Submission: options for establishing a consumer data right in New Zealand

Executive summary

1. Paymark Limited (**Paymark**) is pleased to submit on the Ministry of Business, Innovation and Employment's (**MBIE**) discussion document "*Options for Establishing a Consumer Data Right in New Zealand*".

2. In this submission we respond to three key questions raised in the discussion document: does New Zealand need a consumer data right (**CDR**); if so, what form could a CDR take; and how could a CDR be designed?

3. In summary, we support the establishment of a CDR to the extent this focuses on New Zealand's specific policy needs and delivers measurable beneficial outcomes to consumers and businesses. For this reason, we would like to see a sector-specific CDR implemented in the payments industry, where the potential for benefit is most apparent and where existing frameworks can be supplemented. However, we are wary of a more wide-ranging CDR that could delay ongoing work likely to improve the payments sector and/or impose costs on business that remain to be justified. In addition, a range of issues need to be carefully considered in order for any CDR to be workable.

4. Our key comments in relation to the CDR are as follows:

   4.1. **The CDR needs to respond to New Zealand's specific, identified policy needs**: Ideally a CDR would facilitate increased business efficiency, innovation and transparency, and allow businesses and individuals to have greater choice, flexibility and control over their data. However, the implementation of a CDR will also impose costs on business, which are ultimately borne by consumers. This means there should be a focus on where the overall benefit is most obvious, such as the payments sector. We would like assurances that a CDR would be scoped to identified problems so that these costs can be, or are, justified.[1] The balance of risks and benefits will vary by sector, and so it makes sense to consider a CDR sector by sector.

   4.2. **A "lift and shift" of Australia's CDR risks harm and may be unfit for purpose**: For the reason described in paragraph 4.1, we oppose a "lift and shift" of Australia's sectoral-designation model. New Zealand has a different economy and regulatory environment to Australia, and the CDR needs to be fit for purpose. In particular, the proposed sectoral-designation model is not focused tightly on areas of need and is likely to impose costs through a drawn-out process to design and implement an overarching regulatory framework. In relation to innovation in the payments sector, significant investment has been made through the Payments New Zealand's (**PNZ**) API Centre for the purpose of payment APIs.[2] Stalling that work while an overarching framework is designed would undermine that investment, delaying benefits that could otherwise accrue more immediately to consumers and merchants. A sector-specific approach could get off the ground much faster than a sectoral-designation or economy wide CDR.

   4.3. **It makes sense to focus on payments first:** We propose that a sector-based approach be taken with the payments industry as a pilot sector. Using the existing payments industry-led

---

[1] We understand MBIE has not undertaken any cost / benefit analysis on the use a CDR generally or in relation to specific sector, although it intends to do so. Given this, we think MBIE's preference for a sectoral-designation approach is premature.

[2] See https://www.apicentre.paymentsnz.co.nz/.

work on APIs for accessing bank account information and enabling payment facilitation would be an efficient and economical way to commence the implementation of a CDR. Rather than re-inventing the wheel through an entirely new regime, a payments-specific approach could strengthen and improve an existing framework - although open dialogue and collaboration with industry will be required. A payments first approach would be the best starting point in which to secure real benefits in a relatively short timeframe, with relatively low risks. This approach would not prevent government from introducing future sector-specific frameworks based on learnings from the payments sector or as the need becomes clearer. A more fulsome and informed legislative framework for the rest of open banking, and other sectors, could follow.

4.4. **A CDR in payments would have immediate benefits:** A CDR could potentially help address inefficiencies identified in the retail payments market by encouraging innovation, facilitating choice through competition, enabling movement between providers and requiring transparency of fees. It would ensure focus remains on an area where a CDR is likely to be mostly clearly justified. A CDR could remove the financial disincentives for merchants wishing to change payment gateways (driven by barriers to portability of card tokens[3]), reduce costs to merchants due to the bundling of debit and credit in contactless card transactions, improve choice in payment methods for consumers, make the subsidisation by poorer consumers of the rewards programmes for wealthy consumers more obvious, and free payments innovation from the constraints of the international card schemes. Moreover, Minister Faafoi has long signalled that a CDR is being considered and the payments sector has had enough time to consider and prepare for the likely implications.

4.5. **Payments sector is already trusted and is focused on security**: The work needed to implement additional privacy and security safeguards in a payments-specific CDR would be minimal given the existing security requirements. To operate successfully in the payments sector, data needs to be protected from abuse, fraud, and criminal enterprise, and a high priority is placed on information security. Payment industry participants already develop products with security in mind and new products are generally secure by design. Moreover, international certifications such as ISO 27001[4] can provide evidence of information security. These existing standards could be built into the initial accreditation process and ongoing compliance requirements. In addition, the Payments Card Industry (**PCI**) has a number of security standards that have been well embedded into the payments industry. More generally, for efficiency reasons, any sector-specific CDR should consider the existing industry certifications and look to re-use these rather than duplicate time, cost and effort in creating new accreditation criteria.

4.6. **The design of a CDR is critical to capturing potential benefits:** We support a CDR that is right-sized, supports and leverages pre-existing investments in modern payments infrastructure, allows both read and write access, navigates a sensible path between privacy and data access at reasonable cost, is shaped through the ongoing input from industry stakeholders, and is backed by real enforcement powers. However, we would question the overall value of a CDR if any one of these elements is missing.

