Bendigo and Adelaide Bank and others applications for authorisation (A91546 & A91547) – Response to issues raised in relation to access to the iPhone's NFC function

1 Introduction

In response to questions raised by the ACCC, the applicants set out below further information on the public benefits of access to the iPhone's NFC functionality.

Specifically, the applicants submit and provide further information in relation to the following:

- there are net public benefits to allowing a collective negotiation about access to the iPhone's NFC functionality, and these benefits cannot be achieved without the collective negotiation;

- access to the NFC functionality on the Android platform alone cannot generate the same choice, competition, efficiencies and innovation in integrated mobile wallets in Australia;

- non-integrated solutions (eg NFC stickers) cannot substitute for integrated NFC access or provide the same public benefits;

- the linking of a banking app with the Apple Pay payment mechanism cannot substitute for integrated NFC access or provide the same public benefits; and

- recent submissions do not alter the view that NFC function access will not compromise security or user experience.

2 Access to the NFC functionality provides public benefits

With access to the iPhone's NFC functionality, there will be:

- *greater choice in integrated mobile wallet options;*

- *increased and more effective competition to Apple Pay;*

- *stronger incentives for investment and innovation;*

- *enhanced pressure on Apple to price competitively and innovate for Australian consumer preferences or Australian specific uses; and*

- *better price-quality outcomes.*

Without access, there will be no choice and no competition in iPhone mobile wallets, and Apple Pay will be the only integrated mobile wallet available to iPhone customers.

Without access, there will be no meaningful competition from other contactless payment options such as NFC stickers (which in any case provide little additional consumer value as compared to "tap and go" cards). Further, competition between handsets cannot be relied on to provide:

- sufficient competitive constraint (see section 4 and the Expert Report of Dr Susan Athey[1]); and
- incentives to push development and provide Australian consumers with the best outcomes in relation to mobile wallet technology.

A continued withholding of access to the iPhone's NFC functionality will also result in lost opportunities for investment and innovation. Without access, mobile wallet developers will not have the same addressable market, reducing incentives for investment and innovation, and there will not be the same pressure on Apple to innovate and respond quickly to Australian consumer preferences. This will further result in inefficiency and underutilisation of Australia's NFC infrastructure.

Mobile wallets without access to the iPhone's NFC functionality are not viable competitive substitutes to Apple Pay and have tended to fail (see section 8). Competition for mobile wallets relies on providing consumers a convenient, value-added merchant-user experience they can trust, particularly at this point in the technology's lifecycle and adoption where point of sale mobile payments are yet to really take off. A lack of access to the NFC functionality across both iPhone and Android platforms restricts this competition. The addressable market is reduced and the inability to provide consumers with a cohesive and convenient customer experience across platforms sends mixed messages to consumers, hindering adoption and innovation. A fragmented customer experience across platforms confuses the customer offering (which relies on simplicity for adoption). It also adds to the costs of investing to develop mobile payment technology for consumers and the consumer engagement required to explain the product and its additional value beyond a "tap and go" payment, and provide confidence that consumers can trust the product with their money.

3 Access to the NFC functionality on the Android platform alone does not generate the same level of public benefits

There is no evidence to support claims that access to the NFC functionality on the Android platform alone can generate the same choice, competition, efficiencies and innovation in integrated mobile wallets as access to both Android and iPhones.

It is also a mistake to consider that the relevant factual is represented by what is now available on Android. What has been achieved on the Android platform to date (where access to the NFC function is allowed) is not indicative of the extent of benefits that could be achieved with access to the iPhone's NFC. Mobile wallet technology and uptake is in its early days and the potential for innovation would be greater with access to a broader customer base including the lucrative, and quicker to adopt, iPhone customer segment.

Without the authorisation:

- Apple alone has access to the iPhone's NFC functionality. iPhone NFC capable payments at the point of sale can ***only*** be made via the Apple Pay payment mechanism;
- Apple in its sole discretion determines when or if additional features or services utilising NFC functionality are to be added to Apple Pay, or may prioritise features of interest to overseas markets (e.g. Japanese transit) and not features of significance to Australia; and
- mobile wallet developers have limited options for reaching customers across platforms and all those options result in significant public detriments to competition (see Table 1 below).

Table 1: Detriments of mobile wallet development options without integrated access to iPhone NFC

[1] As noted by Dr Susan Athey: *Even though Apple competes for users of smartphones, it has market power in respect of applications and services for iPhone users. The "competitive bottleneck" occurs because the only way for service providers to access iPhone users is through Apple's platform. The market power held by Apple translates into highly asymmetric bargaining power for Apple when negotiating individually with card providers.*

Option	Public detriment
Provide an NFC-capable integrated solution to Android users but not to iPhone users	Lack of access to iPhone users reduces the addressable market, limiting the commercial viability and incentives to innovate and invest. Incentives are further reduced by the impact and cost of having inconsistent service offerings to customers depending on their choice of smartphone device. Without access to the iPhone's NFC functionality, the applicants are left to explain why an iPhone customer with exactly the same accounts or transaction volumes as the Android customer cannot be given the choice of another wallet alongside Apple Pay, adding to costs and discouraging investment in the Android platform. Therefore, not only do iPhone users miss out, Android users are also denied the potential for greater, safer and more convenient mobile wallet technology. Further information on the importance of reaching the iPhone customer segment in achieving greater choice, competition, investment and innovation is provided in section 4 below
Provide an NFC-capable fully integrated solution to Android users and offer iPhone users a mobile banking app which can interact with and use Apple Pay as the payment mechanism – the Capital One scenario	This option creates the problem of inconsistency and fragmentation in the customer experience across customers with different devices (as described above). Additionally, there is still no choice or competition in the payment mechanism available to iPhone users or competitive pricing pressure on the use of Apple Pay. Payments must still go through Apple Pay. Opportunities for integration and efficiencies are also limited or restricted – the wallet provider can only innovate to the extent and speed allowed by Apple Pay – stifling outcomes and incentives. As an example, the Android version of Capital One with similar functionality and its own payment mechanism was available a year ago. The iPhone Capital One product connected with Apple Pay has only been available since Apple decided to release iOS 10 in September 2016 (prior to that, the only products available to iPhone users were a Capital One card in the Apple Pay wallet and a separate banking app). Further, integration of a banking app with the Apple Pay payment mechanism limits the ability to innovate around the payment mechanism itself - eg, with better security features than those offered by Apple. Further information on the Capital One scenario is provided in section 6 below.
Provide non-integrated NFC solutions to iPhone users or non-NFC solutions	Workarounds such as NFC stickers or wristbands, QR codes or Bluetooth beacons are not close substitutes for integrated NFC mobile wallets. NFC workarounds provide no real benefit over plastic cards and are subject to "card clash" with integrated mobile wallets. They do not deliver a long term viable offering to provide consumers with seamless, convenient merchant-consumer experiences. They are also limited in the extent of innovation and functionality that can be provided compared to in-device NFC functionality. Australian banks and merchants have invested in building an NFC-enabled payments infrastructure that can support mobile payments across Australia and there is world-leading widespread consumer acceptance and use of contactless payments. Other technologies present customers with unfamiliar processes and require merchants to install new infrastructure. Further information on non-integrated NFC solutions and non-NFC solutions is provided in section 7 below.

Option	Public detriment
	None of these options allows the ability to achieve the same public benefits, efficiencies and price-quality outcomes as having access to the iPhone's NFC functionality. Nor do they remove the detriments of not having that access. Mobile wallets without access to the iPhone's NFC functionality are not viable competitive substitutes to Apple Pay and do not provide the same choice, competitive constraint or incentives for investment or innovation. Further, what has been achieved on the Android platform to date (where access to the NFC function is allowed) is not indicative of the extent of benefits could be achieved with access to the iPhone's NFC – ie, it is a mistake to consider that the relevant factual is represented by what is now available on Android. Mobile wallet technology and uptake are in their early days and the potential for innovation would be far greater with access a broader customer base including the lucrative iPhone customer segment.

4 Importance of access to the iPhone customer segment in achieving public benefits

The economics of app development is characterised by two-sided markets in which most customers choose a single platform and most app developers must address both major platforms to succeed.

Australian download revenues are more skewed towards the iPhone than the worldwide average, with 70% of combined Apple App Store and Google Play Store revenues attributable to the Apple App Store.[2] *If these revenues are reflected in customers' tendency to make mobile payments, or use other NFC enabled commercial services, then the importance of iPhone customers to the success of mobile wallets is clear.*

Dr Susan Athey's report notes, at paragraph 62:

> *In Australia, of the 100 most downloaded applications from the Apple App Store on September 19, 2016, 86 were also available in the Google Play store. On the same date, out of the 100 most downloaded from Google Play in Australia, 90 were also available on the Apple App Store. CommBank, Westpac and NAB, the banking applications developed so far by the applicant banks, are also multi-homed across the Apple and Android platforms.*

In Australia, approximately 40% of smartphone sales are iPhones. However, the value and importance of the iPhone customer segment for app uptake, use and expenditure far outweigh this share. For example, iPhone users account for 60% of mobile banking transactions and 70% of mobile application revenues in Australia. The tendency of iPhone users to embrace mobile payments, engage in mobile applications and adopt new technologies is particularly important in relation to technology such as mobile wallets, which involves a behavioural change in the way we pay and interact with our phones for greater convenience and efficiency and is still yet to completely take off or become mainstream.

The average iPhone user is more likely to adopt and value the ability to make integrated mobile payments as well as influence a more widespread adoption of this technology. iPhone users tend to be wealthier and likely to conduct more and undertake larger transactions. They are also more engaged and attached to their mobile devices than Android users. According to Apple CEO Tim

[2] App Annie Index: Market Q2 2016, p 15.

