-users-milestone/ and https://www.openbanking.org.uk/news/uk-open-banking-marks-fourth-year-milestone-with-over-4-million-users/. The number of successful API calls made by third party providers using account providers' Open Banking APIs in the UK also rose over this period, from 13.2m calls a day in March 2020 to 31.8m a day in March 2022 (https://www.openbanking.org.uk/api-performance/).

[9] UK Open Banking also enables payment initiation, and there are additional lessons for Australia to consider as it adds action initiation to the CDR regime. But in responding to this Review we focus on products and services that access and use Open Banking data as currently permitted by the CDR.

[10] In the Open Banking context, 'screen scraping' means the practice whereby third parties gain access to a customer's data using their login credentials (effectively acting as the customer with his or her consent, with the broad data access that this entails).

- Most notably in the UK, open banking success was driven by a standards body that had a mandate to oversee how API standards were implemented by banks - such a body is needed in the CDR ecosystem.

Putting competition at the heart of the CDR regime

Under Part IVD of the *Competition and Consumer Act 2010* (the Act), the object of promoting competition is listed alongside enabling consumer data to be shared 'safely'. Data protection is undeniably important, and the CDR regime should continue to ensure appropriate protection for the consumers who use it. But this needs to be balanced with a focus on competition to ensure more data recipients enter the regulated space, increasing the likelihood and range of the products and services being offered that are attractive to consumers and that create positive 'value exchanges' based on using the CDR. **Excessive compliance and accreditation burdens within the CDR ecosystem are having the perverse effect of encouraging more activity *outside* the CDR's boundaries, ultimately *undermining* consumer protection and privacy.**

Competition starts with promoting entry into and expansion within the CDR ecosystem

Lowering barriers, such as excessive compliance and accreditation burdens, should increase the number of ADRs and the products and services on offer. It is hard to predict in advance exactly which products and services will prove successful with users. Encouraging market entry increases the chance of popular offerings coming to market and breaking through. Increased ecosystem participation should therefore lead to higher user take-up of the CDR.

Lowering barriers would also have the beneficial effect of bringing more Open Banking activity within the regulated space, relying on regulated APIs instead of screen scraping. APIs are safer for users because they operate under the principle of data minimisation, user credentials are not shared with the data recipient and there is a formal liability framework in the event that things go wrong. Finally, whereas data holders cannot easily block screen scrapers even if they have good reason to do so, they can refuse to respond to API requests where they have reasonable grounds to believe that this is necessary to protect their systems or to prevent consumer harm.

In a competitive CDR ecosystem, data recipients are incentivised to build user trust to win market share, and it is efficient to give them scope to innovate in how they do so. In Europe, there have been no major incidents of data misuse or security breaches in Open Banking despite a lighter-touch and less prescriptive regulatory regime. By lowering the CDR's barriers to entry and expansion Australia would enhance competition whilst still ensuring that all data recipients operate at a sufficient baseline of user protection.

In particular, there should be closer alignment between the privacy rules imposed by the CDR and those imposed economy-wide by a reformed Privacy Act[11], particularly in relation to the use and disclosure of data and information security. As the CDR is rolled out in banking, energy, telecommunications, finance, and across the wider economy, it becomes increasingly inefficient to have two standards for privacy protection. Policymakers should seek to more closely align standards between the Privacy Act and the CDR. Greater competition would also be achieved by appropriately lowering the accreditation and compliance obligations for CDR to encourage more firms to become accredited, while also ensuring that data sharing across the economy occurs in an appropriately secure manner by phasing out reliance on screen scraping (see Key recommendation (2) below). As a starting point, in advance of the outcomes of the Privacy Act review, it would be possible to provide greater flexibility in relation to consent and related processes, and to enable ADRs to implement a risk-based approach to implementation of CDR information security controls (rather than mandatory application of all controls).

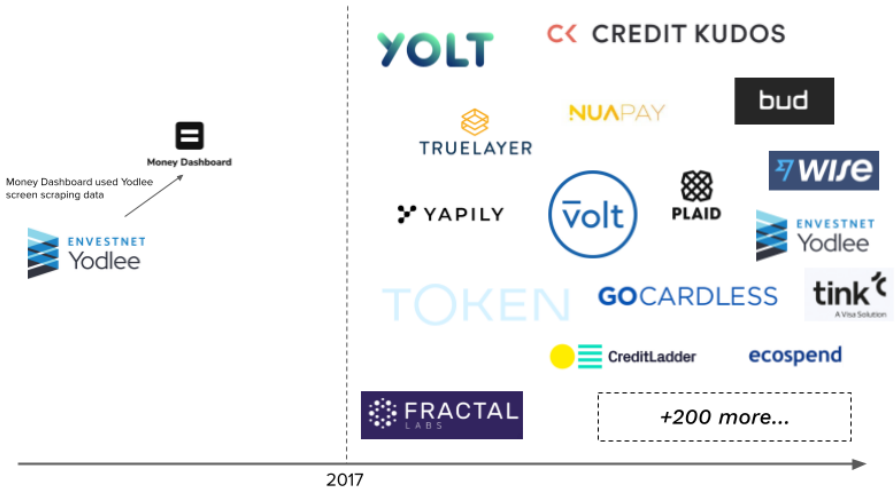
Key recommendation (1): Consistent with the competition focus of other Open Banking regimes, minimise barriers to accreditation and ongoing compliance so that more firms are encouraged to enter the CDR ecosystem instead of operating outside it

Phasing out screen scraping

In the near term, a further foundational element for a successful regime is ensuring a level playing field for firms that want to access data through the CDR as compared with via screen scraping. Currently, an unlevel playing field between regulated and unregulated firms is a key factor behind the slower pace of accreditations and CDR take-up in Australia compared with the experience of Open Banking in Europe, where screen scraping has been phased out.