---

[3] Tokenisation is the process of protecting sensitive card data by replacing it with a one-time use reference value called a token. It's often used to protect merchants against the security risks of capturing, transmitting and storing card data. These tokens are provided by a PCI-compliant payment provider. The payment provider securely stores the card data which can then be called upon when the merchant sends a transaction request using the token. Tokens can be passed through the internet or the various wireless networks needed to process the payment without the actual card number details being exposed. The actual card number is held safe in a secure token vault by the service provider and passed securely to the card acquirer for authorisation. Even if the token is captured by a third party after a transaction, it can only be used once and so is worthless.

[4] See https://www.iso.org/isoiec-27001-information-security.html.

4.7. **Other options are also available to address issues in payments**: With or without a CDR, there are other simple and quick interventions that would help improve the payments and banking environment. Costs to merchants (and ultimately consumers) could be reduced by mandating least-cost routing of transactions, unbundling contactless credit and debit, mandating tokenisation of eftpos cards[5] and/or an enforcement backstop for failures to meet expected timeframes for investment in modern payment infrastructure.

5. Below we expand on these points. We have also responded to MBIE's specific questions in the **attached** Appendix.

6. Note that this submission contains commercially sensitive information and that a separate, confidential version is provided.

Background

7. Paymark was established in 1984 to enable low-cost EFTPOS transaction processing, as a way of enabling banks and merchants to remove cash from the payment system and avoid the costs of cash-handling. EFTPOS transaction processing delivered effective competition and innovation in New Zealand. Since Paymark's inception in the 1980s, we have played a key role in providing safe and secure payment processing services for New Zealanders. We have evolved over time and, whilst we continue to provide payment processing for EFTPOS transactions, we also process transactions that are routed out to the global card schemes, such as Visa and Mastercard (the "schemes" and "scheme transactions"). We provide payment gateway solutions to ecommerce platforms and directly to ecommerce merchants, and we have embraced API-based technology.

8. Of particular relevance to the CDR is our recent work to improve our market offerings. Over the last five years, we have focussed on innovation and have invested millions in developing and building OPEN, a new, state-of the art API-based payment platform and new local debit payment methods for use both instore and online, such as Online Eftpos. OPEN is ready to go: two large consumer banks and two smaller consumer banks are connected. However, it would be far more efficient and ultimately beneficial to consumers and merchants if all retail banks were connected and obliged to provide access to consumers who would benefit from access to innovative payment methods. Given the small size of the New Zealand market, a fragmented approach to network infrastructure is likely to result in higher operational costs and barriers to entry – a bad outcome for merchants and consumers. A CDR could help avoid inefficiencies resulting from duplication in payments infrastructure. Many New Zealand merchants are connected to OPEN and already accept API-based payments; however, they want to offer this service to all their customers. All banks need to be connected so all New Zealanders can choose to pay for product and services online, safely, without the need for a scheme card. A CDR might help facilitate this.

Does New Zealand need a CDR?

9. We support the introduction of a CDR if it is thoughtfully conceived and implemented, and does not forestall pre-existing initiatives likely to improve outcomes for consumers and industry. However, we are concerned that a poorly considered approach may do more harm than good, particularly given that other simpler measures are available that could improve outcomes.

What is the policy problem a CDR would address?

10. In our view, a primary rationale for a CDR is to address inefficiencies and barriers to consumer benefit in the payments sector. It is not clear that a CDR is needed more generally. While the

[5] https://www.zdnet.com/article/samsung-pay-goes-live-across-the-eftpos-network-with-heritage-bank/

discussion document notes a general issue with a lack of data portability, the first pages of the discussion document refer particularly to issues within the payments sector such as:

10.1. high search and switch costs (in the payments sector this is a particular problem for merchants in relation to acquiring services and ecommerce gateway providers);

10.2. the impact of merchant services fees via online and contactless payment methods, particularly during the Covid-19 pandemic;

10.3. the inability of start-up companies in the financial technology space (fintechs) to access consumers' bank data, the corresponding rise of screen-scraping of consumers' banking accounts as a result, and the challenge of entering individual contracts with each bank for this information;

10.4. the slow pace of implementation of open banking in New Zealand via the PNZ API Centre;

10.5. the requirement for bi-lateral agreements with individual banks for the sharing of data or accessing of bank APIs;

10.6. the lack of transparency around the fees that data holders (banks) charge third parties for accessing APIs; and

10.7. data holders (such as ecommerce gateway providers) refusing (merchants) access to data in order to protect a competitive advantage.

11. We agree that these are relevant issues. We also note Minister Faafoi has linked investigation of a possible CDR with concern at a lack of measurable progress towards payment innovation in New Zealand.[6]

12. From our own viewpoint within the payments sector, we see five areas (overlapping with the above issues or other areas touched on within the discussion document) which are of particular importance and that a CDR could help address:

12.1. *High interchange reimbursement fees*: Interchange reimbursement fees have incentivised card issuing banks to grow scheme card use via customer rewards programmes, despite this ultimately costing merchants and customers in circumstances where a local debit alternative (EFTPOS) is almost free. This issue was highlighted in MBIE's 2016 issues paper on the retail payments system in New Zealand.[7] A CDR could increase competition and consumer choice and reduce this cost to the extent it allowed new and easy payment options (e.g. direct debit via mobile apps relying on payment APIs). We are supportive of any initiative that reduces merchant costs, but note that any regulation of merchant fees, including interchange reimbursement fee regulation, should not be contemplated in isolation of any CDR (and vice-versa), so as to ensure consumer benefit. In particular:

12.1.1. EFTPOS transactions are increasingly being supplanted by scheme transactions, which reduces competition and choice for both merchants and consumers in New Zealand. The demise of EFPTOS would render the payments industry beholden to the international schemes and their notion of innovation. If only the global scheme products

---

6 Hon Kris Faafoi *Open letter to API Providers regarding industry progress on API-enabled data sharing and open banking* (December 2019).

