18 October 2024

Submission: Open Banking Regulations and Standards

Executive summary

1. Paymark Limited trading as Worldline New Zealand (**Worldline**) is pleased to submit on the Discussion Paper released by the Ministry of Business, Innovation and Employment (**MBIE**) entitled 'Open banking regulations and standards under the Customer and Product Data Bill' (the **discussion document**).[1] Worldline thanks MBIE for granting us an extension to the published deadline.

2. Worldline previously submitted back in 2020 in response to the initial consultation, on the Draft Exposure Bill in 2023 and the Customer and Product Data Bill (the **Bill**)[2] itself in September 2024 (both written and oral). We note that given the short time frame to respond, following the deadline for written and oral submissions on the Bill, we have not had a chance to thoroughly analyse the questions posed and the impact on our business and our wider our industry. We are concerned that consultation period has not been long enough to gather the feedback required to ensure the regulations and standards will be fit-for-purpose. This may result in a higher risk of harmful unintended consequences.

3. In this submission, we provide general feedback on the proposed regulations and our answers to the questions posed are set out in **Appendix 1**. Please note that our submission contains commercially sensitive information and that a separate, confidential version is provided. In summary:

   3.1. One of the biggest challenges is getting banks on board. The banks have the relationship with consumers, so they are vital to the success on any new debit product. Kiwibank and the Tier 2[3] banks (together the **Tier 2 Banks**) are often overlooked but they are essential for the future success of open banking products by all consumers. Limiting the Customer and Product Data (**CPD**) regime to only the "Big 4"[4] plus Kiwibank will limit the success of the regime.

   3.2. In payments, we are already at risk of several overlapping accreditation processes, standards, regulators, and legislative regimes (see paragraphs 33 and 34 for more information). These regulatory frameworks need to be coherent and work in harmony with each other, rather than competing or conflicting. They should be created, and developed, by industry in co-operation and collaboration with the various regulators and there must be a clear mechanism for versioning. The regulatory burden of compliance and cost of participation, including the levy, could dampen innovation and competition.

---

1 See https://www.mbie.govt.nz/have-your-say/exploring-a-consumer-data-right-for-the-banking-sector

2 See https://www.legislation.govt.nz/bill/government/2024/0044/latest/LMS700098.html

3 See chapter 2 for more information https://comcom.govt.nz/__data/assets/pdf_file/0019/362035/Final-report-Personal-banking-services-market-study-20-August-2024-Amended-27-August-2024.pdf

4 ASB, ANZ, BNZ and Westpac.

3.3. The discussion paper canvasses issues on the scope of designation, regulations and standards. While not fully clear, it appears that MBIE's goal is to have supporting regulations and standards in place to underpin a designation of the banks, targeting 1 December 2025. It is not clear what the delineating distinction between a CPD regulation and a standard is. It's also unclear exactly how industry standards fit in relation to a designation of the interbank payment network being proposed by the Commerce Commission[5] and the API Centre's standards, terms and conditions. These factors, together make the end-state regulatory model opaque, confusing, and challenging to navigate.

3.4. The next steps are also unclear. We hope that any regulations drafted pursuant to this discussion document are published seeking public consultation. Timing of this 'consultation' seems slightly off as it has been published before submissions on the Bill closed. The Bill should be finalised prior to consultation on the regulations otherwise there is a foundational risk which undermines the consultation process. There are obligations in the Bill to consult before setting the regulations. We are concerned this discussion document will be used as a box ticking exercise as regards the consultation obligations required by the Bill, rather than seeking industry collaboration and agreement on the regulations.

3.5. We are also concerned that many questions in the discussion document are very technical. We have already built products that comply with the API Centre standards, which were developed and agreed upon by the industry. Roadmap for API standards[6] must be clear and future ready. Performance of APIs must improve. Presently the bank APIs are not robust enough to deliver consumer trust in open banking payment products. Industry collaboration is necessary when determining regulations - technical standards and regulations, which are imposed on the industry, should not be determined via consultation and written submissions. We want to see continued industry engagement enabling future ready standards that include ISO20022 for data rich messaging and for instore products.

3.6. As a first mover in open banking, Worldline has made a significant investment in developing technology and APIs[7] that comply with international best practice. Should the CDR regime enable less expensive access costs going forward, then those who have gone first should also be able to benefit from those access cost reductions without putting the rest of their existing access agreements at risk. The success of the CDR regime could be derailed if data holders are able to charge accredited requesters access fees that are too high.

3.7. Lastly, safety and security are crucial to building and maintaining trust in the consumer data right (**CDR**). Digital identity services should be embedded from the beginning and to further protect New Zealanders from harm, services that use.

---

5 See https://comcom.govt.nz/__data/assets/pdf_file/0018/362025/Retail-Payment-System-Recommendation-to-the-Minister-to-designate-the-interbank-payment-network-August-2024.pdf

6 See https://paymentsnz.atlassian.net/wiki/spaces/PaymentsNZAPIStandards/overview

7 Application Programming Interfaces (APIs) work as a highly secure channel, allowing two different systems to safely communicate with each other and share information.

Worldline New Zealand

4. Worldline New Zealand was established in 1984 to provide low-cost Eftpos[8] transaction processing as a way of enabling banks and merchants to move from cash to electronic payments. We are New Zealand's leading payments innovator, and we design, build and deliver payment solutions that help Kiwis succeed. Worldline New Zealand has been a part of Worldline SA, our parent company (a French corporation), since 2020. Worldline NZ is New Zealand's leading payments innovator, formerly Paymark. We are a NZ registered business with 180+ employees in Auckland.

5. 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), provide payment gateway solutions to ecommerce platforms and directly to ecommerce merchants, and are leaders in embracing API-based technology for open banking payment services. We connect to over 80,000 merchants and over 40 financial institutions.