[11] See the ongoing review of the Privacy Act 1988 by the Attorney-General's Department. https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988

Chart 2: UK Open Banking market, pre- and post-announcement of screen scraping phase out



Note: this is the overall UK Open Banking market and so it includes fintechs offering payment initiation services as well as account information services.

In Australia, screen scrapers face lower regulatory burdens than providers of CDR-enabled products and services do. Notably, screen scrapers do not require accreditation and screen scraping is not subject to the CDR's bespoke Privacy Safeguards (and related rules). Policymakers had hoped when they launched Open Banking that CDR-compliant APIs would gradually crowd out screen scraping by 'making the practice redundant'.[12] **However, the CDR's heavier compliance and accreditation burden - together with the lack of incentives to join the CDR ecosystem - mean that screen scraping remains widespread.**

The advantages for consumers of regulated APIs have been addressed above. There is broad agreement that screen scraping is an inferior way to access consumer data because of the risks it poses. The Treasury's 2018 Review on Open Banking described screen scraping as 'risky, unstable and costly', noting that it had developed 'out of necessity, rather than because it is an elegant technology design for data sharing'.[13] This echoed the sentiment of some industry participants, who have described screen scraping as 'a quirk of history where a hack to get around poor banking services became entrenched'.[14] The ACCC has stated that 'screen

[12] The Treasury, Review into Open Banking in Australia, final report, p. x. https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf

[13] Ibid, p. 72.

[14] Dave Tonge, 'Credential sharing — the real problem with screen scraping', *Medium* (6 October 2017). https://medium.com/@davidgtonge/credential-sharing-the-real-problem-with-screen-scraping-a35a32860a44

scraping has inherent risks'[15] and that the regulators' role was 'to make sure that a better, safer alternative is available' in the form of the CDR. More recently, in a consultation on updating the ePayments Code, ASIC expressed concern about the 'grey area' that arises when consumers make data available to third parties via screen scraping, in particular regarding whether the practice amounts to 'disclosure' of a passcode.[16] Depending on the answer, consumers might not receive compensation in the event that the disclosure led to unauthorised transactions.[17]

Screen scraping is also sub-optimal from a competition perspective. By contrast with the 'open' APIs used in CDR-enabled Open Banking, screen scraping necessarily relies on proprietary technology, which reinforces incumbent providers of data sharing services. In the United States, which still lacks an Open Banking framework, the number of data sharing third party providers is far lower than in the UK and Europe, with Plaid being far-and-above the dominant one.[18]

Some have expressed the view that phasing out screen scraping while the CDR is still being rolled out could be counterproductive, as it could for instance undermine the data sharing experience if data holder APIs are not yet working sufficiently well. This is misguided. The experience of phasing out screen scraping in the UK and EU shows that this need not harm the broader data sharing ecosystem - on the contrary, both confirmation of a future phaseout, and the phaseout itself, can act as a spur to ensure APIs perform well and the ecosystem grows rapidly within the regulated space.[19] While screen scraping remains available, there is a clear risk that CDR-enabled Open Banking will not mature or gain sufficient momentum.

A clearly communicated phaseout - with an adjustment period if necessary - would allow even data recipients that currently rely on screen scraping to adapt and compete in the new environment. But waiting for the CDR to succeed before setting a date to phase out screen scraping risks undermining the CDR's ability to achieve success in the first place.

From a competition perspective, phasing out screen scraping will level the playing field for data recipients, encourage them to enter the regulated CDR ecosystem and spur the emergence of more CDR-enabled products and services. Indeed, even confirmation of a *future* phase out will be a useful driver of these outcomes.

---

[15] Select Committee on Financial Technology and Regulatory Technology, 27 February 2020. https://www.aph.gov.au/Parliamentary_Business/Hansard/Hansard_Display?bid=committees/commsen/0c22cd39-8139-496a-a9d0-d010b6b7e562/&sid=0002

[16] ASIC, CP 341 Review of the ePayments Code: Further consultation, p. 35-36. https://download.asic.gov.au/media/eh2fceff/cp341-published-21-may-2021.pdf

[17] Ibid., p. 32.

[18] Joshua Macey and Dan Awrey, The promise and perils of open finance, European Corporate Governance Institute Working Paper No. 632/2022 (March 2022), p. 5. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4045640

[19] Below we also explore ways in which policymakers could mitigate any downside risks from the phaseout, by for example allowing screen scraping as a temporary fallback option when APIs fail.

A phaseout of screen scraping will also bring benefits to the broader ecosystem:

- For users: in addition to gaining access to ever-improving CDR-enabled offerings, consumers (and businesses) will benefit from greater protection through the CDR regime when they share their banking data. A screen scraping phaseout will give users control over the data shared and subject all data sharing to data minimisation and a clear liability framework.

- For banks: phasing out screen scraping will address concerns about potential liability for screen scraping-related failures and provide incentives to invest in well-functioning APIs (in turn helping to drive the CDR's success). Increased user demand for CDR-enabled services will mean banks face pressure to develop adequate APIs, especially if there is a dedicated body monitoring delivery (see further below).[20]

- For data recipients: phasing out screen scraping does not mean that screen scrapers will need to exit the market. Firms that currently offer or rely on screen scraping can evolve and become participants in the CDR ecosystem, enabling them to provide their services in safer ways. This has been the experience in Europe. Lowering barriers to entry and expansion within the CDR ecosystem (see Key Recommendation (1) above) will help facilitate this market evolution.