7 Ministry of Business, Innovation and Employment *Retail Payments Systems in New Zealand – Issues Paper* (October 2016).

remain, "innovation" will be entirely directed by the schemes, thereby reducing the small amount of competition that exists today. Iterations on the old do not result in the best outcomes for consumers. The true innovative shifts come from building the products and platforms we should have built (knowing what we know now).

12.1.2. Despite our best efforts, it is already challenging to move incumbents in the payments industry to new payment products and networks largely due to the financial incentives associated with the interchange fee model. The interchange model might be rational for individual decision-makers at issuing banks, but it results in sub-optimal or inefficient outcomes for New Zealanders collectively. The rapidly increasing proportion of scheme cards in use, escalated due to a rise in contactless transactions further to Covid-19 safety concerns, will reach a tipping point where too few merchants will be able to steer transactions away from those that attract interchange fees. "NZ Inc" should be wary of becoming beholden to the schemes for its payment processing system.

12.2. *Bundling of credit and debit for contactless payments*: Merchants who wish to offer contactless payment options are required to offer both credit and debit options. They cannot choose to offer one without the other. This results in high transaction costs for the merchant (given high fees for contactless credit when compared to contactless debit and contactless more generally when compared with contact or dip/swipe) which are ultimately passed on to consumers.[8] As alluded to in the discussion document, this has been a particular issue since the onset of the Covid-19 pandemic when contactless options have become more important. Although interchange reimbursement fees for contactless debit were reduced, the interchange reimbursement fees applied to contactless credit fees were not. Furthermore, we've heard anecdotally that the interchange reimbursement fees for online transactions were, at the same time, increased)[9]. A CDR could encourage alternative competitive contactless payment options.

12.3. *Switch costs for merchants using payment gateways*: Merchants who wish to switch online payment gateways are disincentivised from doing so, because incumbent payment gateways may not agree to the transfer of card tokens to a new provider or will do so only at significant cost. If tokens are not transferred, merchants' customers need to re-enter their card details (and may default on recurring transactions), which can lead to a significant drop-off in customer payments. This issue could be substantially mitigated if the CDR provided a right for merchants to transfer card tokens to a new provider at no, or a reasonable, cost. Lessons can be learned from the telecommunications sector where the incumbent mobile operators were protected until such time as number portability was enabled, thus driving a competitive mobile market.

12.4. *Transparency of fees*: Currently it is difficult for merchants to access information about the cost of acquiring services generally. Merchant services fees generally consist of acquirer fees, processing fees and interchange reimbursement fees. These fees are bundled together and it's challenging for merchants to get a clear picture of their fees. If the fees were more transparent, merchants would more easily be able to compare and switch between acquiring banks. Transparency and therefore competition would be promoted if a CDR included obligations for product information (including pricing by banks and schemes) to be more freely available.

---

8 Evidence from Retail NZ suggests average merchant services fees for contactless debit and credit (at 1.1% and 1.5% respectively) are significantly higher than for merchants in Australia (0.6% and 0.8%) and the United Kingdom (0.3% and 0.6%). See Retail NZ *2019 Retail NZ Payments Survey* (May 2019).

9 Neither Mastercard nor Visa publish previous interchange reimbursement fee rates on their website, making it difficult to make any comparison between the interchange reimbursement fees applying today versus at an earlier point in time.

12.5. *Delay in the implementation of open banking APIs*: Since 2017, PNZ's members and pilot participants have been working together on the development and implementation of API standards for open banking via the API Centre. The introduction of payment APIs would potentially address a number of the issues described above. However, despite the standards being well developed, progress towards implementation has been slow (as noted by Minister Faafoi more than once).[10] In our experience, without any enforcement consequences banks have had little incentive to prioritise resources to the implementation and support of APIs which could require updating of legacy systems and erode parts of their business model. By way of example, we have been involved with the industry working group since 2017 and are a foundation member of the API Centre. Despite this position and our technological readiness, we are yet to execute a bi-lateral agreement with an API provider for the use of the standardised APIs (note, we have executed contracts for use of our own non-standard payment APIs). Smaller fintechs, such as the Kiwi start-up Choice to Pay which initially participated in the API Centre, now appear to no longer have the ability to do so given the ongoing financial and in-kind contributions required to participate. A CDR could help to heighten the priority of progressing APIs within financial institutions. This would likely lead to increased transparency and competition in the payments sector, lower innovation barriers, and assist new entrants (for example, fintechs offering new consumer products) to participate in the emerging fintech sector.[11]

13. Similar benefits from a CDR may be relevant to other sectors but to a varying extent, and with varying degrees of urgency. In other words, while there is a good overall policy case for a CDR in the payments sector, the same may not be true of other sectors. Furthermore, an overly broad CDR risks delaying benefits where they are warranted, as well as distracting away from tools that may be more effective. For this and reasons we discuss further below in paragraph 15, we support a sector-specific CDR.

Alternative mechanisms can also address some of these policy issues

14. With or without a CDR, many of the issues described in paragraph 12 could be helped through complementary measures which can be implemented more immediately. These include:

14.1. *Mandating least-cost routing*: In Australia, there has been an ongoing push to encourage "least-cost routing" to prevent unnecessary fees being charged to merchants for contactless transactions.[12] In other jurisdictions, such as Sweden, merchants must be allowed to choose the form of routing for online transactions that best serves their needs and budget.[13] Mandating least-cost routing would have an immediate effect on merchant and consumer payments costs in New Zealand, by allowing the avoidance of unnecessary fees where a cheaper alternative is available. This change could be achieved through a simple change to the PNZ rules - legislative change is not necessarily needed. This solution is easy technically - the rule change would simply align contactless debit rules with dip and swipe debit rules.