Cook, iPhone loyalty rates are almost twice as strong as the next-highest brand.[3] Australians also exhibit this brand loyalty in their smartphone consumption patterns.

Smartphones are used for a multitude of functions and the choice of handset is not determined by an individual app. Once a customer becomes part of the Apple ecosystem, switching becomes difficult, inconvenient and expensive (eg, the costs associated with a new handset, data transfer, lost in-app purchases and unfamiliarity with a different operating system). As a result, competition between handsets cannot be relied on to provide competitive constraint and better price-quality outcomes in mobile wallets.

The importance of access to the iPhone customers in achieving better mobile wallet outcomes is consistent with the views put forward by Dr Susan Athey and Dr Geoff Edwards in their expert reports, the behaviour of issuers offering both Apple and Android payment mechanisms, and recent case study evidence of the difficulty of sustaining a viable mobile wallet without access to the iPhone's NFC functionality – either by focusing on Android, or by using less widespread or more cumbersome technologies such as QR codes or Bluetooth. Further information on these case studies is provided in section 8.

Around the world, access to iPhone customers is critical to successful app development (that is for any app, not just payment apps). This is because of the high fixed costs of app development and the attractiveness of the iPhone-user demographic in terms of its tendency to early adoption and high spending.

As Dr Susan Athey notes in her report:

> *Restricting competition in iPhone mobile payment apps will cause lower innovation in Android apps as well. Most developers work on apps on the expectation of reaching both sets of consumers, and many would not invest as much (or at all) if they could only reach the Android market. Even though the consumer base on each platform is distinct, the incentives to invest are determined by the aggregate size of the market. Apps have some shared investment and some incremental costs to port to different platforms; the market as a whole determines the incentives to invest. Among the two platforms, the iOS platform has substantially more valuable consumers in terms of demographics and commercial activity.*
>
> *As evidence of the superior desirability of the iPhone user base, the application Instagram was available in on the iPhone for 18 months before the Android version was released. The application built up a user base of 30 million on iOS, and focused on developing a high-quality experience for iPhone users, before making an application for Android phones. This illustrates the value of the iOS audience in motivating innovation.*
>
> *iPhone users are the most satisfied with their smartphone among Australian consumers. Restricting developers' access to this highly engaged, tech-savvy and satisfied group of smartphone users will reduce the incentive to develop advanced mobile payment apps for the Australian market...*[4]
>
> *Access to the large, wealthy pool of iPhone users is needed in order to ensure that developers have sufficient incentive to invest the large sums needed to produce successful, high-quality mobile payment apps.*[5]

The importance of the iPhone customer sector is reflected in overseas research regarding the greater revenue opportunity for mobile payments companies provided by iPhone users than Android users, and the characteristics of iPhone users in Australia. According to research conducted in the US,

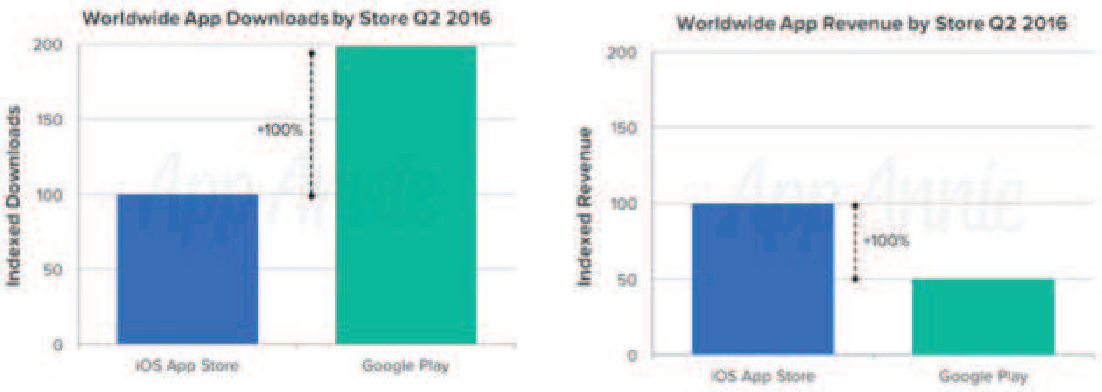
[3] Tim Cook, Q1 2016 earnings call, transcript at http://www.imore.com/tim-apples-ceo-q1-2016: "our iPhone loyalty rate is almost twice as strong as the next-highest brand… Because our customers are very satisfied and engaged, they spend a lot of time on their devices and purchase apps, content, and other services. They also are very likely to buy other Apple products, or replace the one that they own [with a newer model]."

[4] At [99]-[101].

[5] At [103].

Americans who make payments using their iPhones in stores spend nearly double that spent by Android users making the same type of payments.[6] Even though Android accounts for a larger share of smartphones than iPhones do, this does not make up for the shortfall in mobile payment value or frequency. As a result, iPhone customers represent a larger payments revenue opportunity for companies that are interested in developing mobile payment products or other NFC enabled commercial service offerings.

It is also demonstrated by the revenue statistics from the major app stores, Google Play for Android and the Apple App Store for iPhone devices. Worldwide in the second quarter of 2016, there were twice as many downloads from the Google Play store as from the Apple App Store, but revenue generated from the Apple App Store was twice that of the Google Play Store.[7] That is, on average each download from the Apple App Store generated four times the revenue of a download from the Google Play Store.[8]



Source: AppAnnie

Australian download revenues are more skewed towards the iPhone than the worldwide average, with 70% of combined Apple App Store and Google Play Store revenues attributable to the Apple App Store.[9] If these revenues are reflected in customers' tendency to make mobile payments or utilise other NFC enabled commercial services then the importance of iPhone customers to the success of mobile wallets is clear.

Where a mobile wallet is not the primary product of a supplier, for example where it is provided by a bank for the benefit of its retail customers, there are additional challenges in developing an app that can only be used by a fraction of the supplier's customers. Advertising, marketing, service and support are all made more efficient where the same features are available to all customers and operate in the same way regardless of the platform.

The applicants have found that even releasing updates to their iPhone and Android banking apps at different times leads to substantial customer confusion and complaints, and they seek wherever possible to ensure that their apps operate consistently whatever the platform. This is possible for almost every part of a mobile banking app, but not for the NFC function, because of Apple's refusal to provide third-party access to this function.

The tendency for smartphone app developers to address the maximum customer base by developing for multiple platforms, in circumstances where consumers tend to adopt a single smartphone platform,

[6] John Heggestuen, Business Insider Australia, 'IOS users are a much bigger revenue opportunity for mobile payments companies than Android users', 19 June 2014, available at: http://www.businessinsider.com.au/the-biggest-revenue-opportunity-is-on-ios-for-mobile-payment-companies-2014-6?r=US&IR=T (accessed 29 September 2016).

[7] App Annie Q2 Report 2016.

[8] App Annie Index: Market Q2 2016, p 15.

[9] App Annie Index: Market Q2 2016, p 15.

is recognised as an equilibrium allocation where platforms in two-sided markets compete with each other:

> *In one equilibrium allocation all consumers single-home, whereas all firms multi-home. This equilibrium configuration always exists and it mirrors what is seen in the market for smartphones: virtually all consumers use only one smartphone, and almost all apps are available across smartphone providers.*[10]

Apple's insistence on exclusive access to NFC functionality prevents mobile wallet providers from "multi-homing" – that is, making their apps available on multiple platforms – in turn preventing them from reaching the smartphone users they need to make continued investment in these apps worthwhile.

5 Evidence of iPhone user demographics and characteristics

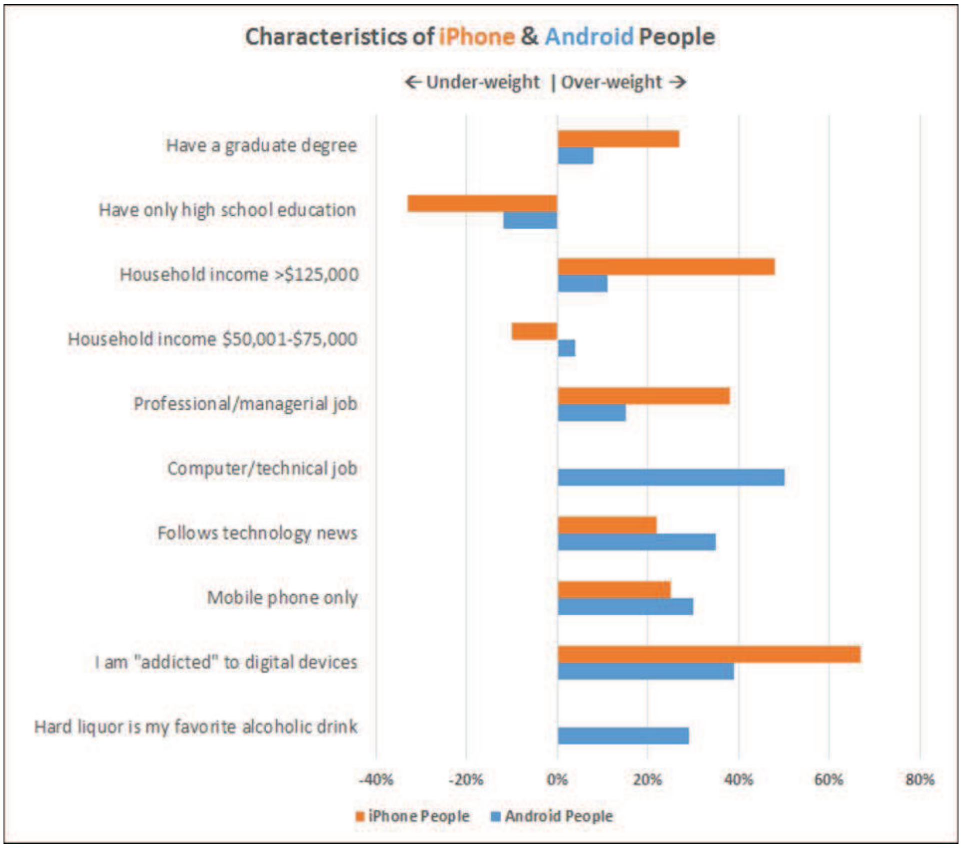
In 2014, *Forbes* published a report on the characteristics of iPhone and Android users, drawing on survey data from CivicScience to explain why app developers focus on the iPhone platform:

> *I'm impressed that iPhone holds a strong lead over Android in app quality several years after Android surpassed iPhone in market share: new apps and new features keep arriving on iPhone well before Android. What might the characteristics of iPhone users tell me about why that happens, and how long it is likely to last?*[11]

The data showed that iPhone users were significantly more "overweight" (ie overrepresented compared to the general population) than Android users on education, household income, professional or managerial employment, and "addiction" to mobile devices as set out in the chart below.

