

July 14, 2023



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

Dear Director

## **Government consultation on proposed reforms to the *Payment Systems (Regulation) Act 1998***

Apple Pty Limited (**Apple**) welcomes the opportunity to provide this submission on the matters raised in the consultation paper published by Treasury on June 7, 2023 (**Consultation Paper**) in relation to proposed reforms to the *Payment Systems (Regulation) Act 1998* (Cth) (**PSRA**).

### **A. Executive summary**

#### **Apple believes in a trustworthy, accessible, innovative and efficient payments system**

1. Apple introduced Apple Wallet with a bold but straightforward goal: to digitise consumers' wallets and allow them to seamlessly carry and use all of their cards (including payment cards, loyalty cards, tickets, boarding passes, health insurance cards, student ID, corporate badges and other physical plastic cards) and keys (including car and hotel keys) in a more secure and private way through iPhone and Apple Watch. To do this, Apple created a unique technical architecture: one that protects personal information, provides consumers with an easy way to select the card of their choice, provides banks with equal and non-discriminatory access, and most importantly, offers the highest level of security.
2. It is clear Apple's consumers enjoy the existing Apple Wallet and Apple Pay experience, with high customer satisfaction and usage in Australia. Attracted to an easy and seamless customer experience, near-zero fraud, industry leading security and consistent innovation, many Australians now leave their physical wallets at home and enjoy the efficiency, security and acceptance of Apple Wallet and Apple Pay across the country and online.
3. Apple agrees with the principles articulated by the Federal Government for the future direction of the payments system – namely that it be trustworthy, accessible, innovative and efficient. The innovation at the heart of Apple Wallet and Apple Pay, and its integration with Apple's devices, has provided, and continues to provide, a material benefit to consumers, financial institutions and other organisations who enjoy a digitisation of their cards, keys, tickets and passes. Apple Pay enables banks and fintechs to deepen their relationship with customers by providing their customers with a larger range of offerings, fast tracking the replacement of stolen or lost cards and most importantly, reducing fraud. Apple is proud that its partners and

their customers have enjoyed the benefits of Apple's innovation by simplifying their daily lives in a more secure and private way.

**Apple Pay is a payment presentment method, with only an indirect and limited role in the payments system**

4. Any assessment of Apple Pay's role in payments needs to be grounded in fact. Apple does not itself provide financial or payment services in Australia. Apple does not issue debit, credit or prepaid cards in Australia, nor does Apple acquire, process, authorise or execute transactions. Apple is neither an issuer nor an acquirer for existing regulated payments systems, and at no point does Apple handle a payer's money or have any control over any payments or transfer of value. Apple Pay does not store any details of a cardholder's existing debit, credit or prepaid card and does not have access to a user's account to determine whether funds are available or store any value or funds.
5. Apple Pay is ultimately a payment presentment method through which consumers can make payments from Apple devices with their existing debit, credit or prepaid cards issued by banks in an easy, secure and private way. Apple has invested significant resources to develop the technical architecture that can be used by banks to offer their customers a safer and more secure way to pay with their cards. Apple Pay can only operate with an existing debit, credit or prepaid card issued by a licensed financial institution. In its simplest form, Apple Wallet is a digital reproduction of a physical wallet – and no more a "payment system" or "participant" than an actual physical wallet would be – however made more efficient, seamless and secure.

**Any expansion of the definitions of "payment system" and "participant" should target actual risk and be assessed against a net public benefits test**

6. The Consultation Paper seeks to explicitly include providers of digital wallets as "participants" in Australia's payment systems. Apple submits that there has been no demonstrated case to date for the need to bring storage of cards (for example in a physical wallet) or their digital presentment (such as Apple Pay) within the scope of the PSRA.
7. Apple believes the proposed expansion of the definitions of "payment system" and "participant" to include entities that do not play any direct role in the payment process, including digital wallets, will increase regulatory burden without a net public benefit, give rise to over-inclusive (type 1) regulatory error and stifle the dynamic innovation that has characterised Australia's payment system over recent years.
8. The proposed power of the Minister to "designate" a payment system or participant (however defined) should be made by reference to a net public benefits test – and focussed on the effect of designation.
9. Any regulation designating Apple Pay as a participant in the payment system should target actual risks and be proportionate and tailored to the limited and indirect role played by Apple Pay. It should not come at the cost of innovation, competition, intellectual property rights or the seamless user experience – and it should certainly not weaken the current privacy and security offered by Apple Pay.

**Apple Wallet and Apple Pay are pro-competitive**

10. Apple is deeply committed to promoting competition. Traditionally, only large banks had the means to develop a digital payment option. As Apple Pay does not favour or provide preferential treatment to any card issuer, all cards and payment credentials receive access to the same interface on Apple devices and the same Apple Wallet technology to enable any bank to facilitate payments for its customers. This allows smaller banks and fintechs to compete on a level footing with larger incumbent banks.
11. When developing Apple Pay, Apple chose a unique architecture to enable consumers to easily switch between cards issued by different banks whilst still supporting contactless payments

initiated from third party apps and enabling non-payment uses of near field communication (NFC) technology such as car keys, loyalty, access to events, tickets and health insurance cards. Apple's pro-competitive technical architecture provides consumers, merchants and developers with greater choice, supporting cards and use cases from thousands of providers.