---

10 See Hon Kris Faafoi *Speech to Payments NZ Conference 26 June 2018* (26 June 2018); and Hon Kris Faafoi *Open letter to API Providers regarding industry progress on API-enabled data sharing and open banking* (December 2019).

11 We understand that financial institutions that are also API providers rationally choose to prioritise regulatory requirements that have significant consequences for non-compliance over industry-led initiatives, which may go some way explain the lack of progress. However, behaviour and outcomes are likely to change if there are real world consequences for failure to progress APIs. Parallels can be seen elsewhere. Spark fought the introduction of new technology (fibre) stating it wasn't required as they tried to protect their incumbent revenues. It was only by creating independent fibre networks that competition in the retail broadband space and the provision of new services occurred. This evolution moved New Zealand up the broadband OECD ladder and made us better prepared to cope with Covid-19

12 See for example the Reserve Bank of Australia's explanation here, which includes links to a number of Australian government report calling for this least cost routing.

13 Under the Swedish Payment Services Act (2010:751).

Scheme debit cards, when dipped or swiped are already routed to local payment processors. Why should contactless debit be treated differently?

14.2. *Regulation of interchange reimbursement fees*: Merchant fees could also be reduced by some form of regulation of the scheme-set interchange reimbursement fees. Interchange reimbursement fees are a revenue stream for the issuing banks (paid by the acquirer to the issuer for each scheme transaction). The acquiring bank recovers this per transaction fee from the merchant. Several other jurisdictions such as Europe and Australia regulate interchange fees by capping charges paid to the issuers. However, simply capping interchange reimbursement fees without providing for data portability should be treated with caution and creates the risk of unintended consequences as highlighted in paragraph 12.1. While in the short-run capping interchange fees could improve merchant costs and benefits to consumers, if this led to the demise of EFTPOS it would also remove an existing competitive constraint, further increasing scheme dominance that in the longer run is likely to lead to increased costs to consumers and merchants. In particular, reducing interchange fees could eliminate any incentive for the banks to invest in new API-based technology or engage with fintechs to deliver more efficient and cheaper payment products. This in turn could stop, not merely limit, investment in technology, both for continued reliability and to maintain comparable functionality with scheme services. It could prevent entry of innovations and technology not sponsored or provided by schemes or international challengers, such as Apple. It is common that market players that lose revenue as a result of regulatory intervention look for new revenue sources, potentially to the detriment of consumers, so if interchange fees are capped, we would want to see a framework that ensures the benefit of any cap on interchange fee regulation is passed on to the consumer both in the short and longer term.

14.3. *Enforcement for failure to progress API implementation*: There are currently few direct consequences for banks' failure to progress implementation of payment APIs. Given the standards are well-developed, the other participants in the API Centre pilot have invested significant sums and time into their success, many of the benefits of a CDR within the payments sector could be realised simply by mandating direct consequences for banks' failure to meet expected milestones for API implementation. The nature of any enforcement powers would need careful consideration but would create incentives for banks to prioritise innovation and reward existing investments in API development.

What form could a CDR take?

We support a sector-specific form of CDR

15. As set out above, we prefer a sector-specific approach, beginning with payments:

15.1. A sector-specific approach allows key problem areas that could readily benefit from a CDR to do so quickly (since the balance of risk and benefit varies by sector). Expansion could take place over time, as further benefits are identified. Other industries, such as telecommunications and electricity, have already made progress towards forms of data portability and/or addressed barriers to consumer benefit, ahead of payments. Focus should therefore be on payments - where problems have been identified, but not yet solved. Existing but as yet unrealised work in the payments sector, such as the API standards developed through PNZ, could be leveraged for more immediate benefit, rather than being delayed while other sectors "catch up". Our experience is illustrative of the importance of progressing the CDR in this manner:

15.1.1. We have invested approximately [redacted] over a period of [redacted] in advancing API technology. As outlined above, we have built OPEN[14], an API-based payments platform, and developed new methods of paying, such as Online EFTPOS[15]. We've also successfully piloted facial recognition technology and worked with merchants to provide new products (such as Online EFTPOS)[16] to help customers buy goods through their banking app without a card. But, these innovations are not yet available to all Kiwis, given the two-sided nature of the payments market (requiring both merchants and consumers to participate) and the banks' role in determining access to payments products. Many merchants interested in using these innovative and less expensive products are hesitant if only a subset of consumers can use them. But, consumers can only use these new products if they are supported by their banks. A CDR based on existing work progressed via the PNZ API Centre could move the dial and create real change in payments, by requiring the banks to allow consumers and merchants access to new products they want. Despite varying degrees of readiness,[17] nearly all of New Zealand's retail banks have been involved in the PNZ API Centre work, supporting the opportunity for these benefits to be quickly realised. However, Paymark and other industry participants cannot keep on investing in these alternative payment methods if there are no means to ensure banks will connect consumers and merchants. The significant investment in the API Centre "pilot" work is likely to be squandered if banks and other participants are inclined to stop work until an overarching regulatory framework is developed.

15.1.2. We support a sector-specific CDR because this would incentivise the continued development and acceleration of work that is already underway, rather than requiring work to be re-started in a prescribed form, by creating "hard" or enforceable deadlines for compliance.

15.2. As discussed more below, privacy (a key consideration) and data protection more generally are heavily ingrained in payments and banking. Existing regulation and high standards in the payments sector would ensure a material head start for a payments-specific CDR, compared to other sectors. Furthermore, any entity that processes card data must comply with Payment Card Industry Data Security Standards (**PCI DSS**).[18] We apply similar standards, which relate to keeping card data safe and secure, to our API-based products even though there is no card data – and this same approach is likely to be feasible for others in the payments sector.