[10] Thomas D Jeitschko and Mark J Tremblay, "Platform competition with endogenous homing", 11 February 2015, available at: http://econweb.umd.edu/~sweeting/EndogHoming_DC-IO-Day.pdf (accessed 17 October 2016).

[11] Todd Hixon, *Forbes,* 'What kind of person prefers an iPhone?', 10 April 2014, available at: http://www.forbes.com/sites/toddhixon/2014/04/10/what-kind-of-person-prefers-an-iphone/#6ef4998d3e5a (accessed 17 October 2016).



Source: CivicScience/Forbes

The report's conclusion reflected these characteristics:

> *iPhone people are a notch up the socio-economic scale: higher income, higher education, higher representation in professional and managerial jobs. They are tech enthusiasts, but more as consumers than producers: a big over-weight for digital device addiction, but none for technical jobs.*
>
> *Why does Apple retain the lead in app quality? The homogeneity of the iOS platform is one big reason: it's much harder to develop for Android due to its many software and hardware variants. This data sheds light on another big reason. iPhone is where the money is, and iPhone people are the most enthusiastic tech adopters. These two factors indicate that Apple's app lead will persist: the problem with Android fragmentation is not going away fast (if at all), and Apple has a strong franchise with the most valuable customers.*

Most of these findings were consistent with previous research undertaken by CivicScience in 2013 on differences between Android and iPhone users:

> *The biggest demographic indicator is household income; Android dominates among the least affluent consumers but the higher up the income spectrum you move, the more likely someone is to prefer iOS. People making over $150,000 in annual income are 66% more likely to choose iOS. This is the most common proxy characteristic we saw in the other correlations uncovered...*
>
> *When crossed with their job type, we found that people in Professional/Managerial roles were more likely to choose iOS...*

> *Finally, when visiting their favorite coffee shop, Android users are 14% more likely to order a regular coffee. iOS users are 28% more likely to order a latte, cappuccino, or other espresso blend.*[12]

These findings are consistent with the banks' experience of customers' use of mobile banking apps and are likely to ensure that access to iPhone customers remains critical for the success of a mobile wallet app.

6 Linking banking apps to the Apple Pay payment mechanism is no substitute for integrated NFC access

Opportunities to link banking applications to the Apple Pay payment mechanism that have recently been made available under iOS 10:

- *are not a substitute for genuine access to the NFC functionality;*
- *do not allow for any real competition with Apple Pay;*
- *come two years after Apple Pay was first launched; and*
- *do not allow the same public benefits as integrated NFC access.*

The ACCC raised a recent update to the Capital One Wallet application for the iPhone as an example of a solution that links a banking application to the Apple Pay application using the additional options for linking between Apple Pay and issuers' applications available under version 10 of the iOS operating system, which was released in September 2016.

While any additional integration or linking possibilities are useful, this is not a substitute for genuine access to the NFC functionality and does not allow for any real competition with Apple Pay.

The applicants understand that the Capital One Wallet application for iPhone performs a number of the functions to be expected of a mobile banking app and are provided by the applicants' own mobile banking apps – such as checking balances, paying bills, and keeping track of payments – but also provides an Apple Pay payment button that links to the Apple Pay application, and may present the payment card selected by the user when it launches the Apple Pay application.

If the applicants' understanding is correct, then this is likely to be an improvement from the customer's perspective over previous implementations, where customers who wished to check their account balances or available credit before choosing a payment card and making a payment would have to launch their mobile banking application, check their balances, exit the application and launch Apple Pay, and then manually select their preferred payment method within Apple Pay before paying with a fingerprint or PIN.

However, this additional integration is not a substitute for access to the iPhone's NFC function for customers, issuers or other application developers for the reasons set out below.

(a) It is still slower and less convenient than a fully integrated solution

While the Capital One Wallet may be quicker and more convenient than previous implementations, it is not as quick and convenient as a fully integrated solution of the kind that would be available if access to the NFC function were provided to third party applications.

[12] John Dick, *CivicScience*, 'How to tell an Android user from an iOS users', 12 November 2013, available at: http://cs-marcomm.demandco.webfactional.com/how-to-tell-an-android-user-from-an-ios-user/ (accessed 17 November 2016).

For example, using the new Capital One Wallet on the iPhone, a customer who wished to check their account balances and available credit paying with the card of their choice may need to verify their identity at least twice – first when opening the Capital One Wallet application, and then again when paying through Apple Pay.

While scanning a fingerprint twice may not appear to be significantly less convenient than scanning it once, it does not take much additional inconvenience – or friction – to affect the customer experience and discourage users from returning to an application (ie, picture a checkout line at busy store, with everybody having to scan fingerprints twice). Further, if a customer' has chosen, or is forced, to secure their mobile application with a PIN or password instead of a fingerprint, entering it twice would compound the inconvenience and cost in terms of the consumer's time value (for example ANZ's own "goMoney" mobile banking application does not implement fingerprint security).

The time taken to accept a payment is also one of the most significant costs for merchants of receiving payments from consumers so additional time taken to access the payment mechanism will also create a cost for merchants. As noted by the RBA:

> *The aggregate resource cost incurred by merchants and financial institutions in receiving payments from consumers is estimated to be about $8.4 billion in 2013, or about 0.54 per cent of GDP. Financial institutions incur the majority of these costs. Around one-third of costs are incurred by merchants, with tender time (the time taken at the till to process the payment) being the most significant component.*[13]

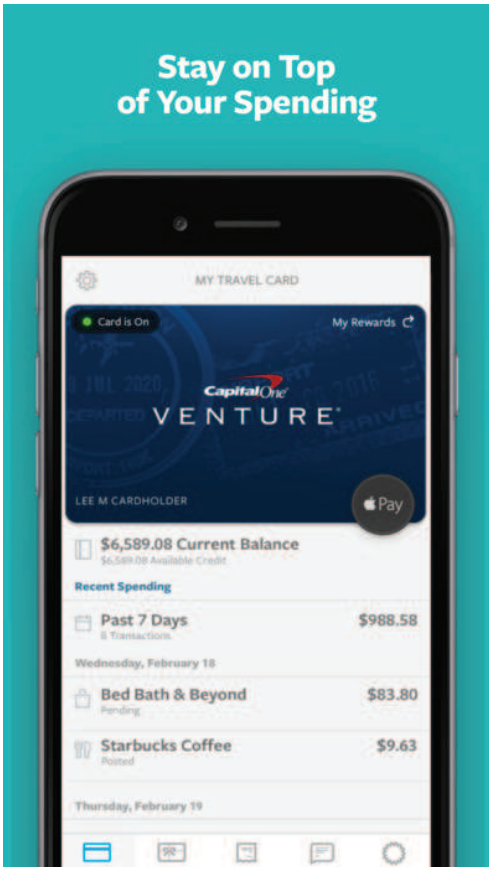
For example, contactless card payments typically take half the time to tender that contact-only payments take. This reduced tender time reduces the merchant cost by 14% for credit cards and by 30% for debit cards. According to the discussion paper:

> *As a 2 second change in tender time implies a one cent ($0.01) change in merchant costs, small efficiency gains or delays can make a large difference to the total resource cost of the instrument.*[14]

Access to the NFC function, without being forced to go through Apple Pay, would allow customers to verify their identity once – when opening the banking app – and then select their payment card and pay without repeating the verification. This appears to be the way the Capital One Wallet operates on the Android platform, where the corresponding button does not link to an external mobile wallet but allows payment through the Capital One Wallet directly.

[13] Chris Stewart, Iris Chan, Crystal Ossolinski, David Halperin and Paul Ryan, RBA The Evolution of Payment Costs in Australia, Research Discussion Paper, at page 2 available at: http://www.rba.gov.au/publications/rdp/2014/pdf/rdp2014-14.pdf.

[14] Chris Stewart, Iris Chan, Crystal Ossolinski, David Halperin and Paul Ryan, RBA The Evolution of Payment Costs in Australia, Research Discussion Paper, at page 40 available at: http://www.rba.gov.au/publications/rdp/2014/pdf/rdp2014-14.pdf.