**Any mandate for common access requirements for payment systems should be premised on safeguarding privacy and security**

12. In designing Apple Pay, Apple opted for the most secure and user-friendly option available. Apple provides access to NFC payment functionality to all issuers on an equal, non-discriminatory basis. Any claim that Apple reserves or makes access to NFC unavailable is largely driven by companies seeking to mischaracterise Apple's technical architecture for their own commercial gain. Banks and others can access NFC functionality from their iOS apps today on non-discriminatory terms to offer their consumers a mobile payment experience directly within their own iOS apps, enabling banks to offer differentiated and innovative experiences whilst still providing consumers with superior security, privacy and the ability to easily switch between card providers and non-bank use cases.

**B. Apple Pay is a payment presentment method – and any reforms should be proportionate to the limited, indirect role such a service has in the payment system<sup>1</sup>**

13. The Consultation Paper proposes to broaden the definitions of "payment system" and "participant" under the PSRA, with the intention to increase the scope of entities caught by the regulatory regime.<sup>2</sup> In Apple's view, there is no demonstrated case to date to bring payment presentment services within the scope of the PSRA regime. As the Reserve Bank of Australia (RBA) noted as recently as March 2021, it did "*not see a case for regulatory action*" insofar as Apple is concerned, in relation to third-party access to NFC technology on Apple devices (by which digital presentments are made through Apple Pay).<sup>3</sup>
14. Defining a "payment system" by reference to an "*arrangement or series of arrangements*" (as opposed to a "*system*") would mean that:
- (a) the perimeter of any designated payment system that is subject to regulation is imprecise, with the consequence that there would be uncertainty as to who is and is not a "participant" in relation to the designated payment system; and
  - (b) one or more arrangements which together constitute only a component part of a system through which payments or transfers of value are effected could nevertheless be designated as a payment system, with the effect of imposing a disproportionate regulatory burden on participants in that payment system.
15. This uncertainty and potential for disproportionate application of regulation is extended by the proposed revised definition of "participant". In particular, the Consultation Paper notes that the proposed amendments to the definition of "participant" are intended to capture service providers and digital wallet services, including those "*without a direct relationship to a payment system*".<sup>4</sup> That is sought to be achieved by including any entity that "*operates, participates in or administers a payment system*" or "*provides services to a payment system, or provides services for the purposes of enabling or facilitating a transfer of value using a payment system*".
16. Such a "one size fits all" approach risks giving rise to unwarranted regulation or overregulation for those entities with only a limited role in the payments ecosystem – in particular, those whose limited participation in a payments chain does not give rise to any financial, payment or

<sup>1</sup> See generally Consultation Paper Q1-3.

<sup>2</sup> See generally Consultation Paper, 6-9.

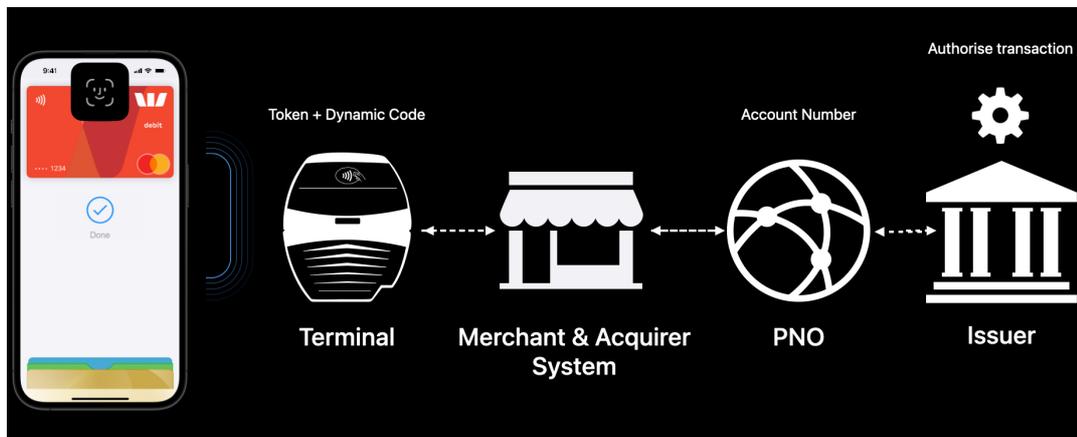
<sup>3</sup> RBA submission into Inquiry into Mobile Payment and Digital Wallet Financial Services, 21 May 2021, 6.