15.3. A "lift and shift" of the Australian model is not suitable for the New Zealand market. The Reserve Bank of Australia has a continued focus, proactive engagement and oversight of the payments industry (including regulation of interchange fees, implementation of least cost routing and the support of a domestic debit scheme) that is simply not present here. Hence, Australia is not an appropriate comparison for the proposed CDR as it relates to the payment sector. More generally, we would expect the degree of existing competition and consumer benefit applicable in relevant sectors of Australia's economy (to the extent this justifies a sectoral-designation approach) to be different to those same sectors in New Zealand, given our different economy, market size, and regulatory regimes. MBIE should, however, review the challenges Australia faced when implementing a CDR, learn from these and find out what they

---

14 See https://www.paymark.co.nz/future/.

15 See https://www.paymark.co.nz/products/online-eftpos/.

16 See https://www.invenco.com/s/news/invenco-technology-puts-nz-motorists-in-fastlane-20Y2w000000cHCJEA2.

17 See https://www.apicentre.paymentsnz.co.nz/standards/available-standards/api-provider-readiness/.

18 See https://www.pcisecuritystandards.org/.

would have done differently, given Australia's progress to date. We note the Australian CDR does not include "write access" which means payment initiation is out of scope. We consider a New Zealand CDR needs "write access" to ensure the problems identified in the discussion document, as they relate to payments, can be addressed.[19]

16. While a CDR could be good for New Zealand, we believe that MBIE's analysis of options against the proposed assessment criteria - justifying MBIE's preference for a sectoral-designation approach – appears in some instances to have been assessed using erroneous assumptions. For example:

    16.1. We note that almost all of the "pros" for a sectoral-designation approach specified on page 15 of the discussion document could potentially apply to a sector-specific approach, but have not been included as such.

    16.2. There is no recognition in the discussion of "cons" on page 15 that a sectoral-designation approach will impose costs through delay and the inability to leverage off existing investment. The analysis suggests that significant implementation costs for sectoral-designation would be offset by overall efficiency gains but it does not make the same point about sector-specific approach, where the argument is much stronger given existing implementation work on payments.

    16.3. There is no recognition that some of the criteria are not a good in themselves. For example, given every sector will face costs through the imposition of a CDR, it is speculative to assume that increased potential "reach" is necessarily always a good when applied to other markets/sectors that are already functioning well and where consumers will effectively offset the regulatory costs put on businesses.

How could a CDR be designed?

17. As noted above, any CDR needs to be right sized and carefully designed in order to be worthwhile. Below we discuss key issues that need to be explored to ensure the success of a CDR. In summary, we consider that a CDR regime must:

    17.1. allow access to consumer data or product information at a reasonable cost;

    17.2. have a competent, well-resourced, and collaborative regulator with appropriate enforcement powers;

    17.3. build on existing work (such as the API Centre), rather than undermining existing investments and/or reinventing the wheel;

    17.4. navigate a sensible path between privacy considerations and data access, and in particular should allow for "write access", contemplate use of intermediaries with appropriate security infrastructure, and take account of the risks to vulnerable consumers; and

    17.5. ensure that the scope of the CDR right, and the definition of the subject data, is fit for purpose (e.g., by taking account of distinctions between primary data versus enhanced data, whether the CDR applies to existing or future data, how shared data is dealt with, the extent of third party rights, and the jurisdictional scope of the right).

---

[19] To allay any fears, we emphasise that payment initiation or the facilitation of payments under a CDR would not by themselves "move the money". The banks would still use the existing clearing and settlement systems managed by PNZ to settle funds

What issues need to be further explored for the proposed CDR?

18. Assuming that a CDR is justified (alone or in addition to any alternative measures described in paragraph 14), a CDR will need to be right-sized to take account of a number of factors which would affect its workability and effectiveness. The discussion document raises some but not all of these at a high level.

19. First, to be of practical use, access to consumer or product information will need to be at a reasonable price (or free). This issue was not explicitly raised in the discussion document, but is essential to the functioning of an effective CDR. For example, we understand that some payments gateways are technically able to transfer card tokens where a merchant wishes to switch providers, but only provide these tokens at a cost that materially deters switching. Likewise, the argument that a CDR will facilitate innovative products by new entrant fintechs hinges on an assumption that those parties will be able to access customer data at a reasonable cost. Therefore, a CDR regime should include an appropriate costs framework that takes account of issues such as systems and administrative costs to the data provider, as well as the impact of these costs on data consumers and third-party providers.

20. Second, the discussion document only briefly touches on who would oversee and enforce the CDR regime. We think that the CDR should sit in a separate and distinct piece of legislation, but do not have a firm view as to whether the regulator should sit within an existing agency (e.g., the Commerce Commission) or be a new body. However, we would prefer there to be one agency (to avoid risking overlapping or conflicting regulatory jurisdiction).[20] Whatever agency oversees the CDR, the regime's effectiveness will depend significantly on that body having:

    20.1. the resourcing capacity and jurisdiction to effectively oversee the regime;

    20.2. quality staff with an understanding of the sector where the CDR applies (e.g., expertise in relation to payments and financial markets, competition, and privacy and technology), and the ability to work constructively and collaboratively with industry participants; and

    20.3. appropriate enforcement powers to ensure that the benefit of the regime is realised.

    A well-resourced regulator with a willingness to work with industry and where necessary exercises enforcement powers would be critical to the effectiveness of a CDR.