6. Over the last 7 years, we have focused on innovation, investing millions in developing and building an API-based payment platform[9] and new local debit payment methods for use both instore and online. We have fully integrated payment APIs with the four largest New Zealand consumer banks and one of the smaller banks. We have New Zealand's first online open banking payment product called "Online Eftpos".[10] Over 500 merchants accept Online Eftpos as an ecommerce payment method. Next, we are looking to digitise Eftpos so it can be used instore via your phone and over our payment APIs.[11]

Commercial matters

7. Many other jurisdictions have not seen huge successes after implementing an open banking or open data regime. The anticipated benefits of open banking have not yet been realised in the United Kingdom largely due to regulatory uncertainty and a lack of viable and sustainable commercial models.[12]

8. Ideally the CDR regime will 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 the CDR regime will also impose costs on business. We would like assurances that the costs of becoming accredited under the CDR regime would take that into consideration and that any imposed levy[13] does not have a stifling effect. We would like reassurance that MBIE is considering that payments businesses (such as Worldline) are facing several designation regimes (for the same business activity).[14] Where possible, minimising the uncompensated and avoidable costs of compliance and participation in the CDR regime.

---

8 Eftpos stands for "electronic funds transfer point of sale".

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

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

11 See https://www.paymark.co.nz/blog/new-conttactless-payments-taking-off/

12 See https://www.finextra.com/the-long-read/891/open-banking-year-six-jrocs-priorities-and-the-uks-future-roadmap

13 Sections 129 and 130 of the Bill https://www.legislation.govt.nz/bill/government/2024/0044/latest/LMS700098.html

14 Retail payments (interbank network), financial market infrastructure (FMI) and Digital Services Trust Framework (DISTF).

9. These proposed regulations do not provide enough detail to fully understand what the accreditation criteria will be nor what the application process entails or the associated costs. We note that being a member of the API Centre incurs costs by way of financial and in-kind contributions and that to be a trusted digital identity service provider a firm must also seek accreditation under the Digital Identity Services Trust Act 2023[15] (**DISTF**). To reduce counter-productive compliance costs and maximise uptake, the CDR regime will need to address any overlap with other existing (and emerging) regulatory regimes and seek out opportunities to lighten the compliance burden and cost of participating.

10. The technology used to make the designated data available needs to be reliable and have high availability. For that to happen, the data holder needs to be incentivised (either via regulatory or rational means). If a service isn't always available, and the data quality is poor, it could lead to a bad customer experience and limit the opportunities for innovative, real-time products to be developed. Even so, data holders should not be able to impose access prices on accredited requestors that are too high or there is a risk they impede competition and innovation. For example, for payments, the access price charged by a data holder should not make it difficult (or impossible) for the service provider to compete with the international card schemes.

11. The options proposed require considered thought and more targeted industry engagement. The payments use case is different to the information use case and a 'one size fits both' approach may not be suitable. We suggest that more targeted consultation take place, specifically in respect of access pricing. For payments, the following items, at a minimum, need to be considered:

    11.1. The access pricing must not be prohibitive; third parties need to be able to put together a sensible and achievable business case in respect of their products and services;

    11.2. The access pricing cannot be so high as to make it difficult for third parties, or fourth parties, to compete with incumbent payment solutions (such as Visa & Mastercard); and

    11.3. Assessing pricing on use case may sound like it's a good idea (price for risk, opportunity, etc) but it could result in subjective rather than objective assessments being undertaken by API providers and third parties would need to agree bilateral contracts with API providers (where the bargaining power is imbalanced).

Lack of competition

12. The decline in local debit usage both affects consumer choice and has broader implications for our financial autonomy. As transactions increasingly move to the international card schemes, we risk becoming entirely dependent on these systems, which could lead to higher costs for consumers and reduced competitiveness for local businesses. While both the Commerce Commission and the Reserve Bank have noted that it is undesirable for New Zealand's financial stability to have payment processing solely in the hands the international card schemes, there continues to be a lack of action on this important issue that will help avoid that outcome.

---

[15] See https://www.legislation.govt.nz/act/public/2023/0013/latest/LMS459583.html

13. It is crucial that we explore and support alternative payment methods that can sustain and enhance our domestic financial infrastructure. Encouraging innovation in this space will not only provide more options for consumers but also ensure that our financial system remains robust and competitive.

14. Fintechs are vital to a flourishing ecosystem and there are some great apps in the market which help with money management. However, most either use a Scheme product, such as prepaid cards (which are not subject to the interchange fee caps) to make the actual payment or they use sub-optimal methods such as reverse engineering and screen-scraping. Fintech's have struggled to get bilateral agreements with banks, so they have little choice but to partner with the Schemes. Worldline has an open banking payment platform, and agreements with the four major banks plus Co-op and Heartland, but those agreements do not allow us to provide payment services to other Fintechs.

15. We would like to support Fintechs to use our payment capability instead of the Schemes. We believe this could provide better outcomes for consumers and merchants, removing unnecessary costs of doing business in New Zealand, but: 1) our API agreements do not provide for partnering; 2) we pay the banks to access APIs so we need to charge the Fintechs; and 3) we cannot compete with the incentives given to Fintechs and banks by the Schemes, which particularly in the case of banks, has a strong tying effect and drives a lot of their behaviour in the market.

16. PNZ is driving a framework for open banking via the API Centre, and it is doing its best in an unregulated environment. However, focus on instore payments is lacking. There is no strategy to retain or protect domestic payments whether that be via open banking or traditional payment cards.