<sup>4</sup> Consultation Paper, 8.

settlement risks (e.g. solvency and liquidity) or misconduct risks to which the reforms are directed – which would undermine the innovation and efficiency objectives sought by the Government. These entities include not only digital wallets, but technology service providers which are only incidentally involved in a broader process (e.g. providers of fraud tools, physical card manufacturers, and payment terminal manufacturers etc) or merchants which accept payments through card-on-file or credential-on-file.

17. To reduce these risks, the definitions ought to include language to ensure that a “participant” in a “payment system” can only include an entity that may add *material* financial or misconduct risks that require regulatory intervention. Not all parties involved in the payments process, even those that might be perceived as being involved in a material way, contribute to such risks.
18. Apple does not itself provide financial or payment services in Australia. Importantly:
  - (a) Apple Pay can only operate with an existing debit, credit or prepaid card issued by a third party issuing financial institution that has agreed to participate on the Apple Pay platform (such as a licensed bank).
  - (b) Apple Pay does not store any details of a cardholder’s existing debit, credit or prepaid card, but rather enables a cardholder to create and store a virtual representation of their existing debit, credit or prepaid card and make use of Apple Pay security features when using that card to make a payment.
  - (c) Apple does not have access to a cardholder’s account to determine whether funds are available, or store any value or funds.
  - (d) Apple does not process or have any control over any payments. It is not a member of the relevant card schemes (e.g. Visa) relating to the cards. All transactions are processed using the existing payment infrastructure operated by issuers, acquirers and their payment network operators. As such, the merchant (as with any other card transaction) obtains comfort that it will be paid from its acquirer, who in turn relies on the authorisation from the issuer as confirmation that it will be reimbursed through the card scheme net settlement mechanism.
  - (e) Apple does not approve whether a card can be provisioned onto Apple Pay, as this responsibility sits with the issuer – Apple provides a presentment method for a cardholder to use that existing card within the existing payment system, subject to the existing regulatory rules which apply to the card issuer within that payment system.
19. Apple’s role with Apple Pay has been to invest significantly in the development of the technical architecture that licensed financial institutions can use to offer their customers a safer and more secure way to pay with the cards issued by their institutions. In providing a presentment method, Apple Pay offers consumers, merchants, and banks with unsurpassed security and privacy. Importantly:
  - (a) Every transaction requires the user’s authentication through Face ID, Touch ID or the user’s passcode.
  - (b) The consumer’s debit, credit or prepaid card is tokenised so that a unique proxy card number (i.e. Token) is then stored on the Secure Element embedded within the Apple device (rather than in the iOS system or on the cloud).
  - (c) Apple does not collect any transaction information that can be tied back to a user.
  - (d) At the time of transaction, the Apple device transmits both the Token and a single use “dynamic cryptogram” that is unique to each transaction and validated by the payment network.

20. The role of Apple Pay in a point-of-sale transaction is illustrated by the following figure:



21. Apple Pay cannot function without the underlying card issued by a regulated financial entity. It merely enables a consumer to request their bank to create a digital credential as a virtual representation of their card and use Apple technology to securely send the credential via NFC to a merchant terminal for onward transmission to their bank to authorise a payment using EMV standards. In particular, for the avoidance of doubt:

- (a) When a consumer enters information about their debit, credit or prepaid card (including store cards) to their Apple device, the card information is encrypted on the device and securely routed to the card issuer or card issuer’s authorised service provider. Using this information, the card issuer determines whether to approve adding the card to Apple Wallet.
- (b) Card numbers are not stored on the device or on Apple Pay servers. If the card is approved, the issuing financial institution or the card company on the issuing financial institution’s behalf (e.g. Visa) creates a device specific credential (Device Primary Account Number or **DPAN**) which is encrypted in such a way that Apple cannot access it. The DPAN is stored in software applications (applets) from the card scheme (e.g. Visa) which reside in the Secure Element and cannot be accessed by Apple. The DPAN is, in effect, the debit, credit or prepaid card in a different form. The DPAN is unique and different from debit, credit or prepaid card numbers; the card issuer or payment network can prevent its use on a magnetic stripe card, over the phone, or on websites. The DPAN in the Secure Element is never stored on Apple Pay servers or backed up to iCloud, and it is isolated from iOS, iPadOS, and watchOS devices and from Mac computers with Touch ID.
- (c) The bank authenticates its customer and (by itself or using a third-party token service provider (**TSP**)) creates the DPAN that is stored on its cardholder’s device. This DPAN (also referred to as a token) is a proxy for and is mapped to the cardholder’s card details. When the cardholder attempts to make a payment, the token and a transaction specific dynamic security code are used when processing the payment. Neither Apple nor the cardholder’s device sends the full debit, credit or prepaid card numbers to merchants. The token and code are released by the applets which reside in the Secure Element and sent to the bank to authorise the payment. The bank/TSP decrypts the token and maps the token back to the actual card details before the bank authorises the payment (using the card number).
- (d) As the cryptogram is generated by the card scheme software application (i.e. the applet) after the transaction is authorised by the cardholder on the device, it facilitates secure mobile payment, by adding an extra layer of security to the payment information sent to the merchant.