21. Third, and as discussed above, any CDR regime needs to recognise and leverage off the existing investment made by participants in PNZ's API Centre work, and be developed with the direct input of industry. Otherwise, there is a risk that existing work that could benefit consumers will stall and investment will be lost. Technical and commercial issues regarding the implementation of payment innovation will need to be recognised and worked through (e.g. through the involvement of industry working groups), and lessons from the API Centre work to date incorporated.

22. Fourth, in a CDR regime it will be necessary to navigate a sensible path between privacy and data access. In this regard, a number of points should be considered:

    22.1. *Read / write access is essential*: Although we appreciate that "write" access could raise additional privacy risks because it may facilitate disclosure of consumer data to third party providers, we consider that it is essential in order to realise the full benefits of a CDR (e.g. by

---

[20] A recent report from the Australia senate supports the creation of a single independent body under their sectoral-designation regime. See Australian Senate, Select Committee on Financial Technology and Regulatory Technology *Interim Report* (September 2020).

allowing for third parties to access bank account information and change the data to initiate a payment). A well-thought through consent framework and high privacy standards would mitigate key risks. However, a CDR limited only to read access would reduce the CDR's scope to transparency benefits (e.g. the ability to compare and switch providers), without necessarily helping grow a payments ecosystem that fosters new products and innovation, nor fixing the payments problems referred to in the discussion document. We also note that there seems to be some confusion in the market as to what "write access" for payments would mean. Some financial intuitions appear to be confusing data and messaging with moving money. Write access, when used for payment initiation, would merely provide a mechanism for consumers to instruct a payment. The existing payment systems, managed by PNZ, would then be used to move the money (by way of clearing and settlement).

22.2. *Payment sector already has high privacy standards:* As mentioned above, pre-existing privacy precautions taken by banks, and payment system participants support the argument for a discrete financial sector CDR that allows write access, and undermine arguments that a CDR will impose significant additional costs for privacy compliance. In general, participants in the financial sector already adhere to high privacy standards, both because it reduces the risk of fraud and reputational damage, and because of the regulatory standards to which participants are subject. Such standards include PCI DSS, and general precautions required for compliance with the Privacy Act 1993. Such precautions could be expanded for the purpose of a CDR without necessarily incurring significant additional costs.

22.3. *Identity verification processes already exist*: Likewise, banks and payments industry participants already have processes in place to identify individuals to comply with "know your client" obligations under the Anti-money Laundering and Financing Countering of Terrorism Act 2009. As such, those in the payments sector are likely to already have significant investments in the identity verification products and standards that will be important to validate consumers' consent to read and write access under a CDR. Moreover, the Department of Internal Affairs' Identification Management Standards provides an obvious starting point for identity verification, along with ongoing complementary work in relation to Digital Identity Trust Framework.

22.4. *Vulnerable groups and consent need consideration*: Care will need to be taken to work through consent processes for more vulnerable individuals. For example, how will consent be managed in relation to blind people when they authorise access to a third party or initiate payment? Will young people be able to rely on a CDR, and if so, are there any additional precautions that should be in place? Will there be protections against predatory conduct by providers (for example, a budgeting service that reads a consumer's transaction history and cross-sells other products)?

22.5. *Cost of privacy standards, accreditation and use of intermediaries*: Although we agree that appropriate privacy standards are important to ensure trust in services provided via a CDR, the costs of compliance need to be distributed so as to encourage smaller players to enter the market. The onerous requirements for accreditation under the Australian regime has in many cases locked out (or significantly slowed the entry of) these providers and reduced the overall benefit that a CDR might be expected to return, benefitting only incumbents. The discussion document notes the possibility of third-party intermediaries that would be accredited and able to perform key obligations on behalf of other parties (e.g. smaller businesses that do not have the capacity to easily implement onerous privacy precautions). Recently Australia updated its CDR to permit accredited intermediaries to collect data on behalf of third-party data recipients, with consumer consent. The change means accredited businesses can use the infrastructure of an accredited intermediary to connect to data holders' APIs, and do not need to build their own. We think this approach would be important under a New Zealand CDR regime, and we would be well positioned to act as an infrastructure intermediary enabling data sharing in a safe and secure way. The use of intermediaries would allow New Zealanders to benefit from consistent rules for data access under shared data infrastructure and governance. Under this

model, data would not be accessed for free by anyone for any purpose. Instead\clear rules and standards could be prescribed to protect consumers' and businesses' data, while at the same time opening up the industry to competition. However, before this could be considered in a New Zealand context, the commercial framework would need to ensure that those intermediaries, that are likely to be burdened with the cost of continued compliance, would be able to sufficiently commercialise data.

23. Fifth, there remains significant ambiguity regarding the scope of a CDR, which would need to be addressed. In particular, the definition of the data subject to the CDR needs to be carefully considered, as this will significantly affect both the utility and cost of a CDR. We make the following comments:

    23.1. To maximise the potential benefits of a CDR we support including both customer data and product data (e.g. the transfer of card tokens). If a CDR includes pre-existing data, this may impose additional costs but could also be a source of significant benefit to consumers and businesses. If pre-existing data is caught, there would need to be a limit to the age of the data caught and sensible exceptions to avoid imposing unreasonable costs and/or unworkable obligations on businesses.

    23.2. It is unclear whether the CDR would only apply to data produced after the introduction of the regime (forward looking data) or also pre-existing customer data.

    23.3. It is unclear how consumer data would be distinguished from, for example, merchant data or financial institution data.

    23.4. Special consideration would need to be given to ensure appropriate coverage for shared data (for example. where there is a shared bank account, or the information concerns payment from one individual to another), given separate obligations that might apply to the information in contract or under the Privacy Act.