Key recommendation (2): To give participation in the CDR a decisive boost, policymakers should phase out screen scraping (as the UK and the EU have done) for data designated by the CDR, commencing with Open Banking

Create a permanent CDR implementation authority

TrueLayer supports the economy-wide expansion of the CDR as a key Government objective. But it is equally important to ensure that existing CDR-designated sectors, notably banking, are set up for success. In addition to the changes recommended above, we believe this goal would be best served by creating a dedicated body to oversee delivery of the CDR (starting with Open Banking), with a specific mission to grow the CDR ecosystem and user base.

This 'authority' would have a pro-competition remit and be charged with serving the whole ecosystem - and empowering ADRs in particular. It would have the mandate to make the CDR standards and oversee their implementation. This would include the ability to issue directions to data holders to address API non-conformance, as well as making changes to the standards in order to address stumbling blocks and drive progress. Acting as an advocate for the CDR, the authority would help accelerate the rollout of the CDR in Australia with a particular focus on the currently designated sectors of banking and energy. The UK Open Banking

[20] In both the UK and the EU, screen scraping has been temporarily allowed as a fallback option when bank APIs are unavailable or non-performing. Because banks generally dislike screen scraping, this has created an additional incentive for them to improve their APIs.

Implementation Entity (OBIE) has followed this blueprint and it both offers a model for a similar independent authority in Australia and illustrates the value of taking such an approach.

The authority should also be responsible for collecting and, where appropriate, publishing metrics that measure success - including from the user's perspective. Some metrics are already published via the CDR performance dashboard, but these focus on system inputs (API availability) and outputs (API response times), and rather than user outcomes.[21] It is also worth noting that these metrics are as reported by data holders, rather than as experienced by ADRs. Adding outcome metrics such as user numbers and, in time, industry-level conversion rates, would help to measure progress towards policy goals, inform engagement by ecosystem participants, and identify where additional interventions may be warranted.

Key recommendation (3): An independent authority should be nominated to be responsible for the development of the CDR ecosystem, with an initial focus on Open Banking

Looking forward

The Government has committed to expand the scope of CDR-enabled Open Banking by adding action (including payment) initiation, 'taking into account any lessons learnt from existing CDR designation processes'.[22] Adding payment initiation functionality will align the CDR in the banking sector with the UK and EU Open Banking regimes. By significantly expanding use cases, payment initiation promises to further drive adoption and - if correctly designed - should bring significant benefits to merchants and the wider economy.

But the issues raised above cannot be left unaddressed pending the introduction of action (and payment) initiation. Consumer and business take-up is needed now to vindicate the CDR, attract continued investment and support participants in building commercially sustainable offerings. If the CDR stalls before the introduction of action initiation, there is a risk that the Open Banking ecosystem will lack the critical mass needed to make the best use of additional functionality, depriving consumers, businesses and the wider economy of the significant additional benefits made possible by these future reforms.

We address below each of the Review's five questions, identifying the relevant Key recommendations and adding further detail and supporting evidence.

We look forward to further engaging with the Government on these important topics.

---

[21] https://www.cdr.gov.au/performance

[22] Government Response to the Inquiry into Future Direction for the Consumer Data Right (December 2021), p. 11. https://treasury.gov.au/sites/default/files/2021-12/p2021-225462.pdf

Response to Review questions

1. Are the objects of Part IVD of the Act fit-for-purpose and optimally aligned to facilitate economy-wide expansion of the CDR?

TrueLayer's view is that the objects of Part IVD of the Act, set out in s56AA, are fit-for-purpose and appropriately focus on the objects of creating **more choice and competition**, and promoting the public interest, by enabling consumers to require the sharing of information relating to them held in designated sectors.

These objects are consistent with the way in which the Productivity Commission, in its Data Availability and Use report, had conceived a consumer data right as a 'fundamental reform in Australia's competition policy in a digital world'.[23] These objects also reflect a guiding principle from the Open Banking Review that Open Banking should be 'done to increase competition for the banking products and services available to customers so that customers can make better choices'.

Our concern is not with the objects of Part IVD of the Act but the way in which other aspects of the regulatory regime, such as the bespoke CDR privacy regime, have impeded the achievement of the object of creating competition. In recommending the creation of a consumer data right the Productivity Commission had noted that 'it is not, nor is it intended to be, a replica of privacy law'[24] and that 'while the protections applying to personal information under the Privacy Act 1988 (Cth) would remain, the recommended reforms would also take Australia beyond the stage of viewing data availability solely through a privacy lens. This recognises that *there is much more than privacy at stake when it comes to data availability and use*'[25] (emphasis added).

Despite the recommendations of the Productivity Commission, the CDR does contain a replica of privacy law that imposes a higher compliance burden for CDR participants than entities that are subject to the Privacy Act, and restrictions on the use and disclosure of CDR data that limit the extent to which existing and new use cases can be supported by the CDR. In turn, this discourages participation in the CDR by potential data recipients and therefore the achievement of the CDR's choice and competition objects. If consumer benefits are to be realised from the CDR in the form of increased competition and a more secure and privacy-enhancing way of sharing data, then the regulatory regime needs to change to ensure

[23] Australian Government, Data availability and use, Productivity Commission Inquiry Report (March 2017), p2.

[24] Ibid, p15.

[25] Ibid, p14.

that accreditation and compliance obligations do not act as a barrier to entry (see Key recommendation (1)).

The objects of promoting competition and choice should be the 'north star' and guiding principle for implementation and decision-making for the CDR. Key privacy safeguards such as informed, express consent and other consumer protections are important building blocks for the CDR, but they need to be implemented in a proportionate and evidence-based manner that does not undermine the CDR's potential to achieve pro-consumer outcomes through increased competition and innovation. It should also be recognised that it is not the purpose of the CDR to regulate conduct or policy issues that are more appropriately dealt with by other laws or regulatory regimes.

2. Do the existing assessment, designation, rule-making and standards-setting statutory requirements support future implementation of the CDR, including to government-held datasets?