22. Insofar as financial or misconduct risks are concerned, as Apple Pay is a mechanism that is simple to understand and use, no detriment is caused to any consumers or any third party as a result of payments that occur through the virtual representation of the debit, credit or prepaid card stored on Apple Pay. As Apple Pay does not store any funds, there is also no potential for loss. In particular, where a debit card causes the payments, there is always a licensed issuing financial institution (i.e. such as ANZ, Macquarie or ING) to which the customer has recourse, including to that entity's external dispute resolution scheme.
23. The high level of security associated with the Apple Pay platform has been recognised by the Australian payments sector. The Parliamentary Joint Committee on Corporations and Financial Services (**Joint Committee**) recognised in its report on *Mobile Payment and Digital Wallet Financial Services* that:
- “developments in mobile payments and digital wallets have enhanced security and reduced risks faced by both consumers and industry, such as fraud mitigation measures and biometric security”.*<sup>5</sup>
24. Apple's differentiated and limited role in payments systems is further illustrated by the fact that:
- (a) In offering Apple Pay, Apple does not collect any transaction information (including sensitive financial data such as the account or card number of provisioned cards) that can be used to identify Apple Pay consumers. No cards or payment details are visible to or retained by Apple. No actual card details are provided to the merchant. The payment data is submitted to the card issuer (or its TSP) to verify the transaction specific code and match the DPAN to the true card number. From that point, the transaction proceeds in the same way as a normal card transaction and the card issuer can authorise or decline the transaction. Payment transactions are made entirely between the user, merchant and card issuer.
  - (b) Apple does not itself provide financial services or payment services in Australia. The debit, credit or prepaid cards used with Apple Pay are issued and operated entirely by licensed financial institutions (i.e. banks, payment services providers and e-money institutions) that choose to use Apple APIs and technical architecture. As such, Apple does not issue cards nor does Apple hold, manage or access customer accounts. All transactions are processed using the existing payment infrastructure operated by banks, acquirers and their payment network operators.
  - (c) Apple does not have access to a user's account to determine whether funds are available. Apple does not store any value or funds. Apple does not enter into receipt of funds at any point and has no role in the processing or execution of the payment transaction. Apple does not provide comfort that a payment has been authorised by the bank. The merchant (as with any other card transaction) obtains comfort that it will be paid from its acquirer, who in turn relies on the authorisation from the issuer as confirmation that it will be reimbursed through the card scheme net settlement mechanism. Apple Pay does not therefore impact in any way on the existing authorisation and settlement arrangements for card transactions.
25. Apple's only role has been to develop the technical architecture that can be used by licensed financial institutions to offer their consumers a safer, more secure and private way to pay with their cards. Apple is not in the category of entities which are currently unregulated by the PSRA but which *“perform roles such as transferring, processing, and storing value”*.<sup>6</sup>

---

<sup>5</sup> Parliamentary Joint Committee on Corporations and Financial Services, *Mobile Payment and Digital Wallet Financial Services*, October 2021, [6.109].

<sup>6</sup> Consultation Paper, 8.

**C. Any powers to designate a system or participant should be by reference to a well-established net public benefits test<sup>7</sup>**

**Proposed “national interest” test for designation**

26. The RBA is the primary body responsible for regulating payment systems in Australia and the PSRA allows the RBA to regulate payment systems where it considers it to be in the public interest to do so, having regard to whether those systems are financially safe for participants, efficient, competitive and not materially causing or contributing to increased risk in the financial system.<sup>8</sup> By contrast, the Consultation Paper recommends providing the Treasurer with the power to designate payment systems and participants “*where it is in the national interest to do so*”.<sup>9</sup>
27. The Consultation Paper appears to distinguish between the concepts of “public interest” and “national interest”, following a recommendation that a power to act in the “national interest” be vested in the Executive Government (through the Treasurer), on the basis that the s/he can “*engage more openly with industry due to not playing a regulatory enforcement role*” and “*engage other agencies where issues beyond the remit of a particular regulator*”.
28. Curiously, the Consultation Paper states that “the national interest is a higher threshold than the public interest”. It also foreshadows the risk of overlap - or conflict - between the “public interest” considerations applied by the RBA, and that of the “national interest” proposed to be applied by the Treasurer in decisions to designate payments systems, by proposing that “decisions taken in the national interest would take priority over decisions based on the public interest”.<sup>10</sup>
29. Apple does not consider that the proposed “national interest” test is appropriate for achieving the policy intentions articulated in the Consultation Paper. Specifically, Apple does not consider that the proposed approach to delineating the Treasurer's national interest powers (as opposed to the RBA's public interest powers) is either clear or effective. Rather, Apple proposes that the existing “public interest” criteria in the PSRA, and those proposed to apply to designation decisions of the Treasurer, be harmonised under a net public benefits test, following the well-established provisions of the *Competition and Consumer Act 2010* (Cth) (**CCA**) which has developed jurisprudence on the meaning of that term.
30. Although the PSRA currently defines the mandate of the RBA by reference to a narrow concept of “public interest” limited to the enumerated factors of financial safety, efficiency, competition and controlling risk in the financial system, this is not consistent with the ordinary concept of public interest or public benefits known to law. Relevantly, in the context of applications for statutory immunity (known as “authorisation”) from various provisions of the CCA, the ACCC is required to apply a net public benefit test which has been the subject of significant judicial consideration over many years. It is well-established by the relevant jurisprudence that, under the net public benefits test in Part VII of the CCA:
- (a) A benefit to the public includes “*anything of value to the community generally, any contribution to the aims pursued by society including as one of its principal elements (in the context of trade practices legislation) the achievement of the economic goals of efficiency and progress*”.<sup>11</sup>
  - (b) The relevant “public” is the Australian public.<sup>12</sup>