17. Eftpos is woefully outdated. The rules for issuing and accepting Eftpos are owned and managed by PNZ yet these rules, and therefore the product, have not been kept current. The substantive acceptance and card design rules remain the same as they were in the 80s. Eftpos machine terminal hardware is an end-of-life product to be superseded by Softpos or 'Tap on Mobile'. Magnetic stripe on the card is an end-of-life technology, and once Tap on Mobile becomes the acceptance device of choice, the Eftpos card can no longer be used. This will likely occur before the 2030 date in which magstripe is no longer allowed by Mastercard. To ensure consumers can use domestic payments easily, and that a competitive constraint on the Schemes remains, we need to replace Eftpos with a more modern product before it is completely gone.

18. Already, some merchants are no longer providing contact (insert/swipe) payment facilities, opting solely for contactless payments to take advantage of the ability to recover costs by applying surcharges. There are new acquiring and terminal offerings in market that are Scheme only, they do not accept Eftpos cards. The contact Scheme debit is sent to the acquirer and Scheme instead of the issuer, locally (in breach of PNZ rules). Very soon, in the absence of meaningful and urgent market intervention, all payments will be Scheme payments. This will have a significant and immediate effect on consumers and merchants. Merchant service fees (**MSF**) will apply to all transactions. Merchants are worried about the prospect of increased costs, and critically, consumers will no longer have a 'surcharge-free' non-cash payment option. Simply regulating surcharges will not be sufficient, as has been demonstrated in other jurisdictions.

19. The payments industry needs to have a comprehensive conversation regarding the future of Eftpos and the move to a new domestic digital debit solution, which can compete with the Schemes and provide real benefit to consumers.

20. In our view, this "future Eftpos" will be an account-to account API product, which can be used online and instore by all merchants. It will have lower overall infrastructure costs compared to existing legacy systems (including Scheme), and, in time, it will combine payments with digital identity and loyalty. However, this sort of innovation requires the payments industry to work together, as it did when Eftpos was first introduced. So far that collaboration is missing, and, in the absence of regulatory drive, perhaps this is an opportunity for the public sector to leverage private sector capability via a public-private partnership to accelerated innovation.

21. We cannot continue to invest in the future of debit (whether online or instore) if we are reliant on a "one bank at a time" approach, particularly when each bank takes years to engage, commit, and the finally deliver. Their willingness to invest profits in improving, innovating, and developing infrastructure at a pace that is commercially viable for Fintechs, and promotes competition, is lacking. Worldline therefore supports cohesive regulatory push that enables pro-competitive outcomes.

API standards need better performance & more functionality

22. The API standards do not currently contain all the functionality required for online transactions let alone instore transactions. Some items are on the API Centre's Minimum Open Banking Implementation Plan (**API Centre Implementation Plan**), but many are not. We are not convinced the API Centre standards will contain everything we need in the version to which API providers will need to build to when targeting the June 2026 fully operational date.

23. If we are to see real competition in the interbank payment network for bill payments, automatic payments, direct debits and direct credits as referred to in the New Zealand Commerce Commission's (**NZCC**) recent proposal to designate the interbank payment network[16] then all banks need to implement enduring consent. MBIE's proposals on consent with respect to payments are not correct. We suggest that if MBIE wishes to alter the consent requirements set out in the API Centre terms and conditions it should be done in a collaborative way with industry players so that the regulations reflect reality.

24. Neither the API standards nor the API Centre Implementation plan provides for instore transactions. For instore transactions, it must, at a minimum, be mandatory that the APIs carry data rich ISO20022 based schema.[17] Moreover, if the banking industry does go ahead with a real-time payments system[18], APIs need to be using that messaging scheme to integrate (and for any existing API-based products to remain relevant). Currently APIs are being built that have little chance of integrating to a real-time system which again, drives uncertainty into the payments innovation market. ISO20022 schema is also necessary for the implementation of robust digital identity services.

25. The API Centre Implementation Plan is largely dictated by the banks as API providers; the third parties must just wait. The standards can only be developed as fast as the slowest bank. While the efforts undertaken so far are steps in the right direction, the API Centre Implementation Plan does not provide sufficient certainty, or the functionality needed to ensure open banking will be fully operational by June 2026. In addition, the

---

[16] See https://comcom.govt.nz/__data/assets/pdf_file/0022/348070/Retail-Payment-System-Consultation-on-our-proposal-to-recommend-designation-of-the-interbank-payment-network-27-March-2024.pdf

[17] See https://blog.seeburger.com/iso-20022-payment-integration-for-real-time-payments/

[18] See https://www.paymentsnz.co.nz/our-work/next-generation-payments/

banks, as API providers, can seek exemptions or extensions from the API Centre. Enforcement is weak as it is via the API Centre membership terms and conditions and there is no real consequence for non-compliance.

26. The lack of certainty is delaying progress in payments innovation. Third-party providers require broad access to banks' APIs to ensure the commercial success of new products. The difficulties we have faced in penetrating the banks has massively (and unnecessarily) inflated the cost of bringing Online Eftpos to market and delayed its ability to stand as a profitable product. Smaller Fintechs without existing stable revenue streams cannot achieve this and we are not permitted to help them. Furthermore, in our stakeholder discussions relating to our Online Eftpos product, Tier 2 Banks non-participation or extended deadlines have been cited to us as a reason for merchants (including government departments) to continue to use POLi. POLi uses screen-scraping, which is less secure as it requires consumers to share their internet banking login credentials with third parties (often contravening banks' terms and conditions). Bank delays in implementing the API standards not only hinders payments innovation but indirectly incentivises and encourages less secure payment methods.

27. Currently, limited resourcing of banks' API products and services means operational service levels are often low, up-time is unreliable and response times can be poor. If something goes wrong, it can be challenging to find someone at the bank to fix it. While there is obvious consumer demand, the lack of resourcing from banks has also been damaging to trust in the product where the resulting unreliability has created a poor experience.