Currently the regulatory framework provides for the CDR to be applied to particular sectors of the economy in a phased way, with separate decision-making (and consultation) processes applying for each designation, and each set of sector-specific rules and sector-specific standards. Having separate processes creates inefficiencies and repetitive consultation processes, and risks stakeholder disengagement due to consultation fatigue. A more efficient approach could be to enable designation, rules and standards for a particular sector, or indeed a particular type of data held across sectors, to be considered concurrently and in a holistic way. This could involve a process of informal engagement with industry, ADRs and stakeholders and followed by a decision-making process that might involve a combined decision on designation and rule-making.

3. Does the current operation of the legislative settings enable the development of CDR-powered products and services to benefit consumers?

Our principal response to this question is Key recommendation (1), summarised in the Introduction at pages 8-9 above:

> **Key recommendation (1): Consistent with the competition focus of other Open Banking regimes, minimise barriers to accreditation and ongoing compliance so that more firms are encouraged to enter the CDR ecosystem instead of operating outside it**

Below we expand on the Introduction's summary of this recommendation.

Competition and Open Banking: an international perspective

UK Open Banking was founded on the goal of increasing competition in retail banking. It was part of the remedies package imposed by the UK Competition and Markets Authority (CMA), following an in-depth investigation of the retail banking market. In its final report, the CMA noted that 'of all the measures we have considered … the development and implementation of an open API banking standard has the greatest potential to transform competition in retail banking markets'.[26] The recent joint statement by the UK Government and UK regulators on the future of Open Banking highlights how greater competition has, among other things, improved access to credit and provided consumers with more information to improve their financial decisions and get better deals.[27]

Similarly, the European Commission has noted that the goals of the Revised Payment Services Directive (PSD2), the EU's Open Banking regime, are to 'facilitate innovation, competition and efficiency' as well as to increase data security standards.[28] And in the United States, the Consumer Financial Protection Bureau has described its (as yet unused) mandate to prescribe regulations for consumer-authorised data access and aggregation as holding 'the promise of improved and innovative consumer financial products and services, enhanced control for

---

[26] CMA, Retail banking market investigation, final report (9 August 2016), p. xxxvii. https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf

[27] https://www.gov.uk/government/publications/joint-statement-by-hm-treasury-the-cma-the-fca-and-the-psr-on-the-future-of-open-banking/joint-statement-by-hm-treasury-the-cma-the-fca-and-the-psr-on-the-future-of-open-banking

[28] European Commission, Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments (27 November 2017). https://ec.europa.eu/commission/presscorner/detail/pl/MEMO_17_4961

consumers over their financial lives, and increased competition in the provision of financial services to consumers'.[29]

In recent years, dozens of new firms have sought to provide consumers with insights based on their financial data. They range from budgeting applications, to services that recommend specific account propositions based on consumers' income and spending data, to software that helps small businesses better manage their invoicing and collections. The benefits from these applications have gone beyond saving money to helping those on low incomes accessing public services. Research in the UK shows how Open Banking helped 750,000 'credit invisibles' access public services and financial products.[30]

Some of these providers have built strong user bases in a short span of time - for example, Credit Karma claims to have more than 100 million members worldwide.[31] Significantly, while banks have started to offer some of these services themselves, they have typically done so only *after* challengers such as neobanks and fintechs first launched them.

These commercial developments have taken place in jurisdictions with and without Open Banking regimes - in the EU and the UK as well as in the United States, for example. But the presence or absence of Open Banking rules has affected the terms under which consumers use the new services: the UK and EU require standardised APIs and strong authentication to facilitate access to bank accounts and set a baseline for data protection. In the United States, on the other hand, these terms vary depending on the commercial agreements (if any) between data intermediaries and banks.

Besides setting the level of protection that consumers can expect, Open Banking rules affect the level of competition in the market. Open API standards and a mandate for banks to allow regulated third-party access have made it easier for challenger firms to start and scale. In contrast, the use of proprietary technology (whether bespoke 'premium' APIs or screen scraping) allows banks to choose which third-party providers consumers may use, leading to a few large intermediaries becoming the dominant channel through which fintechs access consumer bank data. Whereas there are several major Open Banking intermediaries in Europe (e.g. TrueLayer, Plaid, Tink, Token, Ecospend, Bud and Yapily), in the US Plaid is far-and-above the leading provider, and the runner-up (Finicity) is now owned by Mastercard, an industry incumbent.

The level of competition in turn affects consumer outcomes and take-up. The use of Open Banking services in the UK has grown strongly since the regulatory framework came into effect: as at March 2022 there are over 300 registered Open Banking providers, of which

---

[29] Consumer Financial Protection Bureau, Consumer protection principles: consumer-authorized financial data sharing and aggregation, p. 1.
https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf

[30] OBIE March 2022 highlights,
https://www.openbanking.org.uk/wp-content/uploads/MAR-2022-Monthly-Highlights-1.pdf

[31] https://www.creditkarma.co.uk/about-us.

nearly 250 are third party providers.[32] There are now more than 300 businesses in the European Economic Area that are authorised to provide account information or payment initiation services, which were practically non-existent before the introduction of PSD2.[33] Easy access to the regulated Open Banking space has encouraged more firms to register, leading to a broader set of Open Banking options, a higher chance of valued offerings emerging, and increased consumer take-up - all subject to strong data security standards.

The importance of encouraging the largest number of new entrants has been emphasised in recent academic research.[34] It is new entrants that are often the source of innovation and dynamism in markets, with an increased number of products (even with modest commercial prospects) delivering significant consumer benefits. The authors' conclusion is particularly pertinent to the CDR. They note that when product quality is unpredictable - which is likely to apply to new CDR-enabled products seeking to gain a market foothold - the ease of entry is an important factor in determining the value of products available to consumers. In other words, facilitating more entrants will increase the chances of some products breaking through and succeeding in delivering the best value to consumers.