    23.5. The jurisdictional scope of the CDR right is unclear. For example, would it apply to entities that do not pay tax in New Zealand but might provide services to New Zealand customers? In our view, it may be appropriate to adopt a test similar to the Companies Act (and soon to be introduced under the Privacy Act) that hinges on "carrying on business in New Zealand". It is unequitable for New Zealand registered business only to be subject to a CDR. Some of the biggest holders of data (for example, Facebook, Google, Amazon, WeChat, Alipay) should be treated the same as any New Zealand business if they hold the data of individuals based in New Zealand.

    23.6. The scope of third party rights is unclear. For example, would other businesses (third parties) be able to seek information, or only customers themselves or on consent from the customer?

    23.7. There is no mention of commercial considerations. Would data providers be able to recover costs, will intermediaries (as referred to in paragraph 50 of the discussion document) be able to charge reasonable fees to cover their compliance obligations? For this purpose, we think "raw" or "primary" data and "enhanced" or "derived" data are different and should therefore be treated differently.

24. Sixth, the practical ability to implement a CDR needs to take account of providers' existing technology systems and would require significant standardisation to be useful. For the avoidance of doubt, we are not suggesting that the choice or use of technology is regulated, but there does need to be some sort of consistency in respect of data output. This will include the need for:

    24.1. ongoing lifecycle management, to avoid the risk of fragmenting versions and standards undermining standardisation, and

24.2. specification of support standards, platform security, fault / incident management, and consequences for when access to CDR goes down due to systems failures.

Conclusion

Paymark is grateful for the opportunity to submit on the issues raised in the discussion document, and supports a payments sector-specific CDR on the basis outlined above.

Should you wish to discuss any of the points raised in this submission, please contact Pip White.

Appendix – summary of responses to discussion document questions

Does New Zealand need a consumer data right?
Are there any additional problems that are preventing greater data portability in New Zealand that have not been identified in this discussion document?
• The cost of access to non-personal data, such as card tokens / card data held by ecommerce payment gateways. • Digital identity initiatives have not matured.
Do you agree with the potential benefits, costs or risks associated with a consumer data right as outlined in this discussion document? Why/why not?
• We largely agree with the possible benefits. • We do not consider that the document has appropriately addressed the following risks and costs: - that a CDR risks delaying and undermining significant work and investment towards payment APIs. - that currently data portability can come at a cost (i.e., as imposed by banks and others) that may undermine the viability of innovation. - the extent to which privacy accreditation may pose a barrier to entry for fintechs, favouring incumbents. - the risk of costs and dysfunction through fragmentation and poor lifecycle management - the danger of rigid or poorly conceived standards that have not been developed with industry, and do not work. - that the CDR is applied in sectors of the economy, or designed in such a way, that the costs of implementation do not just the net benefits.
Are there additional benefits, costs or risks that have not been explored in the above discussion on a consumer data right?
• See question 2 above. • Consent processes must be well designed. • Liability flows have not been explored. • Any CDR should apply to entities that interact with consumers including the large international data holders such as Facebook and Google.
What would the costs and benefits be of applying the consumer data right to businesses and other entities, in addition to individuals?
We agree that businesses should have access, and control, of their data as we think it would encourage business to move between service providers more easily, which would, in turn, encourage competition.
Do you have any comments on the types of data that we propose be included or excluded from a consumer data right (i.e. 'consumer data' and 'product data')?
We agree with including both product data and consumer data within the CDR. We note that defining what is "consumer data" will be a difficult exercise. In the payments sector, a payment transaction can include processor data, merchant data, cardholder data and bank data. All of this data would need to be within scope of the CDR if New Zealand wishes to solve the payments problems highlighted in the discussion document. More generally, the definitions of "consumer data" and "product information" will need to be drawn so as to ensure this does not undermine reasonable confidentiality protections usually applied for trade secrets.
What would the costs and benefits be of including both read access and write access in a consumer data right?
Unless write access is within scope of the CDR it is difficult to see whether any increased competition

will be realised in new payments methods. An initiation of a payment cannot take place based on read access to data. We recognise that others within the sector consider that "payments initiation" is moving money and therefore it is not data and should fall outside of the scope of CDR. We disagree with this position. Whilst elements of settlement do "move money" at the payment initiation level, this is not the case.

What form could a consumer data right take in New Zealand?

Do you have any comments on the outcomes that we are seeking to achieve? Are there any additional outcomes that we should seek to achieve?

We agree with the outcomes. However, we would also like for the problems to be identified so that the cost of a CDR is justified, and the design of the CDR is crafted to provide the best "fit" for those problems.

Do you have any comments on our proposed criteria for assessing options? Are there any additional factors that should be considered?

We agree with the criteria, however the application and analysis of the criteria does not quite make sense to us. We're not sure on how the initial analysis of options against assessment criteria were achieved. Refer to paragraph 16.

Do you have any comments on the discussion of Option one: Status quo?

This is not an option. If no regulatory framework or enforcement backstop is put in place it is all too easy for businesses to continue with existing business models that favour incumbent providers' profits over and above consumer welfare. Other regulatory items and business needs will continue to be prioritised over the industry-led initiatives.

Do you have any comments on the discussion of Option two: A sectoral-designation process?

Refer to paragraph 4.

This option will take too long for it to be fit for purpose for all industries. It's challenging to standardise legislation as all sectors have own issues and complexities and one-size-fits-all always challenging. The time taken to craft an overarching model is likely to forestall initiatives that could result in more immediate consumer benefit.