Stay on Top of Your Spending

MY TRAVEL CARD

Card is On

My Rewards

Capital One

VENTURE

LEE M CARDHOLDER

Pay

$6,589.08 Current Balance

$6,589.08 Available Credit

Recent Spending

Past 7 Days $988.58

8 Transactions

Wednesday, February 18

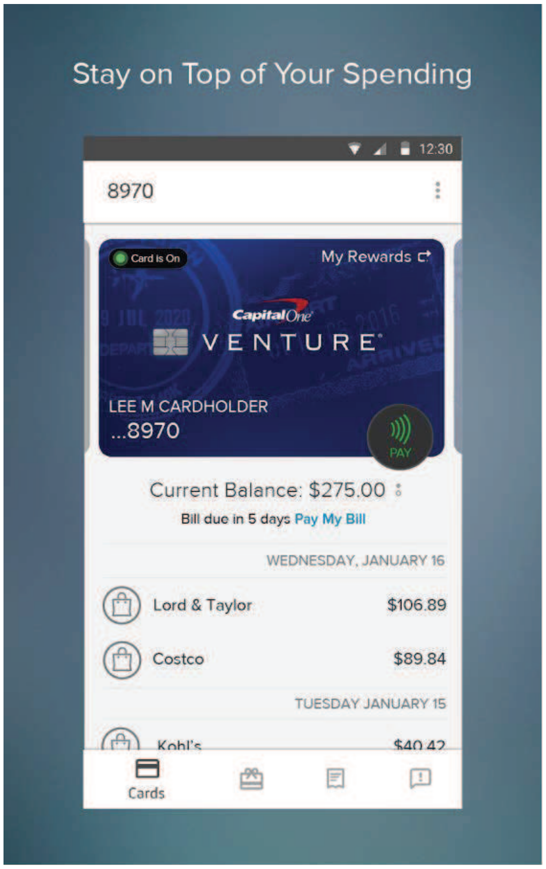
Bed Bath & Beyond $83.80

Pending

Starbucks Coffee $9.63

Posted

Thursday, February 19



Stay on Top of Your Spending

12:30

8970

Card is On

My Rewards

Capital One

VENTURE

LEE M CARDHOLDER

...8970

PAY

Current Balance: $275.00

Bill due in 5 days Pay My Bill

WEDNESDAY, JANUARY 16

Lord & Taylor $106.89

Costco $89.84

TUESDAY JANUARY 15

Kohl's $40.42

Cards

iPhone version **Android version**

This difference between iPhone and Android versions is likely to make marketing and customer support significantly more complex as different processes apply to different parts of the customer base.

In addition, the linking between an issuer's mobile wallet and Apple Pay appears to be one-way – that is, it provides a link to Apple Pay, possibly specifying the payment card to be used, but it is not clear that Apple Pay returns any information to the banking app, such as whether the payment was successfully submitted or the value of the payment. Although this information is available to the banking app through the payment and mobile networks, this communication may not be as quick as communication through the NFC interface, as further discussed below at section 7.

(b) It does not provide any differentiation or innovation in payment mechanisms

The linking suggested by the Capital One Wallet implementation allows an issuer's mobile wallet to initiate an Apple Pay transaction, avoiding the need for a user to manually switch between applications, but it does not allow another wallet to provide a payment mechanism that differentiates itself from, or innovates in relation to, the Apple Pay mechanism. Although it has been suggested that no differentiation is possible in this area,[15] there are in fact a number of different approaches available that may have greater appeal to certain users than the Apple Pay implementation.

For example, while Touch ID is a convenient customer verification method, there are a number of alternative approaches that may be more appealing to some customers. For example, Apple Pay implements a system-wide customer verification method, which means that if you can unlock an

[15] Dr David Glance submission, 9 September 2016, p 3.

iPhone you can make a payment with any card in Apple Pay. Apple's Touch ID implementation allows up to five fingerprints to be registered, and many customers register a family member or partner's fingerprint – or share their passcode with them – for reasons of convenience.

A competing mobile wallet could require different verifications for different cards – for example, ensuring that only certain users can access certain or any cards. Competing mobile wallets could also provide different verification methods that may be more secure than fingerprints, such as a spoken password that would require both a matching voiceprint and a correct password.

(c) It does not provide a solution for the customer segment who prefers payments to be made by financial institutions rather than Apple

There is a large customer segment that would prefer a financial institution rather than a technology company to be trusted with their payments.

According to consumer survey data provided by Retail Finance Intelligence Pty Limited, 73% of iPhone users would prefer an app that allows payments to be made from a mobile phone using a credit or debit card registered to the app to be provided by a financial institution rather than a technology company whose products they use (6%) or a card scheme (21%). This iPhone user percentage is reflective of the preference among all consumers in the sample regardless of the handset.[16]

The integration of a banking app with Apple Pay, such that Apple Pay is exclusively used to provision payment card credentials and to initiate contactless payments, is unlikely to satisfy the preferences of these customers.

(d) It does not provide any price competition to Apple Pay

Apple Pay payments initiated from an issuer's banking application will presumably attract the same fees payable to Apple as any other payment made using Apple Pay. Since Apple Pay will remain the only way for iPhone users to make NFC payments, these prices will remain supra-competitive and will not be subject to any downward pressure. This will particularly be the case if Apple continues to prevent issuers from passing through any of the cost of Apple Pay to customers.

(e) Other developers could provide additional features and functionality more quickly and effectively

The integration of Apple Pay with issuers' banking apps has proceeded slowly over the two years since Apple Pay was launched. The Capital One Wallet for Android added integrated mobile payments in October 2015, almost a year before Apple added the operating system features that allowed the Capital One Wallet on the iPhone to link to Apple Pay.

Previous developments in the integration of Apple Pay with other applications include using another application to provide the second-factor authentication associated with adding a new payment card to Apple Pay; and allowing an application to add a payment card directly to Apple Pay. These are welcome developments, but mobile wallet and mobile payment providers and other issuers remain in the difficult position of waiting for Apple to provide these necessary integrations in its absolute discretion, when a far wider range of innovations could be achieved much sooner if developers had access to the NFC function itself.

This may be particularly evident when seeking to integrate or develop Australian specific features implemented via NFC of great interest to the local market, but of limited interest globally to Apple, such as local transit system integration or integration with various Australian Government specific features such as the Medicare mobile app.

[16] *RFi Australian Digital Banking Program* 2016.

7 Non-integrated solutions cannot substitute for integrated NFC access or provide the same public benefits

While non-integrated solutions can provide part of the functionality of integrated NFC access, in all cases they are less convenient and reliable than integrated NFC access, and there are important areas in which they cannot substitute for integrated NFC access. Customers have a strong preference for integrated NFC solutions, and non-integrated solutions such as stickers are at best a temporary workaround.

Since Apple did not introduce NFC capabilities to the iPhone until 2014 and those capabilities remain exclusive to Apple Pay, issuers in Australia and overseas who wish to provide their own NFC payment capabilities to customers who use iPhones have experimented with non-integrated solutions such as stickers, wristbands and key fobs. For example:

- in the United Kingdom, Barclays offers a range of NFC-enabled accessories under its “bPay” branding, including stickers, wristbands, keychains and a “loop” for a watch band or fitness tracker;
- in New Zealand, ASB offers a sticker, the ASB PayTag;
- In Australia:
  - Coles offers a sticker, the Coles Pay Tag;
  - NAB offers a sticker, the NAB PayTag;
  - CBA offers a sticker, the CommBank PayTag;
  - People’s Choice Credit Union offers a PayTag;
  - AMP Bank offers a PayTag; and
  - Cash by Optus offers a sticker and a wristband.

Each of these solutions is effectively a resized contactless payment card and operates independently of any mobile device. The sticker can be stuck anywhere but is typically attached to the back of a mobile phone or its case.

(a) Communications between the mobile and the sticker

The mobile phone cannot send instructions to, or receive any information from, the sticker. Any information that the mobile phone receives in relation to a transaction made using the sticker must come indirectly from the merchant terminal through the payment network to the issuer’s system, and then through the mobile network to the customer’s mobile phone – where it will typically be received by the issuer’s app.

Using an issuer’s app, a customer may send instructions to the issuer’s systems that will prevent a payment attempted using the sticker from being approved, or change the payment method used to pay for purchases made using the sticker – typically another credit card or transaction account held with the issuing institution. However, the customer cannot physically disable the sticker’s antenna or alter the payment card number or type that is transmitted to the merchant terminal.

Communications between the mobile and the sticker depend on the payment network and the mobile network. The speed of the payment network is increasing but still varies by issuer. For example, ANZ has not updated its core banking information technology in a number of years and it can take more than 24 hours for card payments to appear on online statements or the ANZ banking apps.[17] Other issuers are closer to real-time.

Communications through the mobile data network can also be unreliable due to service interruptions or coverage issues, particularly indoors or in rural areas. Customers on pre-paid accounts may run out of credit, which severs the data connection; and customers travelling overseas may turn off their data to avoid roaming high charges. In these circumstances, while NFC payments will still be possible on integrated and non-integrated mobile wallets, even indirect communication between a mobile phone and an NFC sticker will not be possible.

(b) Communication in integrated mobile wallets

By contrast, an NFC controller integrated into a mobile device can communicate information about an NFC payment, or other NFC uses, to an app running on that device without the need to communicate through the payment network or the mobile network.

In some implementations the NFC controller may communicate directly with an applet in a secure element, which can then communicate at a more abstracted level with applications in the main part of the mobile phone. In other cases the NFC controller may communicate more directly with an application itself, though it will likely be mediated by the operating system. Either way, an integrated mobile wallet allows for meaningful two-way communication between the application and the NFC controller even in card emulation mode.

This communication allows a mobile wallet application to determine which payment card will be used to make a payment according to the user's selection or instruction – for example, the user could instruct the application to make a payment using a debit card if the account balance is above a certain level, but to use a credit card otherwise. Location-based determination could also be used. That communication also allows the mobile wallet to verify each transaction through a PIN or a fingerprint, and to know as soon as a payment has been successfully submitted and the details of that payment, rather than waiting for a response through the payment and mobile networks.

Further communication in NFC card payments is also likely to be possible as communication and payment standards evolve and merchant terminal software is upgraded. Additional communication will also be possible using NFC modes other than card emulation – in particular the peer-to-peer and reader/writer NFC modes that allow for a wider range of applications such as file transfers, the exchange of contact details, or acting a merchant terminal – if Apple chooses to provide a level of access to those modes as well, as other operating systems have done for many years.