The UK's and Australia's approach to regulating Open Banking compared

In the UK, the Open Banking regime does not regulate use and disclosure of data received via Open Banking APIs. Privacy and data protection obligations apply to data processors and controllers (the recipients of open banking data) under general law (including the GDPR[35]). In Australia a key difference with the regulatory regime is that the CDR not only mandates data holders to provide access to 'CDR data', it also regulates the management, use and disclosure of CDR data (which includes any data derived from that data[36]) through an enhanced privacy regime that only applies to ADRs. The concept of 'CDR data' is also much broader than 'personal information' under the Privacy Act (and 'personal data' in the GDPR) and covers information that relates to bodies corporate in addition to individuals; the privacy safeguards in the Act are expressed as protecting the privacy *or confidentiality* of consumers' data.[37]

---

[32] https://www.openbanking.org.uk/news/uk-open-banking-marks-fourth-year-milestone-with-over-4-million-users. And https://www.openbanking.org.uk/wp-content/uploads/MAR-2022-Monthly-Highlights-1.pdf. See also Chart 1 above.

[33] Kinsteller, Open Banking in Europe in Light of PSD2 Review, https://www.kinstellar.com/insights/detail/1611/open-banking-in-europe-in-light-of-psd2-review#_ftn4

[34] Rebecca Janßen, Reinhold Kesler, Michael E. Kummer & Joel Waldfogel, GDPR and the Lost Generation of Innovative Apps, May 2022, https://www.nber.org/papers/w30028. Using the introduction of the GDPR in Europe and analysing data on Google Play apps, the authors find that new restrictions imposed on data use and increased costs of compliance affected both the number of apps in the market (reduced by a third) and - more significantly - the entry of new ones (a fall of nearly 50%). The consequence of entry numbers falling was to prevent the launch of ultimately-unsuccessful *but also* ultimately-successful apps compared to pre-GDPR. The reduction in long-run consumer surplus is estimated to be 32%, and app usage (and by inference revenue) is estimated to fall by 30.6%.

[35] The General Data Protection Regulation, tailored for the UK by the UK's Data Protection Act 2018. For information about the onward sharing of data under PSD2, see https://truelayer.com/blog/data-chain-retrieving and https://truelayer.com/blog/data-chain-agents.

[36] Section 56AI(2).

[37] Section 56EA.

The privacy safeguards in the Act, and related CDR rules, are a key driver of the complexity of the CDR regime and create a material barrier to entry for CDR participation through the accreditation and compliance requirements.

For accreditation, the information security requirements represent the greatest barrier for participation and while the requirement for an independent assurance report is not provided for by the CDR rules[38], the content of the report is governed by the obligations in Schedule 2 of the rules, which include mandatory security controls. In turn the obligations in Schedule 2 of the rules relate to Privacy Safeguard 12[39] - which provides for the rules to specify the 'steps' to be taken by an ADR to protect CDR data from unauthorised access or misuse. This can be contrasted with APP 11, which provides for 'reasonable steps' to be taken to protect personal information by APP entities.

In relation to compliance obligations, the regulation of use and disclosure of CDR data under the CDR regime (through the Act, rules and standards) is complex and difficult to navigate, making it a difficult and time-consuming endeavour to determine whether a use case can be supported in a compliant manner under the CDR. For example, there are many types of use and disclosure consents, and various access pathways that need to be considered to determine if use or disclosure to an unaccredited party is permitted. Even if a use case is supported, there are many mandatory compliance requirements that apply to CDR consent flows (with little room for ADRs to develop their own approaches for consent that could enhance consumer trust and experience) and a multitude of notification requirements which add to ADR costs (eg multiple revocation methods, information kept on multiple dashboards as well as CDR receipts). Contrast this to PSD2 in the EU - where the principle of 'explicit consent' means that, as long as the consumer is informed about what data they are sharing, with whom, and for what purpose - the data can be retrieved by a regulated third party and made use of in line with the customer's instructions, which may include sharing the data with other companies, outside of the PSD2 perimeter.

Informed, express and voluntary consent is and should remain a foundational obligation in the CDR but recalibration of other CDR-specific privacy obligations should occur as a priority to ensure that momentum for participation in the CDR is not lost and the CDR can become a success. In our view, there needs to be an urgent alignment between the CDR and an economy-wide approach to regulation of personal information under the Privacy Act. Given the ongoing review of the Privacy Act, there is a risk that the levelling of the playing field between CDR and use of data in the broader economy may not occur as quickly as needed to ensure that there is a viable market for CDR-enabled products and services. In the interim, there are a number of changes to the CDR regulatory regime that could be explored in order to simplify and reduce accreditation and compliance obligations (while maintaining appropriate safeguards):

[38] The assurance report is however provided for in Schedule 1 of the rules as an ongoing requirement for ADRs.
[39] Section 56EO.

- Provide for consent, and consent related obligations like dashboards, to be regulated by the standards (and not in the rules) to provide flexibility to respond to ecosystem experience and to enable effective oversight by a CDR implementation authority[40].
    - The legislation could contain core obligations for an ADR to obtain consent to collect, use and disclose CDR data that is voluntary, express, informed, specific as to purpose, time limited and easily withdrawn, and the data minimisation principle. The standards could specify mandatory consent requirements, but should be flexible enough to allow ADRs to innovate and design consent flows to optimise consumer experience.
    - Similarly, the existing consumer notifications and dashboard requirements could be reviewed, to remove requirements[41] that increase participation costs with marginal benefit for consumers.
- Provide for ADR information security obligations to be risk-based to determine the appropriate security controls to be implemented to protect CDR data to be determined having regard to the nature of the CDR data managed by an ADR and their circumstances. This could be framed as an obligation in Privacy Safeguard 12 to take reasonable or adequate steps to protect CDR data. The requirements in Part 1 of Schedule 2 of the CDR rules would continue to apply, but there would be flexibility in relation to implementation of the security controls in Part 2 of Schedule 2 based on the ADR's risk assessment. For the accreditation process, this could enable accreditation requirements to focus on demonstration of appropriate governance, systems and controls being in place, through attestation and provision of relevant policies.[42] This could also enable applicants to rely on existing information security certifications that have partial recognition against the full suite of mandatory controls currently in Part 2 of Schedule 2.
- Explore potential amendments to the current consent and CX standards and guidelines with the aim of optimising consent, removing unnecessary friction and increasing conversion. Consideration should be given to alternate authentication and authorisation mechanisms such as mobile (app to app).