28. The performance expectations of payment APIs on API providers set out in the API Centre standards are too low. Consumers lose faith in payments products if they do not work. Having a 99.5% up-time per month is not good enough and indeed none of the API providers we connect to actually meet this. For example, recently, one API provider was down for 5 hours on the Saturday and 8 hours on the Sunday, and this API Provider has been down for over 120 hours so far this year. This unavailability severely impacts the reputation of, not just our open banking payment product, but all open banking payment products. The up time needs to be at least 99.9% per month (at 43 minutes of potential downtime per month, it is still higher than what the public's expectations are and is significantly lower than the standard we are put to on our traditional payments switch). An availability expectation of 99.5% per month (as set out in the API Centre standards) equates to unavailability or down-town of over three hours a month and over two days a year – payments solutions should not be down when people want to pay. API Providers should provide an availability uptime and fix completion times that show that they are providing a service that is robust enough to drive consumer trust and confidence in open banking payment services.

29. The user experience needs more priority and focus. Common complaints, in addition to poor performance, are that banking apps require too many steps and that transaction value limits are not commensurate with the level of risk for a merchant. Critically, some banks have extra steps for the first API transaction, but this is not clearly communicated to consumers - if the first experience is too cumbersome, people are less likely to use it again.

30. Greater certainty over banking implementation of API standards would help reassure payments innovators that regulators are serious about providing a climate in which payments innovators can succeed.

The Tier 2 Banks are vital for the success of open banking

31. The commercial success of any payment innovation ultimately depends on the support of the banks. We agree that there has been very limited investment by the major banks in their core systems. These legacy systems do constrain the ability of the banks to innovate and compete. The major banks cite compliance costs as the number one reason for not being able to give more to open banking. The other reason, and arguably the one that influences banks' overarching behaviour, is profit. Commercially rational, banks want to protect Scheme products that return significant revenue to the issuing banks.

32. All banks ought to be championing open banking and a domestic debit product to help Kiwis succeed. The Tier 2 Banks absence from the open banking ecosystem continues to have a negative impact. Government entities, and retailers, have repeatedly told us that enabling Tier 2 Bank customers is a requirement for them to consider using Online Eftpos. They say that having the four major banks is not enough. Without the Tier 2 Banks participation in open banking, the market and Government agencies will continue to accept outdated screen-scraping solutions which hinder the success of open banking and normalise the risky behaviour of sharing internet banking credentials.

Clear roles & responsibilities of overlapping regulatory jurisdictions

33. The payments industry is navigating its way through several regulatory initiatives across several different regulators. We consider it vital that the CDR regime enabled by the Bill is interoperable with other related frameworks; not just the Privacy Act 2020[19] but also the Retail Payments System Act 2022[20] (**RPS Act**), the Future of Money, the Council of Financial Regulators vision for payments[21] & the Digital Strategy for Aotearoa and the DISTF Act. There is an opportunity to ensure that the differing regulators work together efficiently across all these data sharing regimes and frameworks. They need to be coherent and work in harmony with each other, rather than competing or conflicting. Duplication across regimes should be limited. The regulatory burden of compliance and cost of participation could dampen innovation and competition.

34. The NZCC in their Recommendation to the Minister to designate the interbank payment network[22] has said that they will work with MBIE in developing the CDR regime and that a memorandum of understanding may be necessary to agree respective roles and avoid regulatory overlap. We would like to understand exactly how the NZCC's roles and responsibilities will interact with MBIE's and these proposed regulations when it comes to payments. The potential for conflict and overlap is significant and determining which regime takes precedence in the case of conflict could be challenging to navigate.

35. From our perspective, many regimes appear to cover similar ground and there are overlaps and dependencies. This is challenging for businesses, like us, who will be caught in the middle of several new regulatory measures – indeed we are looking at

---

[19] See https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html

[20] See https://www.legislation.govt.nz/act/public/2022/0021/latest/whole.html

[21] See https://www.cofr.govt.nz/news-and-publications/payments-vision.html

[22] See page 3 paragraph 7 of https://comcom.govt.nz/__data/assets/pdf_file/0018/362025/Retail-Payment-System-Recommendation-to-the-Minister-to-designate-the-interbank-payment-network-August-2024.pdf

potentially three different designation regimes[23] and at least two accreditation processes.[24]

Data policy

36. It is not clear that the data policy applies to our use of data generally or whether it only applies to our use of the data that is obtained as an 'accredited requestor' pursuant to the CPD Bill. We would like clarity on that. Notwithstanding, the data policy requirement does not appear to be hugely different from a well set out privacy policy and we are supportive. We think that consumers should have that information available to them in the areas set out below and in respect of data that is obtained by us as an 'accredited requestor':

    36.1. Data minimisation: accredited requestors are required to minimize data collection to only what is necessary for the service provided.

    36.2. Purpose of data use: the policy must explain all the purposes for which the customer data is used and clearly identify who benefits from each purpose.

    36.3. Use of de-identified data: if de-identified customer data is used, the policy should explain all purposes for which it is used and who benefits from each purpose.

    36.4. De-identification processes: the policy should also detail how customer data is de-identified to meet privacy and security standards.

37. For security reasons we would not want to disclose where our data is stored geographically. If we reveal this information, we may inadvertently provide potential attackers with valuable intelligence that could be used to identify vulnerabilities or exploit our systems. Maintaining a level of ambiguity in this regard is essential for protecting any sensitive data and mitigating the risk of unauthorised access. We could perhaps disclose at a country level where data is stored so that consumers could research the legal regimes in those countries but not anything more granular than that.

The detail

38. *Consent:* The proposed regulations as regards consent for API-based payments are considerably different to what happens today. We would caution against MBIE changing these without engaging collaboratively with the industry, especially considering consent requirements are already set out in the API standards and have been worked through over a number of years. Consent for payments is managed by the API provider. Changing this would mean substantial work to a product which is already in use, and which has received zero complaints as to use and consent.