(c) NFC stickers on NFC-enabled mobile phones can lead to card clash

NFC stickers were developed in an era when fewer phones, and no iPhones, had integrated NFC capabilities. Now that most new mobile phones and all new iPhones have an integrated NFC controller and antenna, any NFC sticker attached to such a phone can lead to radiofrequency interference or "clash" between the two NFC systems.

This can lead to unpredictable results, as a merchant terminal will need to choose which NFC system to communicate with, and will either choose one on an unpredictable basis or refuse to communicate with either. Since the signal of the integrated NFC antenna will often be amplified using the power of the mobile phone battery, it will tend to prevail over the sticker.

This effect may be reduced by placing the sticker as far as possible from the NFC antenna, but most users will not be aware of card clash or of the internal layout of their phones when they attach the sticker, and remembering which part of the phone to orient towards the contactless payment terminal does not provide for a seamless customer experience – particularly where a user is interacting with a

[17] Renai Lemai, *Delimiter.* "ANZ Bank says no business case for core banking IT overhaul", 11 July 2016, available at https://delimiter.com.au/2016/07/11/anz-bank-holds-firm-core-banking-overhaul-trend/ (accessed 26 October 2016).

wide range of payment terminals, including in the near future public transit terminals, whose own NFC antennas may be placed in different locations.

For this reason alone the applicants do not consider that NFC stickers are anything but an interim measure. They would be surprised if Apple were to encourage or even allow participants in Apple Pay to add their own NFC stickers to NFC-enabled iPhones.

In a report attached to Apple's submission dated 26 October, Dr Christopher Pleatsikas suggests that ANZ provides "both integrated and non-integrated mobile wallets to its customers" but does not appear to be using these terms in the same way as Dr Geoff Edwards and the applicants use them. To the applicants' knowledge, ANZ has never offered an external NFC tag or sticker. ANZ does offer its own mobile wallet application, ANZ Mobile Pay, on the Android platform, making use of the access to the NFC functionality provided by Android – as well as participating in Android Pay. On the iPhone it participates in Apple Pay but cannot provide its own integrated mobile wallet application due to the lack of access to the iPhone's NFC functionality, and it offers mobile banking applications but none of its own NFC payment applications using tags, stickers or otherwise.

The report of Dr Christopher Pleatsikas attached to Apple's submission dated 26 October 2016 argues that this concern only arises where cardholders use mobile wallets from more than one issuer, and in those cases users will only want to use Apple Pay.[18]

This is incorrect from a technical perspective and not supported from a user perspective. Card clash will become an issue as soon as a user engages the iPhone's NFC functionality by adding a payment card to Apple Pay: from then onward, an NFC sticker attached to the iPhone will be vulnerable to card clash and will deliver unreliable results. A user will therefore have to decide whether to use Apple Pay or an NFC sticker but cannot in practice use both.

In these circumstances the applicants agree that, if Apple Pay remains the only integrated mobile wallet permitted on the iPhone, customers with cards from more than one issuer – and in all likelihood most other customers – will choose Apple Pay rather than a wallet that relies on an NFC sticker. This is not due to an inherent preference of iOS users for using a third party mobile wallet when they have cards from multiple issuers, as Dr Pleatsikas suggests (such users may instead inherently prefer to use multiple issuer proprietary mobile wallets, all else equal), but rather this is due to Apple Pay being, in this case, the only integrated mobile wallet available to iOS users. If access to the NFC function were available, the applicants consider that a likely outcome would be that customers with cards from more than one issuer would load most or all of their cards into Apple Pay, and would also load some or all of their cards into issuers' separate apps, depending on which apps provide them with greater value than Apple Pay in terms of useful information or financial rewards.

Customers would then have a choice of different mobile wallet applications for different circumstances. As set out in section 10 below, there is no reason why this choice should compromise customer experience – rather, it will enhance customer experience by better meeting customer preferences.

(d) Only integrated mobile wallets can switch between multiple cards

An integrated wallet can tokenise multiple payment cards and allow the customer to switch between them easily, for example by swiping across the mobile screen. Depending on the user's selection, a different card and even a different kind of card can be presented to the merchant – for example, an American Express credit card, a Visa or MasterCard credit card or debit card, or another card scheme such as Interac in Canada or eftpos in Australia.

The kind of card that is presented will have consequences for the merchant, the issuer and the customer. For example, different cards and different schemes involve different interchange fees and may be subject to different merchant surcharges. Different cards may attract different rewards when used at different retailers.

[18] Pleatsikas Report at p 14.

An NFC sticker can only present a single payment card to a merchant and that card can never change. A customer can use a mobile banking or payment app to communicate with the issuer's servers and change the account that is linked to that card – for example to a different transaction account or credit card account. However, the original payment will always be made using the payment method associated with the sticker itself. This means that if the sticker is really a Visa or MasterCard credit card, then linking a payment method that would otherwise be less costly will not reduce the cost of the transaction.

As a result, only an integrated NFC wallet allows a customer to choose between different payment types in a meaningful way that reflects the underlying cost of those payment methods. This will become critical as merchants are limited to surcharging at or below their reasonable costs of processing the payment – and also as eftpos is now able to provide contactless payments typically at a lower cost than the credit card schemes.

Further, NFC stickers make it difficult or impossible for the cards of multiple issuers to coexist on the same device. Even if there were room for multiple stickers on a mobile phone, card clash would make the results unpredictable. An NFC sticker cannot be physically disabled by a mobile application: the application can only instruct the issuing bank's servers not to accept any transaction submitted by that sticker; the sticker will continue to try to make payments – that is, the sticker remains a "live" NFC antenna for transaction purposes at all times, with the "stop" only occurring after the terminal attempts to verify and complete the initiated transaction. As a result there is no way to prevent card clash by "turning off" stickers.

(e) Only integrated wallets can easily secure transactions with a PIN or fingerprint

An NFC sticker itself cannot provide any additional security over what is available on a contactless card: that is, a sticker will process all payments under $100 without requiring any customer verification, while payments over $100 will require a PIN to be entered into the merchant terminal. An integrated mobile wallet can secure transactions in a number of ways that provide a better balance of security and convenience and can give effect to consumer preferences. For example, fingerprint identification can provide far greater security than contactless cards for payments under $100 while providing at least the same level of convenience.

The only way an NFC sticker can be made secure using a mobile wallet application would be for the application to instruct the issuer's server to block payments made using the sticker, and only instructing the server to unblock payments when the user had opened the application and entered a PIN or a fingerprint. There are a number of risks to this method:

- First, it assumes that the sticker is turned "off" (ie, the issuer's server declining payments using the sticker) most of the time. Where this relies on the customer turning the sticker "off" after every transaction, this assumption is clearly vulnerable to human error and to criminal activity – for example, if a criminal snatched a wallet with a sticker while the user was making a transaction, the sticker would not be turned "off" and would remain live and insecure. If the application were to automatically turn the sticker "off" after a period of time or when the user exited the application, this would fail if the application crashed, if the mobile phone ran out of power or if the data network failed to deliver the message. That is, it is not safe to assume that the sticker is "off".

- Second, turning the sticker back "on" would come at a significant cost to time and convenience. The application would need to be opened and unlocked by a PIN or fingerprint in advance of the payment to ensure that the sticker was turned "on" before the NFC payment was submitted. This would introduce substantial delay – which may be acceptable when paying for a purchase but not when tapping on or off in public transport – and would also be susceptible to issues with the data network.

In summary, while this method may provide some additional security over a contactless card, it will be substantially less convenient. As a result, it is not likely to be useful to customers and will not substitute for the verification provided by an integrated mobile wallet.

(f) Only integrated NFC wallets can potentially allow payments over $100 without a PIN

Integrated NFC mobile wallets are consumer devices that can provide their own customer verification method, known as a Consumer Device Cardholder Verification Method (**CDCVM**), to allow payments over $100 using a fingerprint, a PIN entered into the device, or another verification method such as iris recognition. This capability is not available to an NFC sticker.

The applicants have not yet taken advantage of their capability in their Android mobile wallets for a number of reasons. The CDCVM standard is new and many merchant terminals in Australia have not yet been upgraded to recognise this form of verification. Further, banks that need to offer both integrated and non-integrated digital wallets in order to reach the majority of their customers have incentives to maintain consistent thresholds for all contactless payments in order to avoid customer and merchant confusion.

If they are able to move to integrated digital wallets and CDCVM terminal infrastructure becomes more widespread, they may well decide to implement PIN-free transactions over $100. The applicants are happy to discuss their plans with the ACCC on an individual and confidential basis.

(g) Tokenisation is more secure and more convenient on an integrated mobile wallet

Tokenisation is not limited to integrated mobile wallets and it is possible to store a token on an NFC sticker. However, this token must be generated and stored before the sticker is sent to the customer. It will not be possible to update the sticker with a new token if the old token is compromised; and the user cannot add another payment card to the sticker by requesting a new token. This is less secure and less convenient than tokenisation through an integrated mobile wallet, which can be provisioned "over the air" as often as is considered necessary.