[40] This might require amendments to Privacy Safeguards 3, 5 and 10, as well as modification of the rules and standards.
[41] For example, the obligation to offer two methods to withdraw consent, providing consent records in CDR receipts and dashboards, and dashboard obligations that apply for use cases where data collection and use is a one-off event.
[42] This would align more closely with the UK where AISP applicants must demonstrate that they have robust governance arrangements and internal procedures and control mechanisms.

4. Could the CDR legislative framework be revised to facilitate direct to consumer data sharing opportunities and address potential risks?

The CDR legislative framework envisages that consumers will have the ability to direct that their data is shared with accredited third parties, or to choose to receive their data themselves 'for use as they see fit'. This aspect of the CDR ('direct to consumer' access) had its genesis in the Productivity Commission's Data Availability and Use report recommendations and was initially provided for by the CDR rules in the banking sector, but postponed following consideration of an initial draft standard for provision of direct to consumer access to data in human-readable form.

TrueLayer supports the principle that consumers should be able to access the data about themselves, and in equivalent format, that they are able to consent to share with third parties. This is consistent with the object of the CDR to create more choice and competition by empowering consumers to get the value of their data. We also consider that it would be possible for the CDR technical standards to provide for this form of access in a standardised machine-readable format with appropriate security controls.

In our view, the key issue with direct to consumer data access is not whether the framework should, and could safely, facilitate this kind of access but rather the timing and extent to which this should occur across designated sectors given the current barriers to entry that exist for participation as an ADR (and which we have discussed in the previous section). We consider that these issues need to be addressed before direct to consumer access is contemplated, otherwise this will exacerbate the issues with participation in CDR by incentivising businesses to obtain indirect access to machine-readable data via consumers to avoid CDR obligations.

5. Are further legislative changes required to support the policy aims of the CDR and the delivery of its functions?

Our principal response to Question (5) is Key recommendations (2) and (3) - both summarised above at pages 9-13. Below we expand on the Introduction's summary of these recommendations.

Key recommendation (2): To give Open Banking a decisive boost, policymakers should phase out screen scraping (as the UK and the EU have done) for Open Banking activities covered by the CDR

The experience of phasing out screen scraping in Europe

Australia is not the only market where ecosystem participants (consumers, banks, and data recipients) have disagreed about the scope for screen scraping in Open Banking. When the EU (which at the time included the UK) implemented PSD2, the European Banking Authority (EBA) that was charged with drafting regulatory technical standards proposed to ban screen scraping by reference to PSD2's security requirements.[43] These security requirements meant that all access to accounts (including via screenscraping) was regulated.

Some third-party providers (TPPs, i.e. data recipients and intermediaries) pushed back on the EBA's proposal, arguing that prohibiting screen scraping while banks had not developed dedicated APIs was premature and could undermine the goals of PSD2.[44] The European Commission, which was responsible for issuing the final rules, responded to these objections by including a fallback provision whereby TPPs would be allowed to screen scrape when a bank's API was unavailable.[45] This fallback option remains heavily used in some EU markets where bank APIs are still not functioning well.

In the UK, where Open Banking was supported by an order from the CMA (in addition to PSD2) and led by a dedicated entity, API development and performance are generally regarded as more successful than in most EU markets. Consequently, TPPs have had to resort less to

---

[43] European Banking Authority, Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2), final report (23 February 2017), p. 11.https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf

[44] See, for example, Nick Wallace, 'Commission right to reject screen scraping ban', *EUObserver*, 30 August 2017. https://euobserver.com/digital/138824 and the Manifesto for the impact of PSD2 on the future of European Fintech https://www.paymentscardsandmobile.com/wp-content/uploads/2017/05/Manifesto-for-the-impact-of-PSD2-on-the-future-of-European-Fintech.pdf

[45] European Commission, Delegated Regulation (EU) 2018/389 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R0389

screen scraping, and the scope for non-standard interface access to consumer data has been gradually reduced.[46] (In light of the UK's experience, we believe that a dedicated CDR implementation authority - see Key recommendation (3) - would help to ensure screen scraping is not necessary even as a fallback.)

Overall, the European experience shows that neither the announcement of a future screen scraping phaseout, nor its implementation over time, need discourage the growth of a rich data sharing ecosystem. The steady increase in the number of registered Open Banking providers in the UK and in the EU shows that TPPs can adapt and thrive without screen scraping.

CDR-enabled Open Banking and the market for data recipients

In the UK, consumer take-up of Open Banking has strongly correlated with entry into the Open Banking ecosystem and availability of Open Banking-enabled products and services. A similar pattern can be expected in Australia: more ADRs are likely to lead to more CDR-enabled products and services, and in turn stronger user take-up. Conversely, a smaller CDR ecosystem will reduce the range of CDR-enabled services and attract fewer users. Because there will still be new fintech offerings and user demand for them, data-sharing activity will happen, but it will be less and will mostly occur outside the regulated space.

