Re Authorisation Applications A91546 & A91547

Submission by David Thornton

1. Introduction

Bendigo and Adelaide Bank, Commonwealth Bank of Australia, National Australia Bank and Westpac Banking Corporation (the applicant banks) seek to enter into an agreement between themselves and any other card issuers that would otherwise contravene the prohibition on cartel provisions under the *Competition and Consumer Act 2010*.

The Australian Competition and Consumer Commission (the Commission) is bound by s 90(5A)[1] to not grant authorisation for such an agreement to be made unless it would result in a benefit to the public, and such benefit would outweigh the detriment to the public caused by any lessening of competition that would result from the agreement.

However, there is a dearth of substance to support the applicant banks' proposed public benefits flowing from any authorised collective negotiation or boycott. Where the applicant banks have sought to characterise their application as one that promotes "competition, security and transparency",[2] the practical effect of their application, if granted, will be the strengthening of the Australian banking cartel, maintenance of the status quo in relation to fraud and public data security standards; and, the imposition of further costs and fees upon Australian consumers of banking services in the resultant vacuum of competition.

It is emphatically the opinion of this submission that the application should be rejected.

2. Future with and without

Following *Re VFF Chicken*,[3] the statutory test contained in 90(5A) requires the Commissioner to apply the "future with and without" test, which involves comparing the case where collective negotiations have been authorised (the factual) with the case where they have not (the counterfactual). In comparing these two cases, the Commissioner is required to look at the difference between likely market outcomes and make a determination whether authorisation would tend to reduce market inefficiencies or increase them. The Tribunal in *Re VFF Chicken* held that inefficiencies of particular salience in assessing an application were a) productive inefficiencies, b) allocative inefficiencies and c) dynamic inefficiencies.[4]

In the counterfactual, allocative and dynamic market efficiency will quickly converge upon their rightful maximum because the current market is perfectly poised to herald the introduction of Credit Card Tokenisation processes (CCT processes, or simply Tokenisation) in Australia. While this does require issuing banks (including the applicant banks) to innovate and invest in the technologically advanced method of CCT — it maximises the rightful benefits to society that include the reduction of credit card fraud borne by the general public in their capacity as consumers requiring payment solutions.

---

[1] *Competition and Consumer Act 2010* (Cth).

[2] Application for authorisation of limited collective negotiation in relation to mobile wallet and mobile payment systems, 25 July 2016, Page 1.

[3] *Re VFF Chicken Meat Growers' Boycott Application* [2006] ACompT 2.

[4] Ibid, [74]—[82].

If the authorisations are granted, allocative and dynamic market efficiency will be lost as the applicant banks are no longer compelled by market forces to invest or innovate in technology that serves the overall public good, because they need not concern themselves that other members of the negotiation cartel will break ranks and succumb to market pressures by adopting CCT processes to protect consumer transactions.

3. Public benefits and detriments examined

The benefits purportedly offered to the public by the applicant banks are notionally referred to as increased competition, and compliance with industry best practice principles.

3.1. Illusory increase in competition where products not fungible

The applicant banks seek to characterise their mobile payment solution as a promoter of competition in the “Mobile Wallet” market. However, to the extent that the banks have applied to negotiate on the requirement of CCT processes, they lose the property of fungibility with Apple’s product.

The effect this will have on the public will be dramatic: in the factual case where the applicant banks are authorised to negotiate as a cartel with respect to security standards, and where they are successful in offering such products without the requirement of CCT, the applicant banks will essentially be permitted to “ride on the coattails” of Apple Pay.

This is because the applicant banks’ mobile payment cards will be able to look and appear to operate in exactly the same way as Apple Pay. This could include the requirement of a CVM (customer verification method) via the Touch ID fingerprint sensor which is a flagship feature of Apple Pay from the perspective of the consumer. The only difference will be that data is transmitted in the same insecure fashion as a physical contactless credit card, and bear the same risks to consumers of credit card fraud.

Apple has made and delivered upon claims in respect of the security of Apple Pay, which which will not be delivered upon by the applicant banks “Mobile Wallet” apps notwithstanding apparent countenancing from Apple by inclusion on their App Store. The practical effect of this will be that consumers of the applicant banks’ apps are at best ill-informed and at worst mislead — but still just as vulnerable to credit card fraud.

3.1.(a) Potential for innovation not realised

The applicant banks submit that they should be authorised to negotiate collectively in order to bring about innovation in the electronic payments market. However, even where an adverse third party is not involved in negotiations to achieve innovation, the applicant banks have a history of reticence.