<sup>7</sup> See generally Consultation Paper Q4-5, Q8.

<sup>8</sup> <https://www.rba.gov.au/payments-and-infrastructure/payments-system-regulation/approach-to-regulation.html>

<sup>9</sup> Consultation Paper, Annexure 1 (Recommendation 7).

<sup>10</sup> Consultation Paper, 13

<sup>11</sup> *Re Queensland Co-operative Milling Association Ltd* (1976) 8 ALR 481 at 507-8; *Application by Medicines Australia Inc* [2007] ACompT 4; ATPR 42-164 at [107].

<sup>12</sup> *Re Qantas Airways Ltd* [2004] ACompT 9; (2005) ATPR 42-065 at [196] citing *Re Howard Smith Industries Pty Ltd* (1977) 28 FLR 385 at 392.

- (c) Similarly, a detriment to the public includes “*any impairment to the community generally, any harm or damage to the aims pursued by the society including as one of its principal elements the achievement of the goal of economic efficiency*”.<sup>13</sup>

31. Apple submits that a harmonised net public benefits test will resolve the potential for conflict between the powers of the RBA under the PSRA, and the proposed designation criteria to be applied by the Treasurer when making designation decisions. The test is of sufficiently wide import to include concepts of the “national interest”, including the non-exhaustive list of matters at page 12 of the Consultation Paper, without artificially delineating between concepts of “public” and “national” interest.

### **Designating payment systems**

32. The decision to “designate” a payment system or participant would potentially enliven substantial regulatory obligations on “participants” and would have a significant effect on the proprietary (including intellectual property) and commercial rights obligations for entities involved in the payments system.
33. As noted in section B above, the scope of entities proposed to be subject to the PSRA (including designation) vary substantially in terms of their role in the payments process and, consequently, the risks (financial, operation or misconduct) to which their services or conduct may give rise. The assessment of whether a payment system or participant should be subject to “designation” must therefore be undertaken on a case-by-case basis having regard to the facts and market dynamics in issue. An indiscriminate approach which punishes successful through to recently established payment systems or participants risks chilling the efficient use of, and investment in, the digital economy.<sup>14</sup>
34. In this regard, Apple submits that the criteria for designation should be carefully framed to focus the test on *the effect of designation* in promoting public benefits in the payments landscape. That is, the test for designation should require that the regulatory obligations to which a designated entity would be subject (for example, the provision of access, or increased access, to payments architecture) as a result of designation would promote a net public benefit (rather than merely assessing whether increased regulation would promote a public benefit). This approach is consistent with that applied under the National Access Regime (**NAR**),<sup>15</sup> where the substantive test for “declaration” under the NAR is focussed on the effect of declaration, rather than merely assessing whether access (or increased access) would promote competition.
35. A designation criterion framed in this way would require a comparison of the future under the status quo against the future state where increased regulatory obligations (such as in relation to mandated access to payment infrastructure) is granted through designation.
36. As the Productivity Commission observed in relation to the equivalent criterion under the NAR, a designation-focused test is the most effective way to target the economic problems that access regimes are designed to address.<sup>16</sup>

### **D. No basis for “increased access” to hardware components used by Apple Pay<sup>17</sup>**

37. The Consultation Paper recommends that common access requirements for payment systems be developed, in consultation with operators of payment systems, to facilitate access to those systems.<sup>18</sup> Apple provides all third parties that can meet the technical and commercial requirements for Apple Pay with access to the NFC functionality on Apple devices using Apple

<sup>13</sup> *Re 7-Eleven Stores Pty Ltd* [1994] ATPR 41-357 at 42,683.

<sup>14</sup> DPSI Treasury 16 February 2023 submission, [78].

<sup>15</sup> *Competition and Consumer Act 2010* (Cth) pt IIIA.

<sup>16</sup> Productivity Commission, Inquiry Report No 66, “National Access Regime” (25 October 2013) p 249.