The CDR can therefore be a tool to increase choice and competition not just in designated sectors, but in the market for data-sharing as well. At present, the prevalence of screen scraping means a few incumbent intermediaries with proprietary technology dominate - this was also the case in Europe before Open Banking rules came into force (see Chart 2). By phasing out screen scraping and moving data-sharing activity into the CDR, policymakers can create the conditions for new intermediary providers to compete with incumbents. This competition will itself drive innovation in CDR-enabled products and services and give more options to firms seeking to leverage the CDR to attract consumers.

How best to phase out screen scraping

The most appropriate way of providing for a planned transition away from screen scraping would be a matter for the Government to determine - this might take the form of amendments to the Part IVD of the Act prohibiting other forms of data access where CDR APIs have been mandated for a sector and/or through amendments to the ePayments Code. Ours is not a proposal for an economy-wide prohibition on screen scraping but instead a transition plan (with an appropriate timeframe) for moving away from reliance on screen scraping. As part of this approach, there could be a process for testing compliance of CDR APIs (similar to what occurred in the EU and UK) and the ability for screen scraping to be allowed as a fallback option where defined standards have not been met.

---

[46] Financial Conduct Authority, Changes to the SCA-RTS and to the guidance in 'Payment Services and Electronic Money – Our Approach' and the Perimeter Guidance Manual, Policy Statement PS21/19 (November 2021), p. 8. https://www.fca.org.uk/publication/policy/ps21-19.pdf

In the EU and UK, to incentivise the use of so called 'dedicated interfaces' - which in practice were implemented by banks using API technology, the following steps were taken:

- All banks were required by law to make PSD2 data available by one of two means:
    - A dedicated interface (i.e. API) or,
    - A modified customer interface - which meant the bank would still enable screen scraping - so long as the TPP complied with PSD2 identification requirements - which meant passing an electronic certificate to the bank before being allowed to screen scrape.
- Where a bank chose to implement a dedicated interface (API) - they were required to support a '**fallback mechanism**' - to enable TPPs to gain access to data via an alternative mechanism if the API became unavailable. In practice this was intended to be similar to the modified customer interface mentioned above - meaning banks who built APIs would have two 'builds' ahead of them, and two infrastructures to support.
- However, where a bank chose to implement a dedicated interface (API) - if the banks' dedicated interface met certain criteria[47] assessed by the competent authority (the FCA in the UK) - they would be exempt from the requirement to build the fallback. They would also be allowed to **block** screen scraping access - allowing access to data only through the API.

Most banks, already keen to discontinue the insecure practice of screen scraping, chose the API route, and were incentivised to ensure the quality of their APIs by the need to obtain the exemption, to avoid having to build and maintain a secondary piece of infrastructure, i.e. the fallback mechanism.

Phaseout costs?

There will be some costs to a screen scraping phaseout, notably for data recipients that currently use screen scraping, and screen scraping intermediaries. But transition costs will be limited in time and result in a safer and more transparent Open Banking ecosystem, benefiting not only consumers (and businesses) but the future growth of CDR-enabled products and services.

The European experience shows that firms that previously relied on screen scraping, such as Plaid and Yodlee, can successfully transition to regulated Open Banking APIs - further enhancing competition within the Open Banking ecosystem. Lowering barriers to entry into the CDR (Key recommendation 2) will reduce the transition costs for screen scrapers. Indeed, some of the firms involved in screen scraping in Australia are already also ADRs, which should make their transition away from screen scraping even easier and less costly.

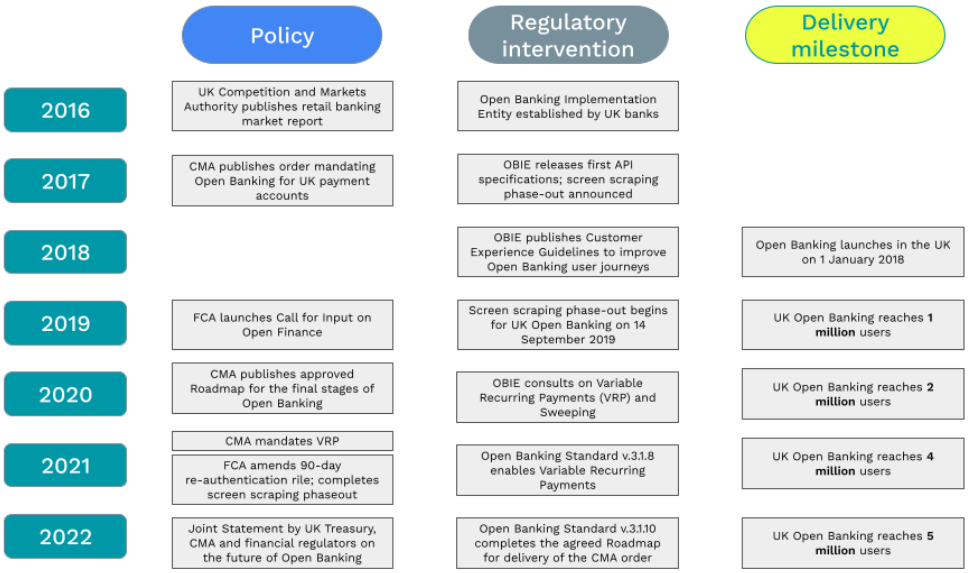
[47] https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-the-conditions-to-be-met-to-benefit-from-an-exemption-from-contingency-measures-under-article-33-6-of-regulation-eu-2018/389-rts-on-sca-csc-

Key recommendation (3): An independent authority should be nominated to be responsible for the development of the CDR ecosystem

The UK's OBIE

The UK CMA's Open Banking order required UK banks to set up an entity that would 'agree, consult upon, implement, maintain and make widely available without charge open and common banking standards' for account information and payment initiation services.[48] This Open Banking Implementation Entity (OBIE) was created in 2016 and has since worked with banks, third-party data aggregators and other financial firms to agree and implement standards and rules for Open Banking in the UK. It is funded by the UK's nine largest banks and, although its mandate will come to an end this year after completion of the CMA order, a similar entity will in future continue to monitor Open Banking and its extension to other types of accounts (i.e. Open Finance)[49].