39. *Derived Data:* The definition of derived data is very broad and may compromise data holders' proprietary insights. We recommend that the legislation has mechanisms to limit the scope of what "derived" means, and that it specifically excludes materially enhanced information[25] or information that has been "de-identified".[26] In Worldline's

---

[23] Retail payments (interbank network), financial market infrastructure (FMI) & DISTF

[24] DISTF and CDR

[25] See https://www.oaic.gov.au/consumer-data-right/consumer-data-right-legislation,-regulation-and-definitions/consumer-data-right-data

view, de-identified data, derived data and data that has been materially enriched by a data holder using their own internal methods should be excluded from the CDR regime, particularly if it is protected by existing intellectual property rights. Furthermore, applying the CDR regime to pre-existing (7 years) of data[27] could be highly problematic and costly.

40. *Digital identity:* The use of digital identity services as a verification and authentication mechanism will be key to ensuring the 'authorisation' to share data has been given by the individual to whom the data relates or, in the case of a business, under the correct delegated authority. While it seems obvious that the identity of all entities in the data sharing chain need to be verified, we do not know how this will be done. The number of scams and fraudulent claims by those pretending to be others (whether it be someone pretending to be an individual or a business) are many, varied, and increasing both in frequency and sophistication. For this regime to be successful, New Zealanders will need to trust the system and its processes. Robust digital identity services need to be embedded in the regime from the beginning to provide reliable verifiable authentication that a person or business is who they claim to be. Businesses and consumers both need access to these services and verifiable credentials need to be issued not only private data holders but core Government agencies, such as the Department of Internal Affairs, Ministry of Transport, Ministry of Health, Ministry of Education, Inland Revenue and the Ministry of Social Development. Worldline suggests that MBIE engages with Digital Identity New Zealand (**DINZ**).[28] DINZ has an impressive range of members across many industries and could provide valuable support to MBIE on their journey towards creating a safe data sharing environment.

41. *Screen scraping should be banned*: Worldline firmly believes that any service that requires consumers to share their online banking credentials with third parties should not be allowed to operate. These services access the bank accounts of others using their login credentials to retrieve account information or make money transfers. The purpose of this legislation to is enable the secure sharing of data. It seems contrary to the purpose to then let unsafe practices continue. If these unsafe methods are allowed to operate, firms may not choose to go through the cost of accreditation when they can simply go around the regime. We note that recently Minister Bayly has said that he expects screen-scraping to make an orderly exit[29] but, without prohibition and enforcement, New Zealanders are still being put at risk. We understand that there is a desire to solve the issue of screen scraping by making it 'easy' for POLi and other such services to move to APIs. This is great news for those New Zealanders that use POLi, and other screen scraping services, as their data will be safer. However, as a first mover in open banking, Worldline has made a significant investment in developing technology and APIs that comply with international best practice, and we pay banks for accessing their APIs. Should the CDR regime enable less expensive access costs going forward, then those who have gone first should also be able to benefit from those access cost reductions without putting the rest of their existing access agreements at risk.

---

[26] See https://www.cdr.gov.au/sites/default/files/2024-01/De-identification-of-CDR-data-under-the-Consumer-Data-Right-guidance-published-31-January-2024.pdf

[27]

[28] See https://digitalidentity.nz/

[29] See https://businessdesk.co.nz/article/finance/bayly-expects-screen-scraping-to-make-orderly-exit-from-open-banking

Comms plan

42. Worldline would like to see clear and transparent communications published by Government around the risks and benefits of the regime. It would be wonderful to see trusted advisors across sectors, communities and iwi out educating businesses and consumers.

43. Consumers need to know who they can trust and who is accredited. A trust mark (or something similar) to identify that a data requestor is accredited would be beneficial. However, we need to know more about how this be managed and monitored. Consumers need to be able to rely on the trust mark so there needs to be accountability when or if an accredited requester ends up being untrustworthy.

Conclusion

Worldline is grateful for the opportunity to submit in relation to the proposed open banking standards and regulations. We are excited to be a part of what should become a thriving open data network. We would like to work together, within our industry, and across others to truly unlock the value of data for New Zealand consumers and business. We hope further consultations, in respect of designations, regulations and standards, will be given the time and attention needed ensure success of the regime.

We are supportive of the increased focus on the digital economy, but we would like to see more alignment and cohesion. Having many regulators with overlapping priorities can be challenging. We are at risk of several overlapping accreditation processes, standards, regulators, and legislative regimes. How these regulations and the designation of the interbank network combine to enable progress and give New Zealanders access to innovative products and services. Investment in open banking is considerable and requires certainty.

We welcome the opportunity to work collaboratively and cooperatively with MBIE to assist in delivering on the overarching objective; to promote competition and innovation for the long-term benefit of customers.

Should you have any questions in the meantime, please contact Julia Nicol, Head of Public Affairs, Regulatory & Corporate Communications on julia.nicol@worldline.com.