<sup>17</sup> See generally Consultation Paper Q8.

<sup>18</sup> Consultation Paper, Annexure 1 (Recommendation 11).

Pay. Apple submits that any proposal to mandate third-party access to payments infrastructure distinguish between technical interoperability and broader concepts of economic access, having regard to intellectual property considerations as well as the privacy and security of end-consumers.

**Apple Pay is already accessible to all card issuers on a non-discriminatory basis**

38. Apple Pay is available to any card issuer on equal, non-discriminatory terms. Issuers all pay the same fees to Apple, regardless of their size, and are presented equally in the user experience on Apple Pay. Consumers can easily switch between cards issued by different banks and benefit from having full transparency over what card they are paying with at any time. The user (and not any one particular bank e.g. an incumbent bank with dominant market power) is always in control of the default settings and which cards are enabled on their devices.
39. Traditionally, only large financial institutions had the means to create a digital payment option. Apple Pay is offered to all banks on a level playing field, such that Apple Pay has significantly reduced the barriers to entry and expansion for banks to create mobile payment propositions downstream. The smallest banks in Australia (including those without a banking app) can enjoy equal exposure in Apple's user experience to the largest incumbent banks, making it easy for customers to choose among them. In recognition of these benefits, over 120 financial institutions in Australia have decided to bring their cards and competitive offerings to customers via Apple Pay.
40. Apple has also committed to providing participating banks with access to alternative payment networks to the major international schemes. Apple has invested significant resources to enable the eftpos network on the Apple Pay platform from 2016, which has allowed consumers to easily choose between different payment networks, reduce costs for merchants, and support domestic competition among payment networks.
41. To the extent that there is any proposal to require access to the technical architecture that underpins Apple Pay (e.g. providing access by third parties to the NFC controller or Secure Element), such a requirement would be inappropriate and give rise to significant user harms and stifling of competition as between providers of different virtual presentment methods.
42. Specifically, Apple Pay's contactless payments are built around the following elements which benefit consumers and act as a competitive point of difference for Apple as against alternative competing virtual presentment models: a Secure Element, an NFC controller, Secure Enclave, and Apple Pay Servers. In particular, the Secure Element is a tamper-resistant physical chip, incorporated in the device itself, which stores all relevant payment credentials and the encryption keys to protect the transaction data, while the NFC controller routes payment communications from the NFC reader directly to the Secure Element. The Apple solution only allows for payments to be made through the use of the Secure Element.
43. When designing the Apple Pay solution, Apple has focused on three process flows to secure the payment credentials and the integrity of the Secure Element.
  - (a) *First*, the delivery of payment credentials comes directly from the payment provider and is loaded securely into the Secure Element. Apple servers act as the orchestrator of this operation and has built a solution so that no parties between the payment provider and the Secure Element can read the credentials.
  - (b) *Secondly*, Apple has designed a tightly integrated link between the Secure Enclave and the Secure Element to manage the release of these credentials subject to the approval of the biometrics controls (Touch ID, Face ID) or a passcode.
  - (c) *Thirdly*, Apple protects the delivery of the payment credentials from the Secure Element to the payment terminal.

44. The NFC controller is critical to security as it effectively acts as the gateway to the Secure Element from the point-of-sale terminal. Providing access to the NFC controller to third-party applications inevitably raises security concerns. These third parties would effectively have access to the one element that has a direct access to the Secure Element, which would provide potential hackers with increased opportunities to launch attacks that they otherwise would have difficulty with, or be precluded from, launching. Whilst attacks can never be entirely excluded, providing access to the NFC controller automatically increases the security risks and would call into question the system that Apple has built around its Secure Element.
45. More broadly, providing access to the NFC controller to third parties would increase the security risks for the rest of the operating system. It would necessitate the creation of a channel between the NFC controller and these third-party apps to route messages from the radio interface to these apps. This channel, which would run through the iOS system, would increase the attack surface within the iOS system and increase the risk of attacks which could compromise the security of the overall device.
46. When the user authorises a transaction, which includes a physical gesture (e.g. a double click on an iPhone) as well as an authentication (e.g. Face ID) communicated directly to the Secure Enclave, the Secure Enclave then sends signed data about the type of authentication and details about the type of transaction (contactless or within apps) to the Secure Element, tied to an Authorization Random (**AR**) value. The AR is generated in the Secure Enclave when a user first provisions a credit card and persists while Apple Pay is enabled, protected by the Secure Enclave's encryption and anti-rollback mechanism. It is securely delivered to the Secure Element through the pairing key. On receipt of a new AR value, the Secure Element marks any previously added cards as deleted.
47. Apple's iOS incorporates a multi-layered approach in terms of securing the individual components and overall system including the NFC. Specifically with respect to the NFC, there are both hardware-based and software-based protections in place. With each additional potential access point to NFC, the potential for there to be a weakness in the system increases and the security is reduced.