Chart 3. Key events, regulatory interventions and milestones in UK Open Banking delivery, 2016-2022



The key insight behind the OBIE is that Open Banking is not a single event but a years-long process, requiring ongoing oversight and amendment to ensure adequate delivery of APIs, attractive user journeys and effective competition (Chart 3). As the current Trustee of the OBIE recently noted 'Four years ago, open banking was a concept in name only. Today, more than five million consumers and small businesses are benefiting from open banking-enabled

[48] Competition and Markets Authority, Retail Banking Market Investigation Order 2017, pp. 19-20. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/600842/retail-banking-market-investigation-order-2017.pdf

[49] https://www.gov.uk/government/publications/joint-statement-by-hm-treasury-the-cma-the-fca-and-the-psr-on-the-future-of-open-banking

products, and this is only the start. We did not make so much progress by accident, it was by design. The UK's leadership in open banking was enabled by our pro-competition approach and the ambition of our regulators and government. This forward looking leadership provided the confidence and the means through which innovation has flourished.'[50]

While the OBIE has at times faced criticism for high operating costs and inadequate governance, it is generally agreed that its leading role in UK Open Banking has made this regime comparably successful. Outcome metrics bear this out, with the UK by far the largest Open Banking jurisdiction in Europe in terms of users and registered firms. And whereas other official bodies involved in Open Banking had broader missions (e.g. prudential oversight or competition between payment systems), the OBIE's narrow focus made it an effective and credible advocate for the ecosystem. The OBIE's functions include taking into account the views of a wide range of stakeholders including fintechs and consumer groups, and driving the Open banking project 'forward and [taking] decisions in the interests of consumers and the promotion of competition'.[51] Importantly, the OBIE Trustee also has the power to address compliance issues directly with banks[52]. The OBIE was also staffed with technical experts who were able to effectively hold banks to account on elements of technical delivery.

The success of Open Banking in the UK can be contrasted with the 'midata' programme that the UK government launched earlier, in 2011. Midata was conceived as a bold and broad vision to empower consumers across the economy through data sharing. It would make possible new services that would help consumers 'whether it be in getting the best deal on their mobile phone contract or energy tariff, or managing their lives more efficiently'.[53] But midata lacked a dedicated authority to ensure its progress, and the programme as originally conceived stalled.

Unlike the OBIE, the Australian implementation authority need not be constrained by the OBIE's origins as part of the remedies package from a competition inquiry. Instead (similarly to the process currently being undertaken by the Joint Regulatory Oversight Committee - JROC - to design OBIE's successor entity with the extension of Open Banking and beyond to Open Finance[54]), an Australian implementation authority can be designed with the broad economy-wide vision of CDR mandate in mind, and put on a permanent footing and with permanent, but flexible, oversight powers.

Australia's CDR Implementation authority

The design of an Australian CDR implementation authority should look closely to the functions and powers that were conferred on the OBIE by the CMA order, and in particular its pro-competition mandate and ability to oversee API implementation in accordance with regulatory requirements. A key element of the new entity would be an equivalent of the OBIE

[50] https://www.openbanking.org.uk/news/cma-consultation-response/

[51] See clause 2, Schedule 1 to the CMA Order.

[52] The OBIE Trustee has the power to issue compliance directions to banks: clause 11.6 of the CMA Order.

[53] https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment

[54] https://www.gov.uk/government/publications/joint-statement-by-hm-treasury-the-cma-the-fca-and-the-psr-on-the-future-of-open-banking/joint-statement-by-hm-treasury-the-cma-the-fca-and-the-psr-on-the-future-of-open-banking

trustee - an independent appointee who can ensure that the entity's functions and mandate are fulfilled. One model would be to create a Government authority or agency, with an independent chair, and an advisory board that includes representatives from Treasury's CDR Division, the ACCC and the OAIC. The Data Standards Chair and Body could also be integrated into the new authority, given the oversight role it would have over standards implementation.

The functions of the implementation authority should include the following:

- Overseeing the implementation roadmap for the CDR approved by the Government and API implementation by data holders.
- The ability to issue directions to data holders to rectify API performance and data quality issues that do not conform with CDR requirements, and to refer ongoing compliance issues to the ACCC where necessary.
- The requirement to regularly collect and publish key CDR success metrics:
    - The number of consumers using the CDR.
    - The number of API calls (including, for example, the number of consents attempted).
    - Industry-level conversion rates[55]. The conversion rate measures the proportion of consumers who have started a user journey who go on to complete it (they are returned to the ADR after being sent to the relevant data holder to authenticate and authorise data sharing). As such it is a powerful measure of an important suite of system features and characteristics such as API availability, response times and level of user 'friction'. If there is an issue with any of these (e.g. requirements imposed on the user journey are frustrating users) then this will translate to a lower conversion rate, signalling to regulators and policymakers the need for potential corrective action.
    - API performance data that is independent (rather than self-reported by data holders) and that accurately reflects ADR experience in the ecosystem.
- Monitoring incidents raised by ecosystem participants in order to identify and address systemic ecosystem issues[56]
- Making and adjusting standards and guidelines where needed in response to ecosystem performance (e.g. consent optimisation).

[55] In the early phases, firm-specific conversion rate data may be commercially sensitive, and so we suggest that this data should only be published in aggregated industry-level form until the CDR has further matured.

[56] For information about the kinds of issues being experienced in relation to incident management, see explanation here: https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/509