Appendix 1

Status quo and problem definition	
1.	How do you expect the implementation and use of open banking to evolve in the absence of designation under the Bill? What degree of uptake do you expect?
	It will continue slowly under the API Centre. This discussion document does not appear to expedite anything not already in plan. We would like to see the Tier 2 Banks included. We do not think it appropriate for MBIE to be so involved with the technical detail – where something is already in the API standards (and therefore agreed by the industry), MBIE should not seek to change those by a written submission consultation process. MBIEs role should not be in developing technical standards, it should be in creating a market by regulating fees, standardised terms and conditions, and accreditation criteria for open access. MBIE should also consider allowing for entities such as Worldline to open-up access to its API payments platform to fourth parties. Shared infrastructure can provide a cost-effective way for other Fintechs to get to market quicker.
2.	Do you have any comments on the problem definition? How significant are the risks of suboptimal development and uptake under the status quo?
	This regime does not appear to be expediting or improving anything that has not already been agreed upon by the industry. We need Tier 2 Banks, we need enforcement of dates, we need more progress on API standards and better API performance.
3.	What specific objectives should the government be trying to achieve through a banking designation? What needs to happen to achieve these objectives?
	Wide-spread use of payments products that can compete with Visa & Mastercard. We need a modern version of Eftpos before it exits the market. Consumers like using Online Eftpos which means they appreciate having a choice when shopping online. We are seeing record transaction numbers each month (noting that these numbers, while positive, are significantly lower than our traditional payment products). Online Eftpos also receives positive feedback from consumers, despite the fact the experience is not as seamless as it could be. They say that it is “fast”, “easy”, “secure”, “simple” or “easier than entering bank card details” and they like that merchants seldom apply a surcharge. We can bring that experience instore if regulatory impetus and bank support is present.
4.	Do you have any comments on the criteria that should be used to assess designation options?
	Accreditation should not just be in respect of the data requestor being fit and proper but that the use case for which the data is being requested is robust. Each service/use case should itself be accredited alongside the data requestor as a company.
The Scope of an open banking designation	
5.	Do you agree that the banks covered, and timeframes should be based on the API Centre Minimum Open Banking Implementation Plan? Do you have any concerns about the specific implementation dates suggested?

	Too slow and the other banks are missing. The API Centre implementation plan is largely dictated by the banks as API providers; the third parties must just wait. The standards can only be developed as fast as the slowest bank. While the efforts undertaken so far are steps in the right direction, the API Centre Implementation Plan does not provide sufficient certainty, or the functionality needed to ensure open banking will be fully operational by June 2026. In addition, the banks, as API providers, can seek exemptions or extensions from the API Centre. Enforcement is weak as it is via the API Centre membership terms and conditions and there is no real consequence for non-compliance.
6.	Do you have any views on the costs and benefits of designating a wider range of deposit takers, beyond the five largest banks?
	All banks should be included only then will all New Zealanders have access to safe open banking products. If the smaller banks are excluded unsafe practices, such as screen-scraping and reverse engineering will continue.
7.	Do you agree that, in the first instance, only requests by accredited requestors be designated? Do you have any comments on when and how direct requests by banking customers could be designated under the Bill?
	No comment.
8.	Do you have any comments on the customer data to be designated?
	We would like to continue having access to the same customer data that we have today in accordance with the API Centre standards.
9.	Do you have any comments on whether product data should be designated? What product data should be included? When should the product data designation come into force?
	Transparency of fees, including processing fees, in payments would be welcome especially from Apple and the international schemes.
10.	Do you have any comments on designating payments under the Bill? Should other actions be designated? If so, when?
	Interplay between the CPD regime, the API Centre and the Commerce Commission's potential designation of the interbank network is confusing. It is difficult to picture what the end state may be and how the different regimes interact.
The benefits, costs and risks of an open banking designation	
11.	Do you agree with our assessment of how the designation will affect the interests of customers (other than in relation to security, privacy and confidentiality of customer data)? Is anything missing? For businesses: What specific applications and benefits are you aware of that are likely to be enabled by the designation? What is the likely scale of these benefits, and over what timeframe will they occur?
	No comment.
12.	Do you agree with our assessment of the costs and benefits to banks from designation under the Bill (other than those relating to security, privacy or confidentiality)? Is anything missing? For banks: Would you be able to quantify the potential additional costs to your organisation associated with designation under the Bill? i.e. that would not be borne under the Minimum Open Banking Implementation Plan.
	No comment.
13.	Do you agree that the designation will promote the implementation of secure, standardised, and efficient regulated data services?
	Yes, if dates and standards are mandated and enforced.

14.	Do you have any comments on the benefits and risks to security, privacy, confidentiality, or other sensitivity of customer data and product data?
	No comment.
15.	Are there any risks from the designation to intellectual property rights in relation to customer data or product data?
	Yes, derived data where the data has been materially enhanced should be excluded.
Accreditation criteria – what specific criteria should business need to meet before they can become accredited to make requests on behalf of consumers?	
16.	Do you have any insights into how many businesses would wish to seek accreditation, as opposed to using an accredited intermediary to request banking data? For businesses: How likely are you to seek accreditation? What would make you more or less likely to apply?
	We will apply if the regime is more beneficial to us than the existing agreements we have. For example, we would like to support Fintechs to use our payment capability instead of the Schemes. We believe this could provide better outcomes for consumers and merchants, removing unnecessary costs of doing business in New Zealand, but: 1) our API agreements do not provide for partnering; 2) we pay the banks to access APIs so we need to charge the Fintechs; and 3) we cannot compete with the incentives given to Fintechs and banks by the Schemes, which particularly in the case of banks, has a strong tying effect and drives a lot of their behaviour in the market.
17.	Do you agree that directors and senior managers of accredited requestors should be subject to a fit and proper person test? Do you have any comments on the advantages or disadvantages of this test, or other options?
	Accreditation should not just be in respect of the data requestor being fit and proper but that the use case for which the data is being requested is robust. Each service/use case should itself be accredited alongside the data requestor as a company.
18.	Do you agree that requestors whose directors and senior managers have already met the 'fit and proper' licensing or certification test by the Reserve Bank, Financial Markets Authority or Commerce Commission should be deemed to meet this requirement without further assessment?
	No comment.
19.	Do you consider that, in the absence of insurance or guarantee requirements, there is a significant risk of banks or customers not being fully compensated for any loss that might reasonably be expected to arise from an accredited requestor breaching its obligations?
	Potentially, yes, in the absence of insurance mitigating the risk.
20.	Do you have any comments on the availability and cost of professional indemnity insurance and/or cyber insurance, and how this may impact on the ability of prospective requestors to participate in this regime?