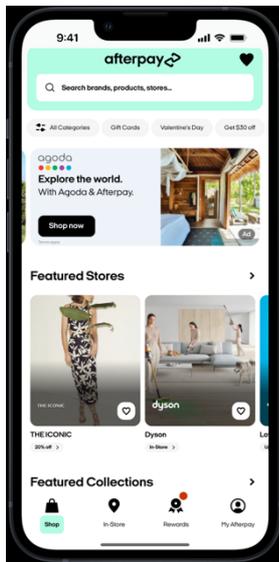
**Apple Pay provides all iOS apps a convenient, non-discriminatory ability to access NFC directly from their iOS apps**

48. Apple Wallet is designed so that all banks can access the hardware security and NFC infrastructure of Apple Pay to offer their consumers the ability to initiate a payment directly from their own iOS apps. For banks that elect to enable this feature, the user can open the mobile app, access any other features the bank chooses to offer within the app, and select the payment card of their choice to make an in-store payment. When the payment is concluded, the user is returned to the iOS app. In other words, banks can ensure their consumers can go through the entire mobile payment experience without ever having to leave the bank's app.
49. Afterpay is just one example of a payment innovator using Apple's open NFC access to offer its consumers an instalment plan for in-store purchases using Afterpay's iOS app. The following demonstrates how an Afterpay user is able to use the Afterpay iOS app to make a payment using Apple's NFC technology while interacting directly with Afterpay (without any Apple branding).

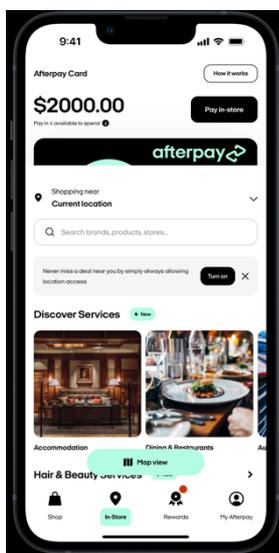
July 14, 2023



Step 1: a user selects the Afterpay app on their iPhone

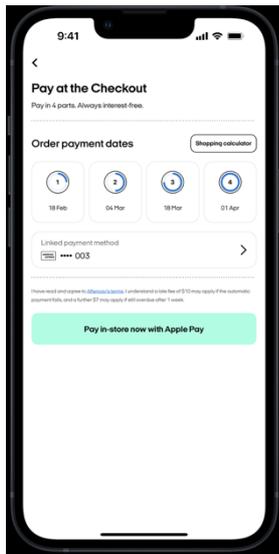


Step 2: once the user is inside the app, they can then navigate to the "In-Store" tab at the bottom of the screen



Step 3: once the user is in the "In-Store" tab, they can then navigate to the black "Pay in-store" button in the top right-hand corner of the screen

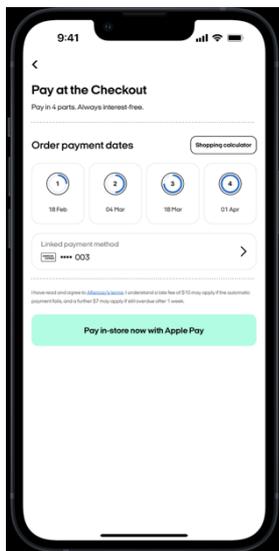
July 14, 2023



*Step 4: once the user is in the “Pay in-store” screen, they can then navigate to the aqua “Pay in-store now with Apple Pay” button*



*Step 5: the user is then able to initiate the payment from within the app using Apple’s NFC technology. Note there is no Apple branding – the user only interacts with Afterpay*



*Step 6: once payment is made, the user is returned to the Afterpay app*

50. Banks who advocate for access to pair the NFC functionality of Apple's devices with any app are motivated to make their own payment cards available exclusively within their own digital wallet or general banking apps. This would allow these banks to bypass the current architecture, which allows consumers to seamlessly select between competing payment cards at the point of transaction (which is the user experience available in a physical wallet).
51. Because Apple Wallet enables multiple payment (and other) cards to be stored, this benefits consumers who can easily choose between any of the cards at the point of sale without unnecessary friction – which would be imposed by banks self-interested in exclusively preferencing their own payment cards at the expense of competition, device security, user experience and consumer benefit.
52. This risk is particularly amplified in Australia, where the former chair of the ACCC has noted that “a cosy banking oligopoly is surely at the heart of recent problems, so we must and will find ways to get more effective competition in banking”. The architecture of Apple Wallet directly addresses this market concentration, as placing issuers on an equal playing field stimulates downstream competition from more than 100 banks and fintechs, who if acting independently would never have been in a position to offer their consumers the enjoyment of a secure and effective technical architecture for digital contactless credential presentment.