(h) Stickers are a weak substitute for integrated NFC mobile wallets

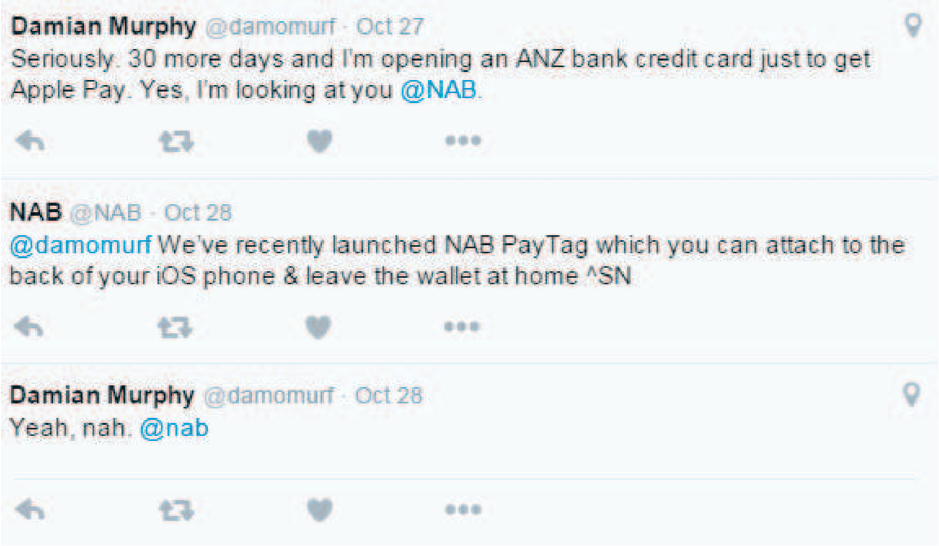
While a non-integrated mobile application with an external NFC sticker can approximate some of the functions of an integrated mobile wallet, it cannot perform any of these functions as securely, seamlessly and conveniently, and cannot perform some of these functions at all. Where mobile wallets and mobile payments must be at least as convenient as contactless cards, it is unlikely that non-integrated mobile wallets will ever be widely adopted – particularly where integrated alternatives are available.

Those of the applicants who have experimented with NFC stickers have provided individual and confidential responses to the ACCC in relation to their reasons for offering these stickers and their experiences with them. Those responses are certainly consistent with the conclusions of the report cited by the ACCC in investigating the possibilities of non-integrated wallets:

> *Not wanting to leave iPhone customers out in the cold, probably knowing that they drive technology adoption more than the handful of Android handsets owned by people who actually know what NFC is, the Commonwealth Bank developed the PayTag. It's a sticker that contains the same NFC circuitry as in the traditional card. Stick it on your device and tap away…*
>
> *I don't think most of us will be throwing away our wallets just yet. It smells so much of a hack that unless you're super desperate for this sort of feature, I don't know why you'd tarnish your iPhone's form with this sticker.*[19]

[19] Anthony Agius, *Reckoner*, "Commonwealth Bank's PayTag – Hands On", 21 January 2014, available at http://reckoner.com.au/2014/01/commonwealth-banks-paytag-hands-on/ (accessed 29 October 2016).

The following exchange on Twitter is also reflective of many customers' attitudes towards non-integrated mobile wallets.



Damian Murphy @damomurf · Oct 27

Seriously. 30 more days and I'm opening an ANZ bank credit card just to get Apple Pay. Yes, I'm looking at you @NAB.

NAB @NAB · Oct 28

@damomurf We've recently launched NAB PayTag which you can attach to the back of your iOS phone & leave the wallet at home ^SN

Damian Murphy @damomurf · Oct 28

Yeah, nah. @nab

8 Case studies: Failure of mobile wallets without access to the iPhone's NFC functionality

A number of recent case studies illustrate the importance of obtaining access to the NFC function on the iPhone. In all of these case studies, Android had a comparable share of smartphone sales to that in Australia and mobile wallets were prevented from reaching their potential by Apple's refusal to provide access to the NFC functionality, which forced them to either:

- make use of the NFC function on the Android platform and remove iPhone users from their potential customer base for this product; or
- attempt to reach both iPhone and Android customers by avoiding use of the NFC function and using less widespread and more inconvenient technologies such as QR codes and Bluetooth.

(a) Semble

Semble was a joint venture in New Zealand between two banks (ASB and BNZ), three mobile carriers (2degrees, Spark and Vodafone) and a payments network operator, Paymark (owned by ASB, BNZ, ANZ and Westpac). It offered NFC payments using cards from its issuer members as well as the Snapper public transport card, which can be used in buses and taxis and in parking meters.

Semble launched in 2015 on the Android platform using NFC-enabled SIM cards from each of the mobile carriers. However, it closed in July 2016. Its failure was attributed in part to its lack of support for the iPhone platform:

> *The app did not work with iPhones, so was limited in the number of customers who could access it.*[20]

This limitation had been identified as a challenge to Semble since its announcement in October 2014:

> *The most obvious [stumbling block] is that Semble is Android-only at this point.*
>
> *With its new iPhone 6 and 6 Plus, Apple has finally added an NFC (near-field communications) chip, NFC being the key technology for making wireless instore payments. But as [Semble CEO Rob] Ellis notes, Apple isn't allowing any app makers access to its new phones' NFC at this point – the better to promote its own Apple Pay (being launched in the US this month) for instore payments…*
>
> *When will it? No one knows. Vodafone CEO Russell Stanners struck a relaxed pose on this issue at the Semble launch last night, telling NBR it was typical for Apple to hold a new technology tight for a few months before opening it up.*[21]

This echoed the common expectation that the iPhone's NFC infrastructure would eventually be opened to third party applications:

> *Apple did the same thing last year when it introduced the Touch ID fingerprint sensor with the iPhone 5S. For the first year, you could use the sensor to only unlock your phone and buy apps and media from iTunes. But with iOS 8, Apple is opening up Touch ID to developers, so you will be able to use it within third-party apps as well. It's safe to assume that's exactly what will happen with the NFC chip next year.*[22]

This assumption appears to have been encouraged by Apple following the launch of Apple Pay:

> *An Apple spokesperson confirmed the lock down of the technology, saying developers would be restricted from utilising its NFC chip functionality for at least a year. Apple declined to comment on whether NFC capability would remain off limits beyond that period.*[23]

In fact, Apple's first public statement that it intended to prevent third party use of the NFC functionality in the longer term came in July 2016 in response to the Swiss Consumer Protection Authority's complaint to the Competition Commission:

> *We will not open NFC for third-party payment services – for safety and convenience reasons.*[24]

Apple has since confirmed this position in its response to the present application. Mobile wallet providers like Semble, who had been hoping that Apple would treat the NFC function in the same way as it has treated other functions such as Touch ID, have not been able to sustain their operations on the basis of Android customers alone.

[20] Susan Edmonds, *Stuff*, 'Developers of Semble mobile wallet app "refocusing", 15 July 2016, available at: http://www.stuff.co.nz/business/82147557/Developers-of-Semble-mobile-wallet-app-refocusing (accessed 17 October 2016).

[21] Chris Keall, *NBR*, 'Telcos unite behind Semble mobile wallet, but 5 stumbling blocks remain', 9 October 2014, available at: https://www.nbr.co.nz/opinion/telcos-unite-behind-semble-mobile-wallet-5-stumbling-blocks-remain (accessed 17 October 2016).

[22] Pranav Dixit, *Gizmodo*, 'The iPhone 6's NFC chip only works with Apple Pay', 17 September 2014, available at: http://www.gizmodo.com.au/2014/09/the-nfc-chip-in-your-new-iphone-is-only-good-for-apple-pay-for-now/ (accessed 17 October 2016).

[23] Claire Reilly, *CNET,* 'Apple locks iPhone 6 NFC to Apple Pay', 16 September 2014, available at: https://www.cnet.com/news/apple-locks-down-iphone-6-nfc-to-apple-pay/ (accessed 17 October 2016).

[24] Translated from the German "Wir werden NFC nicht für Drittanbieter von Bezahldiensten öffnen – aus Sicherheits- und Bedienkomfortgründen". Henning Steier, *Neue Zürcher Zeitung*, 'Apple Pay startet in der Schweiz', 7 July 2016, available at: http://www.nzz.ch/digital/bezahlsystem-apple-pay-startet-in-der-schweiz-ld.104159 (accessed 17 October 2016).

(b) SureTap

In Canada, the Suretap wallet was introduced in 2015 by card issuers Rogers Bank and CIBC in collaboration with mobile carriers Bell, Rogers, Telus, Koodo and Virgin Mobile and around 45 retailers and 90 loyalty programs. It used the NFC function enabled on Android and BlackBerry mobile phones to make payments and store gift and loyalty cards.

However, Suretap was discontinued in August 2016. Its chief operating officer Almis Ledas attributed the failure in part to a lack of access to the iPhone's payment functionality:

> *"If we'd been able to deploy a wallet on Apple and non-Apple handsets, we would have more access for issuers and it would still be in existence today," Ledas says. "We went to Apple and talked about getting access to the secure element. The answer was clear – no."*[25]

Suretap president Jeppe Dorff has also attributed the wallet's failure to an inability to scale, and to execute effective mass market advertising campaigns, because of a lack of access to iPhone customers – in turn due to a lack of access to the iPhone's NFC function.

As a result, despite being pre-installed on most Android and BlackBerry mobiles sold in Canada and attracting around one million customers, the Suretap wallet was not able to survive.

(c) CurrentC

In the United States, **CurrentC** was launched by some of the largest retailers including 7-Eleven, Walmart, Best Buy, Lowe's, Sears, Target and CVS, together accounting for around 110,000 retail locations and $US1 trillion in annual sales.

It used QR code scanning and supported automatic discounts and loyalty programs, and was developed in part to provide retailers with a payment option that was cheaper than the merchant fees charged by the card schemes.

A number of CurrentC merchants were reported to have attempted to promote CurrentC over Apple Pay by disabling the NFC capabilities of their merchant terminals. Most of these merchants now accept Apple Pay. CurrentC closed down in June 2016.