	Yes, public and products liability including professional indemnity. In respect of the banking sector, MBIE may wish to utilise work already completed by the API Centre in respect of insurance. Any entity/company should have appropriate current liability & professional indemnity insurance cover prior to entering the regime. We do not see how a cyber insurance would cover anyone other than the insured, i.e., it's not going to help anyone related to the incident other than whoever is paying the premium. We have not seen a policy which covers third parties. Need to be careful not to make the regime too expensive - costs imposed on third parties may be too high and onerous which may impact uptake.
21.	Do you agree that a principles-based approach similar to the Australian CDR rules is an appropriate insurance measure?
	Yes.
22.	Do you agree that accredited requestors in open banking should be required to be a member of a financial services disputes resolution scheme?
	Yes, but would be good to utilise one of the existing options and not make them cost prohibitive otherwise it may impede adoption. Worldline is already a member of Financial Services Complaints Limited (FSCL) and that costs ***CONFIDENTIAL*** (based on the number of Online Eftpos transactions we process), and the FMA's fees are currently ***CONFIDENTIAL***. This could go up if the API calls/requests increase. We are a member of FSCL as it is a requirement of being registered as a Financial Services Provider because we are 'involved in managing the means of payment', particularly for Online Eftpos. For people to have confidence in the system it is healthy for there to be an independent resolution service for complaints. Having said that, to the extent requestors are enabled for the designated information not designated actions (i.e. payment initiation), the transaction is about personal data and isn't (strictly speaking) a financial transaction so perhaps the Privacy Commissioner be a more appropriate route for complaints. It would be better to power them up and make the Privacy Act more fit for purpose and give the Privacy Commissioner some teeth to issue proper fines.
23.	Do you consider that information security requirements should form part of accreditation?
	Yes, we think that ISO27001 compliance should form part of the accreditation.
24.	Do you have any comments on the level of prescription or specific requirements that should apply to information security? For businesses: What information security standards and certifications are available to firms in New Zealand, and what is the approximate cost of obtaining them?
	In addition to the API Centre security requirements, we think that ISO27001 compliance should form part of the accreditation. For us, the project is approximately ***CONFIDENTIAL***.
25.	Do you agree that additional criteria of accreditation be the applicant demonstrate compliance with its policies around customer data, product data and action initiation and with the Act?
	Depends on what is involved. MBIE should consider the overall burden on accredited requesters. If the regime is too onerous it could impede uptake.
26.	Do you consider any additional accreditation criteria are necessary?
	Security and insurance requirements that are perceived as onerous, may make access expensive or impossible.

Fees – what restrictions should there be on fees for providing customer data or initiating payments?	
27.	What would be the impact of requests under the Bill being free, for banking?
	Please refer to paragraphs 7 to 11.
28.	If requests under the Bill were not free, what limits or restrictions should be placed on charging fees? Do you have any comments on the costs and benefits of the various options?
	As a first mover in open banking, Worldline has made a significant investment in developing technology and APIs that comply with international best practice. Should the CDR regime enable less expensive access costs going forward, then those who have gone first should also be able to benefit from those access cost reductions without putting the rest of their existing access agreements at risk. The success of the CDR regime could be derailed if data holders are able to charge accredited requesters access fees that are too high. The options proposed require considered thought and more targeted industry engagement. The payments use case is different to the information use case and a 'one size fits both' approach may not be suitable. We suggest that more targeted consultation take place, specifically in respect of access pricing. For payments, the following items, at a minimum, need to be considered: • The access pricing must not be prohibitive; third parties need to be able to put together a sensible and achievable business case in respect of their products and services; • The access pricing cannot be so high as to make it difficult for third parties, or fourth parties, to compete with incumbent payment solutions (such as Visa & Mastercard); and • Assessing pricing on use case may sound like it's a good idea (price for risk, opportunity, etc) but it could result in subjective rather than objective assessments being undertaken by API providers and third parties would need to agree bilateral contracts with API providers (where the bargaining power is imbalanced).
The detailed rules for open banking	
29.	Do you agree with the proposals to ensure that consents given to accredited requestors are sufficiently informed? Are there any other obligations that should apply to ensure that consents are express and informed?
	The consent process for payments is quite different to non-payment services. Worldline is not able to comment on the process for non-payment services, but for payments the consent provisions set out in the API Centre standards should remain. The consent flows for join-accounts and for ongoing payments (subscription, recurring etc) have not been correctly described. We do not agree with the discussion document.
30.	Should customers be able to opt out of specific uses of their data that are not necessary to provide the service? Do you have any comments on the advantages and disadvantages of this?
	Yes. Consumers should be able to opt out – indeed only the data specifically required for the particular service should be collected in the first place.
31.	Should customers have the ability to set an expiry on ongoing consents? Do you have any comments on the advantages and disadvantages of this?