#### **E. Engagement with regulators should be limited to consultation only<sup>19</sup>**

53. The Consultation Paper proposes to provide the Treasurer with the power to “allocate responsibilities under the PSRA to the RBA or another Treasury portfolio regulator” (for example, the ACCC).<sup>20</sup>
54. Apple submits that any responsibilities of other portfolio regulators for matters relating to payment systems should be in accordance with current legislation. The responsible agency for the purposes of the PSRA should be, as is currently the case, the RBA as the principal subject matter expert. It is appropriate for other agencies that have specialist expertise to be consulted in respect of relevant issues, but that engagement should be limited to consultation only and should not be “allocated” in the way contemplated by the Consultation Paper. Effective regulation of this critical sector should unambiguously be conferred on a single accountable agency with subject matter expertise (i.e. the RBA) and not spread among several agencies whose roles may overlap or may have principal functions outside the payments sector competing for their attention.

#### **F. Conclusion**

55. In conclusion, Apple submits that:
  - (a) **Any increased regulatory burden caused by expanding the definitions of “payment system” and “participant” should be proportionate to the particular and different roles that entities that may be brought into the payment regulatory regime play in the payment process.** The payments sector in Australia is comprised of varied and dynamic participants, some of which do not play *any* direct role in the payment process (as the Consultation Paper acknowledges). The proposed expansion of the definitions of “payment systems” and “participants” would result in a significantly larger proportion of those entities being caught by the PSRA and subject to increased regulatory burden. Such a “one size fits all” approach is likely to give rise to overinclusive (type I) regulatory error, and to stifle the dynamic innovation that has characterised Australia’s leading payments system over recent years.

Apple does not issue debit, credit or prepaid cards in Australia. Apple also does not acquire, process, authorise or execute transactions. Apple is neither an issuer nor

---

<sup>19</sup> See generally Consultation Paper Q9-11.

<sup>20</sup> Consultation Paper, 14-15.

an acquirer for existing regulated payments systems. Rather, Apple Pay is a method through which consumers can use their existing debit, credit or prepaid cards to make payments from Apple devices in an easy, safe, secure and private way.

Any regulations that are proposed to apply to “*all entities involved in the payments value chain*” should therefore be tailored to reflect Apple’s (and other digital wallet providers’) limited and indirect role in the payment process, and the absence of any financial or misconduct risks to which Apple services can conceivably give rise.

- (b) **The proposed power of the Minister to “designate” a payment system or participant (however defined) should be made by reference to a net public benefits test – and focussed on the effect of designation.** The Consultation Paper proposes that the Treasurer be empowered to “designate” a payment system or participant where it is in the “national interest” to do so, where designation would result in regulators developing regulatory rules for designated entities, and the power for the Treasurer to give binding directions to operators of, or participants in, payment systems.

The Consultation Paper foreshadows overlap - and in some cases, potential conflict – between the public interest factors currently applied by the RBA under the PSRA, and the proposed national interest criteria for designation decisions of the Treasurer. It is undesirable to design an ex ante regulatory system which may result in such conflict. Apple submits that the existing “public interest” criteria in the PSRA, and those proposed to apply to designation decisions of the Treasurer, be harmonised under a net public benefits test, following the well-established provisions in Part VII of the CCA (for applications for statutory immunity from relevant provisions of the competition law) which has been reformed and judicially considered over many years to reach its currently applicable well understood form. A net public benefits test would align the concept of “public interest” with that recognised at law and avoid the perceived conflict with separate “national interest” considerations.

In addition, the designation criteria should be carefully framed to focus the test on the effect of designation in promoting public benefits in the payments landscape. Designation criteria framed in this way would require a comparison of the future under the status quo against the future state where increased regulatory obligations (such as in relation to mandated access to payment infrastructure) is granted through designation.

- (c) **Insofar as Apple is concerned, proposals to mandate third-party access to digital wallet architecture ignore the fact that Apple already provides access to NFC payment functionality to all issuers on non-discriminatory terms.** Apple submits that any proposal to mandate a different third-party access to payments infrastructure distinguish between technical interoperability and broader concepts of economic access, having regard to intellectual property considerations as well as the privacy and security of end-consumers.

In particular, any proposal to mandate access to the Apple Pay technical architecture (including NFC technology on Apple devices) risks exposing consumers to significant security and privacy harms, and risks increasing financial and misconduct risks. Apple Pay is specifically designed to protect consumers from the detrimental effects of malicious code. With each additional potential access point to NFC, the potential for there to be a weakness in the system increases and the security is reduced.

- (d) Responsibility for enforcing the PSRA should be with the RBA only as the single responsible subject matter expert and any engagement with other regulators within

July 14, 2023

the Minister's portfolio should be limited to consultation on topics within their field of expertise.

56. Apple does not propose to provide feedback in response to all of the questions raised in the Consultation Paper. For the avoidance of doubt, where Apple has not addressed a specific question or topic in the Consultation Paper, Apple should not be taken to agree with or acquiesce to the proposals canvassed or views expressed in the Consultation Paper. However, if Treasury has any specific questions to ask Apple in relation to any topics it has not addressed in this submission, Apple would be happy to assist.