(d) Paymit

In Switzerland, Paymit, a peer-to-peer and QR-code based mobile payment system backed by UBS, Zürcher Kantonalbank and the SIX Swiss stock exchange, announced that it was merging

[25] Gary Ng, *iPhone in Canada*, 'Suretap Wallet to Shut Down in August, Lays Partial Blame on Apple', 14 July 2016, available at: http://www.iphoneincanada.ca/carriers/suretap-wallet-shut-down/ (accessed 29 September 2016).

with rival Twint, a Bluetooth Low Energy and QR-code based payment mobile system backed by Credit Suisse and PostFinance, in May 2016. Twint chose QR and Bluetooth instead of the more widely accepted NFC because of lack of access to the iPhone's NFC functionality:

> *Twint wants to offer a payment solution that can be used with both iOS and Android smartphones. NFC cannot currently be used with iPhones (iOS).*[26]

A new Twint will be launched in 2017, again combining Bluetooth and QR-code payments. Swiss media reports that, apart from now being later to market than Apple Pay:

> *Twint faces another significant disadvantage against Apple Pay: Apple blocks NFC (Near Field Communication) technology in its smartphones for other payment operators. With a 50 per cent share of the smartphone market [in Switzerland], that is a serious obstacle. It was already enough to cause the Swisscom payment app Tapit to fail.*
>
> *In the meantime, Apple Pay can connect with the payment terminals of most Swiss retailers. The Bluetooth technology, which Twint relies on, is not yet widely used in stores.*[27]

The reference to Tapit is to a previous mobile wallet developed in 2014 by Swisscom but also used by the other Swiss mobile carriers Orange and Sunrise, which allowed contactless NFC payments using Visa credit and prepaid cards issued by Cornèrcard and MasterCard credit cards issued by the Aduno Group/Viseca, along with building access.

However, it was limited to Android smartphones. At launch the Tapit press release concluded that "Tapit for the iPhone is still in development", but without access to the iPhone's NFC function it could not be developed. Tapit closed in 2015 and rolled into Paymit.

Switzerland has recently seen the failure of mobile wallets using NFC technology limited to Android devices, and multi-platform wallets limited to QR code and Bluetooth technology.

- It is not surprising that the Swiss consumer protection authority has recently filed a complaint with the Swiss competition commission in relation to Apple's refusal to grant Twint access to the iPhone's NFC technology.[28]

9 Recent submissions do not alter the view that NFC function access will not compromise security

The applicants have examined claims made in recent submissions regarding access to the NFC function and security and remain of the view that no evidence has been advanced to support the suggestion that providing access to the NFC function would affect the security of any mobile wallet or mobile payment system available on the iPhone, including Apple Pay.

The submissions refer to a number of reports that are said to be relevant to the security implications of providing access to the NFC function. When examining the claims made in the submissions and the reports they rely on, it is important to distinguish between potential security issues that happen to involve Android devices, and the suggestion that the potential security issues actually arise *because of* the provision of access to the Android NFC function. None of the claims about potential security issues are directly linked to the provision of access to NFC functionality.

[26] Twint, FAQs, 'Why is beacon technology used rather than NFC?', available at: https://www.twint.ch/en/support/faq/ (accessed 29 September 2016).

[27] *Finews*, 'Apple Pay arrival unseats Swiss competition' July 2016, available at: http://www.finews.com/news/english-news/23608-apple-pay-arrival-unseats-swiss-competition (accessed 29 September 2016).

[28] *Telecom Paper*, 'SKS files Apple m-payments complaint with Weko', 6 July 2016, available at: http://www.telecompaper.com/news/sks-files-apple-m-payments-complaint-with-weko--1152095 (accessed 30 September 2016); Apple, Press Release; Apple, Press Release, 'Apple Pay now available in Switzerland', 7 July 2016, available at: http://www.apple.com/newsroom/2016/07/apple-pay-now-available-in-switzerland.html (accessed 30 September 2016).

It should also be remembered that, while Apple has an interest in protecting its reputation for security, the card issuers have just as much at stake in terms of reputation – and also have financial liability for any fraudulent or unauthorised payments. The issuers have every incentive to ensure that the security of mobile payments is not compromised.

(a) Relay attacks

In its submission, Apple argues that:

> *Android devices, which provide open access to their NFC radios to banks, have been shown to be susceptible to third party attacks that can compromise the customer's card information.*[29]

The report Apple cites in support of this claim refers to a demonstration of an Android application that uses the device as an NFC *reader* to initiate transactions using any physical contactless cards located within NFC distance of that device.[30] There are a number of conditions and limitations to this demonstration that appear to make such an attack extremely unlikely in real-world situations.[31] Perhaps the most relevant consideration is that to fall victim to such an attack requires a person to have actively downloaded, installed, given NFC permissions to, and run a malicious application on their phone as a minimum before any of the other limitations on the likelihood of such an attack occurring can even come into play.

This possibility arises on the Android platform only because Android allows users to install applications from any source on their devices. On the iPhone platform, users are only permitted to install applications from the Apple App Store, and apps are only allowed on the App Store after being thoroughly scrutinised reviewed by Apple.

It is inconceivable that Apple would allow an application of the kind described in this report into the App Store and onto users' iPhones, if Apple were to provide access to the iPhone's NFC functionality. It is more likely that Apple would apply additional and stricter criteria before require additional measures before approving an NFC app for the iPhone, and would only allow apps that could demonstrate that they are secure.

(b) Samsung Pay

Apple's submission argues that:

> *There have also been reports of non-NFC security issues related to Samsung Pay, which is why it is so important to Apple to maintain the tight integration of our hardware, software, and services such as in Apple Pay.*[32]

The report that Apple's submission links to in relation to this claim refers to a demonstration of a method to obtain tokens used by Samsung Pay's magnetic secure transmission (**MST**) hardware, which emulates older magnetic stripe technology. Samsung has responded that it is extremely unlikely that a token obtained in this way could be used to make a fraudulent payment, since not only the token but a unique cryptogram generated when the customer authenticates a payment must also be captured, and the fraudster would also have to ensure that the genuine payment is not completed as that would invalidate the fraudulent signal.

Samsung concludes:

[29] Apple Submission, 26 August 2016, at p 10.

[30] Cammy Harbison, *iDigitalTimes*. "New Android NFC attack could steal money from credit cards anytime your phone is near", 31 May 2015., available at http://www.idigitaltimes.com/new-android-nfc-attack-could-steal-money-credit-cards-anytime-your-phone-near-445497 (accessed 28 October 2016).

[31] See Anoynmous, "Practical experiences on NFC relay attacks with Android: Virtual pickpocketing revisited", available at https://conference.hitb.org/hitbsecconf2015ams/wp-content/uploads/2014/12/WHITEPAPER-Relay-Attacks-in-EMV-Contactless-Cards.pdf (accessed 28 October 2016).

[32] Apple Submission, 26 August 2016, at p 10.

> *This skimming attack model has been a known issue reviewed by the card networks and Samsung pay and our partners deemed this potential risk acceptable given the extremely low likelihood of a successful token relay attack.*[33]

Even if these reports do show a vulnerability in Samsung Pay, Apple acknowledges that these reports do not relate to the NFC function or the provision of access to that function. Further, the applicants understand that Samsung does *not* provide software access to the MST function at present, so Apple's argument that there is a correlation between open access and security is not supported by this example.

(c) Other attacks

Mr John Montagu argues in his submission that:

> *In many instances amongst the security and cryptography community commentary exists that attackers have been able to exploit access to the NFC radio via the published APIs on the Android platform to make fraudulent and or unauthorised payments. There are many sources for the commentary discussing the attacks.*[34]

However, the only source Mr Montagu cites is a recent Europol report that notes:

> *The possibility of compromising NFC transactions was explored by academia years ago and it appears that fraudsters have finally made progress in the area. Several vendors in the Darknet offer software that uploads compromised card data onto Android phones in order to make payments at any stores accepting NFC payments.*[35]

Apple attaches the same Europol report to its submission dated 26 October 2016, along with a news report that notes that "police are unsure exactly how the attacks are being carried out and how common they are" and quotes a member of the European Cybercrime Centre's academic advisory board who describes the evidence of these attacks as "anecdotal".[36]

In these circumstances it is difficult to determine the relationship between these fraudulent transactions and the provision of access to the NFC function. It appears that this report describes the on-boarding of illegally or fraudulently obtained card details onto an NFC-enabled mobile phone. However, this kind of fraud does not depend on open access to the NFC function.

For example, early versions of the Android operating system allowed NFC card emulation only for Google Wallet – a precursor to Android Pay – and did not provide a public API for other developers. However, unofficial modifications of the Android operating system emerged that allowed other developers to use the NFC card emulation function even though it was not available under the official operating system.[37]

This kind of fraud is also possible where NFC access remains both officially and unofficially closed. For example, soon after the launch of Apple Pay it was widely reported that organised crime groups were loading fraudulently obtained card details into Apple Pay and using them to purchase high-value items from stores that accepted NFC payments – with some issuers reporting that up to 6% of Apple Pay transactions were affected by this kind of fraud.[38]

[33] Samsung FAQs, 7 August 2016, available at http://security.samsungmobile.com/doc/Press_Guidance_Samsung_Pay.pdf (accessed 28 October 2016).

[34] John Montagu Submission, 18 October 2016.

[35] Europol, *Internet Organised Crime Threat Assessment 2016* at p 30.

[36] Leo Kelion, *BBC News,* "Europol warns of Android tap-and-go thefts", 28 September 2016.

[37] Sarah Clark, *NFCWorld,* "SimplyTapp proposes secure elements in the cloud," 19 September 2012, available at http://www.nfcworld.com/2012/09/19/317966/simplytapp-proposes-secure-elements-in-the-cloud/ (accessed 28 October 2016).

[38] Daisuke Wakabayashi, *Wall Street Journal,* "Fraud Comes to Apple Pay", 3 March 2015, available at http://blogs.wsj.com/digits/2015/03/03/fraud-comes-to-apple-pay/ (accessed 28 October 2016).