	Customers should be able to choose the duration and cancel when they wish. It's not a great customer experience to have to renew when you still want the service but on the other hand it might be challenging to keep track of all the consents you have given over time. If there is to be a maximum duration, it will depend on the risk and use cases in each sector. For Worldline an 18-month maximum could be acceptable. The API Centre standards on customer consent are a good start. For payments, consumers should be able to give a recurring consent, should they want to. In our experience, consumers want to be able to provide ongoing consent in relation to: i) recurring bill payments; ii) for those services currently paid via direct debits; and iii) for purchases made at preferred merchants and are frequented by the shopper.
32.	Do you agree with the proposals in this paper to help ensure that consents given to accredited requestors acting as intermediaries are sufficiently informed? Are there any other obligations that should apply to ensure that consents given to intermediaries are express and informed?
	We do not think the consumers will know whether and what intermediaries are involved, it will be very difficult to manage the intermediary consents independently. We think it must be linked to the end service for the consumer. For example, data aggregators – consent from user should cover the consent from underlying data sources and data aggregator consent cannot exist independently.
33.	Do you agree with the proposals to ensure that payment authorisations given to accredited requestors are sufficiently informed? Are there any other obligations that should apply to ensure that payment consents are express and informed? Should there be any other limitations on merchants or other unaccredited persons collecting authorisations, or instructing payments?
	By their nature they are informed. The payment cannot happen unless the consumer: 1) inputs their phone number; and 2) authorises the transaction via their banking app. The consent requirements in here are not based on what happens today and are incorrect. They must be consistent with the API Centre requirements for payments.
34.	Do you agree with the proposals in this paper for customer dashboards for viewing or withdrawing consent?
	No, for payments the consumer should be able to see this in their banking app not via a dashboard provided by Worldline. Consumers would not logically seek that information from us, they would first go to their bank.
Joint customers	
35.	Should there be any exceptions to joint customers being able to access account information, other than those provided by clause 16 of the Bill? What would the practical impact of additional exceptions be on the operation of open banking?
	No comment.
36.	Are regulations needed to deal with joint customers making payments, or are the default provisions of the Bill sufficient? What would the practical impact of the default provisions of the Bill on the operation of open banking?
	The consent requirements set out in the draft Bill that relate to joint account holders are not fit-for-purpose when it comes to payments. Ideally all those as named account holders should approve a payment prior to it being made, especially if it has a high value. There may however be some way of delegating consent (authority to act) but that would need incorporated into the bank terms and conditions so as to avoid a breach.

Secondary users	
37.	Are there any issues with designating authorised signatories on a customer's account as secondary users? What else should regulations provide for secondary users?
	This may breach bank terms and conditions. The bank terms and conditions may need to be updated to provide for this.
Payment limits	
38.	How should payment limits be set?
	Payment limits should be set similar to internet banking to prevent fraud and security threat. However, the payment limits should be set by banks in conjunction with the accredited requestors and depending on the threat to security risk. For example, there could be higher payment limit set to use cases linked to government agencies and partners who specialise in payments, than to impose a flat limit based on small use cases involving higher risk. Consumers should also be able to increase the limit at their own risk.
Remediation of unauthorised payment	
39.	Do you agree that accredited requestors should remediate banks for unauthorised payments that they request? Are there any other steps that should be required to be taken where unauthorised payments occur?
	Payment service providers cannot initiate a payment without there being a request from a consumer or a merchant. Worldline cannot make an unauthorised transaction itself as the consumer needs to authorise the transaction in the banking app. There should be clear guidelines for accredited requestors around maintaining audit history around payment initiation and the user session details.
Content of the register and on-boarding of accredited requestors	
40.	What functionality should the register have? Is certain functionality critical on commencement of the designation, or could functionality be added later?
	In the case of data holders, the data they hold. In the case of accredited requestors, the use-case for the data and related consent framework/scope. These items should be included: • Assurance of quality. • Risk management processes. • Security controls and potentially any standards they follow. • Certification that is issued to accredited requestors that people can verify and vice versa.
41.	What additional information needs to be held by the register to support this functionality? Should this information be publicly available, or only available to participants?
	There should be a register with public information on accredited parties with software applications that use the open banking services. The details on the services and detailed information on version and threshold etc can be held within the parties. However, the details should not be linked to any sort of revenue or market base and encourage competition. Worldline thinks that having this information available would help build trust.
42.	Is it necessary for regulations to include express obligations relating to on-boarding of accredited requestors? If so, what should these obligations be?

	Yes, or else it may never occur. Where a request adhering to the standards is made banks should enable it within "90" days. Open banking framework implies the parties able to use the services freely but in responsible manner.
Content of policies relating to customer data and action initiation	
43.	Do you agree with the proposed content of accredited requestor customer data policies? Is there anything else that should be required to be included?
	Yes – what has been proposed does not appear to be that much different to what we include in our privacy policy, and we agree that consumers should have access to that information. However, and in respect of the geographical location, we would only provide this at a country level. In accordance with security best practices, we would not disclose specifically where the data is stored. By revealing this information, we may inadvertently provide potential attackers with valuable intelligence that could be used to identify vulnerabilities or exploit our systems. We think that a level of ambiguity in this regard is essential for protecting any sensitive data and mitigating the risk of unauthorised access. Given the potential security implications, I would recommend opposing the proposal to disclose the data location.
Standards for open banking	
44.	Do you agree with the proposed standards? Should any additional standards be prescribed?
	We need the standards to embrace ISO20022 and for there to be standards for instore transactions. See paragraphs 22 to 31 for more information.
45.	When should version 3.0 of the API Centre standards become mandatory?
	We do not know what will be in version 3.0 so it's difficult to say when they should be mandatory.
46.	If product data were included in the designation, what standards should be adopted or developed for product data?
	No comment.
47.	Do you have any comments on performance standards that should apply?
	The expectations in the performance standards set out in the API Centre standards are too low to ensure consumer confidence. Please refer to paragraphs 27 and 28, and Appendix 2 for more information. API Providers need to make sure that the APIs are available and up at least 99.9% of the time and that fixes are completed in a timely manner.
48.	How can MBIE most effectively monitor performance?
	API Providers should provide an availability uptime and fix statistics to show that they are providing APIs that are robust enough to drive consumer trust and confidence in open banking payment services.
49.	Are existing institutional arrangements with the API Centre fit for purpose, to achieve desired outcomes? If not, what changes should be considered? How should the approach change over time as other sectors are designated?
	More generally, and for efficiency reasons, existing industry standards and certifications should be considered. To the extent possible, MBIE should look to re-use these rather than duplicate time, cost and effort in creating new standards and/or accreditation criteria.
General Comments:	
See our submission, paragraphs 1 to 43.	