Do you have any comments on the discussion of Option three: An economy-wide consumer data right?

This option will take too long, be too complicated or be too simple. There is a danger the right will be so non-specific as to be rendered useless, resulting in nothing meaningful ever getting progressed or implemented. We note that the economy-wide data portability right implemented via the EU's General Data Protection Regulation (GDPR) was developed as part of a process that took the best part of ten years, and given its broad application is only described in narrow terms in the text of the GDPR itself.

Do you have any comments on the discussion of Option four: Sector-specific approach?

We agree with a sector-specific approach and suggest that the sector be narrowly defined to begin with. This approach would give greater flexibility, agility and will allow for faster implementation. It is more likely to identify problems and allow for the design of outcome-based solutions. It makes sense to start small, achieve results and then branch out. This approach will be faster to market as it's tailored to the relevant sector. This approach does not prevent learnings from the pilot sector being applied in other sectors, or as part of a broader framework to be developed subsequently.

This discussion document outlines four possible options to establish a consumer data right in New Zealand. Are there any other viable options?

Pilot or proof of concept in payments, with real enforcement consequences for implementation failures. This would capitalise on work done by PNZ, increase momentum and realise benefits for consumers and merchants.

Do you have any comments on our initial analysis of the four options against our assessment criteria?

Yes, we're not sure that the criteria are correct or that they have been correctly applied, refer to paragraph 16.

We think some of the assumptions require explanation. In particular, we're not sure why MBIE views a sector-specific approach as less useful than a sectoral-designation approach, nor why factors such as speed and cost do not seem to have been given sufficient weight compared to other areas. For example:

- Trust – sector-specific is rated lower on privacy on the assumption that accreditation and shared standards wouldn't apply. It is unclear why;
- Reach – we note that while sector-specific CDR would be less wide ranging than other options, reach is not a good in itself. Arguably, it is only useful insofar as it addresses perceived problems / provides obvious benefits, and should only be weighted to the extent it maps appropriately against these. It is also unclear to us why a CDR couldn't begin in problem areas and be expanded via complementary legislation in future if justified;
- Speed – it is unclear why sectoral-designation and sector-specific are rated the same. This seems wrong. We consider sector-specific will be much faster in delivering real benefits to sectors with known problems or obvious scope for improvements;
- Cost – sector-specific is rated as higher cost than sectoral designation. This doesn't appear to acknowledge that there will be significant implementation costs for businesses in all cases, and focusing where there is the greatest chance for upside could provide the greatest net benefit / reduced cost; and
- Flexibility – sector-specific is rated the same as sectoral-designation, although arguably it would allow for more sector-focused solutions.

Do you agree or disagree with our assessment that Option two is most likely to achieve the best outcome using the assessment criteria?

We disagree, please refer to paragraphs 4, 15 and 16.

How could a consumer data right be designed?

Do you agree with the key elements of a data portability regime as outlined in this section? Are there any elements that should be changed, added or removed?

We note that an onerous accreditation regime could become a barrier to entry and that a sensible balance needs to be found. We note that being a member of the API Centre incurs costs by way of financial and in-kind contributions. We are not convinced that an accreditation regime will remove the need to have a bi-lateral agreement with data holders, unless the CDR also specifically sets out the price and liability framework for which access will be provided to third parties.

Do you have any feedback on our discussion of any of these key elements?

We do agree that limitations on the prices charged by data holders needs to be considered. The technology used to make the CDR available needs to be reliable and have high availability. If it isn't always available this will lead to a bad customer experience and limit the opportunities for innovative, real time products to be developed.

Are there any areas where you think that more detail should be included in primary legislation?

The legislation needs to make sure that all relevant entities are captured by the legislation so that a level playing field is achieved. For example, overseas companies that operate or that New Zealand consumers use should not be excluded from regulatory jurisdiction.

Data platform stability, and service levels, should be considered.

How could a consumer data right be designed to protect the interests of vulnerable consumers?

Consumer consent is important when considering data rights and use. Collaboration with

representatives of vulnerable consumers should take place from the start, and their expertise should be considered and incorporated.

Do you have any suggestions for considering how Te Tiriti o Waitangi should shape the introduction of a consumer data right in New Zealand?

We are supportive of recognising data as taonga. The CDR should be developed in a way that builds trust and value for Māori.

How could a consumer data right be designed to ensure that the needs of disabled people or those with accessibility issues are met?

The legislation, which is about accessing and controlling consumer data, should be accessible to all consumers, by design. Collaboration and consideration should be incorporated from the start.

To what extent should we be considering compatibility with overseas jurisdictions at this stage in the development of a consumer data right in New Zealand?

Refer to paragraphs 4 and 15.3.

We think New Zealand should progress its own path. We cannot think of any glowing examples of overseas legislation and as New Zealand is small (sub-scale market) the complexity of overseas legislation would cost too much, take too long to implement and fail to deliver measurable benefit to consumers.

Do you have any comments on where a consumer data right would best sit in legislation?

Refer to paragraph 20. We think a standalone act would make it clearer.

Do you have any comments on the arrangements for establishing any new bodies to oversee parts of a consumer data right?

Refer to paragraph 20.

What are the pros or cons of having multiple regulators, or a single regulator, involved in a consumer data right?

We think a single regulator that is resourced appropriately and has capable expertise in relevant sector(s) would be most effective. We note that recent reports out of Australia support the suggestion of a single regulator clear jurisdiction.

If government decides to establish a consumer data right, do you have any suggestions of how its effectiveness could be measured?

- Number of new participants in the sector – increased competition.
- Innovation of products and services.
- Costs to consumers decrease.
- Ability to switching between providers improves.