Even where the on-boarding process is improved by mandatory two-factor authentication, it is still possible to load fraudulently acquired card details into any mobile wallet through social engineering – for example, by calling a call centre and persuading an operator to verify a card by answering security questions with the help of Google searches – or by automatically trying all of the 1000 possible three-digit verification numbers.[39]

In these circumstances, although Europol report refers specifically to Android phones, it is unclear that the *provision of access to the NFC function* on Android devices itself plays any significant role in this fraud. It is even less clear that the provision of access to the iPhone's NFC function would raise these issues, given the other safeguards available to the Apple ecosystem, particularly Apple's control over the applications that can be installed on the iPhone, the secrecy surrounding Apple's source code (compared to Android's source code, which is publicly available) and the greater difficulty in modifying the operating system of the iPhone compared to Android devices.

(d) None of these cases affect the security of NFC mobile wallets

Critically, all of the exploits referred to in submissions take advantage of older and less secure payment methods such as magnetic stripe technology, or card numbers and expiry dates stored "in the clear" on merchant servers where they can be stolen. Even EMV (or "chip-and-pin") contactless cards are vulnerable where they provide a less secure "fall back" option for older merchant terminals, and they are often required to do so.

By contrast, the applicants are not aware of any report that the payment methods used by NFC mobile wallets have been compromised on any platform. That is, if an authentic card is added to an NFC mobile wallet with security features that may include a hardware secure element, tokenised credentials and strong encryption, a secure customer verification method such as a long PIN or fingerprint verification, and a dynamic cryptogram generated for each transaction, it does not appear to have been demonstrated even in a controlled environment that these credentials can be stolen and used for fraudulent transactions.

This appears to be the case for NFC payments made using Apple Pay, Android Pay, Samsung Pay and the many payment applications on the Android platform using either an embedded or SIM-based secure element or software host card emulation – all of which have been endorsed as secure by the card schemes.

It certainly appears to be the case whether or not the operating system provides access to the NFC function to competitive payment applications, and no argument has been advanced to explain why providing such access should threaten the security of an authentic user's payment credentials stored in this way.

(e) Comparisons between host card emulation and secure elements are not relevant

Apple's submission dated 26 October 2016 says that:

> *Apple designed Apple Pay so that the most sensitive payment information was located in the secure element, which is a tamper resistant hardened module within each device. On other platforms like Android, which permit direct access to the NFC radio, payment credentials are stored in the cloud using host card emulation (**HCE**), which is widely seen as a less secure security method prone to outside attack.*[40]

While Apple provides a number of articles or reports that examine the relative security of HCE and secure element solutions, it is not the case that HCE implementations are widely seen as materially less secure than implementations using a secure element. Perhaps the most authoritative of the

[39] Thomas Fox-Brewster, *Forbes*, "Here's proof Apple Pay is useful for stealing people's money", 1 March 2016, available at http://www.forbes.com/sites/thomasbrewster/2016/03/01/apple-pay-fraud-test/ (accessed 28 October 2016).

[40] At p 4.

sources cited by Apple, the Federal Reserve Bank of Boston, suggests that HCE is sufficiently secure where it uses tokenisation, as all modern implementations do.[41] HCE is subject to EMV standards, and HCE solutions have been certified by Visa, MasterCard and the other card schemes as secure.

It is also not true that platforms that provide access to the NFC function necessarily use or require the use of HCE. Many Android devices, particularly the most popular Samsung models, include embedded secure elements much like the iPhone's, and third party applications can store card information securely on those secure elements – as Westpac currently does with its Android application for Samsung phones. A number of BlackBerry devices also have embedded secure elements and provide access to authorised applications to use them for NFC payments.

The Android platform also allows access to secure elements embedded in SIM cards, as used by Cash by Optus and by many Android wallets overseas. The BlackBerry and Windows platforms also allow access to SIM-based secure elements.

If NFC access to the iPhone's NFC were available, then NFC apps could potentially make use of HCE, of secure elements on SIM card, or of the iPhone's embedded secure element. This would be a matter of the issuer's preference and of commercial negotiation with Apple. If Apple is concerned about the security of HCE solutions, it can provide access to the iPhone's secure element – as is provided on other platforms. If it is concerned about other applications accessing the iPhone's secure element, it can require issuers to demonstrate that their solutions meet industry standards of security.

Under any secure element implementation, it should be impossible for an application on the secure element to access any other application's data, and the applicants would expect that Apple's implementation would make sure that this is the case.

(f) NFC access does not raise particular security concerns

Mobile phone users use their devices to store and communicate a wealth of valuable information which has the potential to cause immense financial and personal damage if compromised or exploited. Payments and transfers can be initiated through web browsers, e-mails, text messages, Bluetooth connections, QR codes and mobile banking apps. These payments may be of significant value and may not always be recoverable in the case of fraud.

By contrast, NFC payments are typically low-value payments that are already highly secure and are in almost all cases recoverable in the case of fraud. It is not clear that these payments present a unique security concern such that access to the NFC function should be denied to other developers – particularly where there is no evidence that such access would compromise security, and no such restriction applies to other functions that can have far more serious consequences if compromised.

Apple has not provided any credible argument to the applicants that granting access to the iPhone's NFC function would present a particular threat to the security of iPhone payments or any plausible harm to iPhone users. If it has provided any such argument to the ACCC on a confidential basis, the applicants urge the ACCC to test this argument with an independent technical and security expert. Otherwise, the only conclusion to be drawn is that Apple is refusing to provide access to the NFC function in order to prevent competition with Apple Pay and avoid any downward pressure on the supra-competitive fees it can charge for Apple Pay.

10 Recent submissions do not alter the view that NFC function access will not compromise user experience

Apple's submission dated 26 October 2016 asserts that providing access to the NFC function would "fundamentally break the simplicity and ease of use of the Apple Wallet app", including because it

[41] Susan Pandy and Marianne Crowe, Federal Reserve Bank of Boston, Payment Strategies and Brian Russell, Giesecke & Devrient, "Understanding the Role of Host Card Emulation in Mobile Wallets", 10 May 2016.

would require a user to go into the device settings every time they wanted to change the application associated with the NFC radio:

> *This simple user experience is critical for consumers and any friction in that process inhibits consumer adoption, particularly given the fact that Apple Pay is new and consumers are only now starting to use their Apple devices, instead of their physical cards, to perform these tasks*.[42]

The applicants agree that a simple user experience is critical and any friction can inhibit consumer adoption – that is precisely the reason why non-integrated workarounds such as NFC stickers, and the partial integration of banking apps with Apple Pay, cannot substitute for integrated NFC access.

However, given Apple's control of the iPhone's hardware and operating system, the applicants would be surprised if Apple could not provide a more elegant and user-friendly governance mechanism than it describes here. For example, a potential governance mechanism might broadly provide that:

- if the user has an NFC application open when the iPhone is presented to an NFC terminal, then that application will be used to make the payment; and
- if the user does *not* have an NFC application open when the iPhone is presented to an NFC terminal, then:
    - if the user has specified a default NFC application in the user settings, that application will be used to make the payment; and
    - if the user has not specified a default NFC application, Apple Pay will be used to make the payment.

The applicants further understand that is possible to associate different applications with different NFC functions such as payments, loyalty cards, public transport or building access, so that a different application is invoked and/or a different card presented depending on whether the mobile phone is held to a merchant terminal, a public transport terminal, or another device. The applicants are confident that Apple could use this information in its governance mechanism to provide a simple and elegant user experience that also provides choice and responds to the preferences of different users.

Crucially, the applicants expect that unless the customer exercises a positive choice, their experience will be exactly the same as at present; that is, Apple Pay will be the only NFC payment application and will operate exactly as it does today.

11 The resources required to provide NFC access would not be significant

Apple argues that it is unlikely that it would "commit significant effort, resources, and funding to build and make available to four banks in Australia". While the applicants acknowledge that there will be some resources required to provide NFC access, it is not clear that these would be significant.

The applicants understand that Apple has already developed a private application programming interface for its own use of the NFC function, which overlays the interface provided by the manufacturers of its NFC controllers. It would not be a significant undertaking to make public, and to document, certain elements of that programming interface for other applications to use.

Apple would have to develop a governance mechanism to coordinate multiple applications seeking to use the NFC function, but such a governance mechanism need not be complex, and similar mechanisms have already been developed for other platforms.

[42] At p 6.

Apple expends substantial resources continually updating its iOS operating system, releasing a major version update and a number of “point” updates each year. The applicants would expect that providing access to the NFC function would be a relatively minor task compared to other updates. And the applicants would not be collectively negotiating on the basis that Apple will provide this access for free, but only on reasonable terms subject to individual negotiation.

The applicants would also hope that access to the NFC function would not be limited to themselves but could be made available more broadly – beyond the applicants and the collective bargaining group to retailers, technology startups, transport operators, government services and others – to increase customer choice and innovation and, ultimately, the value of the iPhone platform to customers. However, that is of course a matter for Apple.

12 There may not be a better opportunity to address public detriments associated with not having access to the iPhone NFC functionality

Issuers are under pressure to participate in Apple Pay on sub-optimal and inefficient terms to avoid losing customers to competitors who offer Apple Pay. The authorisation allows an improved balancing in relative bargaining positions and a real chance of better outcomes and public benefits for Australians. These are precisely the circumstances where collective negotiation is necessary to avoid public detriments and achieve fair and efficient outcomes, and where collective boycott is required to bring the other party to the negotiating table.

The limited nature and framework for the collective negotiation minimises any potential detriments that may be expected from collective arrangements, including minimal risk of delay. Once a critical mass of issuers have agreed to Apple’s “take it or leave it” terms and conditions, there may not be another comparable opportunity to achieve the more optimal outcomes of choice and enhanced competition, which would place pressure on Apple to provide better price and quality offerings. Further, without access to the iPhone’s NFC functionality there simply will not be the same incentives and ability to innovate for the benefit of Australian customers on either the iPhone platform or other platforms.