If the applicant banks could demonstrate their willingness to innovate unilaterally, without coercion or force from third parties, the premise of their argument that collective negotiations would serve the public benefit by promoting innovation would carry some weight. However, in the case of the New Payments Platform (NPP), the Governor of the Reserve Bank of Australia was required to threaten “regulatory” action if the financial services sector failed to innovate:

> The governor of the Reserve Bank has given a pep-talk, wrapped in a warning, to Australia's biggest banks, saying they need to keep working together to deliver on their commitment to provide real-time

> payments to their customers – otherwise the RBA will be "duty bound" to consider making it happen.[5]

Even though the Governor appealed to the financial services sector on behalf of the public good, stating that:

> "The biggest risk with this project is probably not a technical one. It is the risk that, in 10 or 15 years' time, we will look back and see that we missed an opportunity to provide something that will fully and efficiently support the payments needs of our economy. We owe our citizens a better outcome than that".[6]

This did not dissuade the financial services sector from announcing

> The nation's new nervous system for electronic payments will be delayed by a year after five institutions stepped back from funding the $1 billion project… Westpac was the last of the big banks to sign up [taking] about three months longer to agree to the contract [than the other big banks].[7]

This delay was caused just two months after the initial warning issued by the RBA, and serves as an ominous example of the applicant banks' willingness to engage in anti-competitive behaviour, where competition and innovation would otherwise serve not just a public interest — but even the banks' own interest:

> the big banks need to remember they will benefit from new infrastructure, despite the fact that it will allow new competitors to enter the market.[8]

In light of this, the applicant banks' argument in favour of innovation through collective negotiation and collective boycott becomes untenable.

3.2. Ostensible "best practice industry standards"

The applicant banks have sought to rely on subterfuge and misconstruction of the facts in asserting that a grant of authorisation to negotiate collectively, would promote "best practice standards".

It has become a matter of public record that Apple requires partner banks (issuing banks) both domestically and internationally, to conform to *global* best practices in fraud prevention and consumer data security protection that have been developed by EMVCo.[9]

However, in order to avoid the costs of "acquiring particular tokenisation services from the card schemes",[10] the applicant banks have engaged in the most egregious subterfuge and misconstruction of the facts in order to assert that their collective negotiation would:

---

[5] http://www.smh.com.au/business/banking-and-finance/rba-tells-banks-to-build-new-payments-system--or-we-will-make-you-20141023-11ag03.html

[6] Ibid.

[7] http://www.smh.com.au/business/banking-and-finance/payment-systems-1-billion-overhaul-delayed-a-year-20141202-11yfoi.html

[8] Above n 5.

[9] EMVCo Payment Tokenisation Specification Technical Framework v1.0 (See: https://www.emvco.com/specifications.aspx?id=263)

[10] Above n 2, Page 10.

> "[promote] best practice industry standards and guidelines for mobile wallet security and related issues, such as the APCA Third Party Digital Wallet Security Guidelines".[11]

In fact, this is patently false. The applicant banks have a direct interest in promoting and complying with the APCA Third Party Digital Wallet Security Guidelines (the APCA Guidelines), but they in no way represent best practice standards of the industry.

The APCA Guidelines were first published 24 May 2016, or at approximately the time that negotiations with Apple for the introduction of Apple Pay broke down. The guidelines state that although the minimum standards of a Tokenisation Service Provider (TSP) must meet the EMVCo's Payment Tokenisation Specification — Technical framework version 1.0, in respect of the actual use of card tokenisation services:

> "Tokenisation is not compulsory for transactions made using a Third Party Digital Wallet if the Third Party Digital Wallet includes an embedded secure element solution".[12]

Interestingly, although 18 terms are defined for a mere three pages of industry best practices guidelines (c.f. 39 terms in EMVCo's 84 page specification) — the APCA Guidelines define "Card" but not "secure element" or "embedded secure element solution".

Beginning with the iPhone 5S, and unique to Apple's iPhone range of smartphones, Apple has included a particular type of co-processor referred to as the "secure enclave".[13] This co-processor is responsible for storing certain highly sensitive customer information such as an iPhone user's fingerprint or their (tokenised) credit card number.[14]

The problem with the APCA Guidelines is that the mere presence of a "secure element" will not alleviate the risk of fraud present when credit card tokenisation is not used.

In order to fully understand this, it is necessary to examine the differences between a standard credit card transaction, a tokenised credit card transaction and a tokenised credit card transaction performed on an iPhone making use of its secure enclave.

3.2.1. Typical credit card transactions compared

Modern credit card transaction, although instant and ubiquitous, involve global cooperation of banking and financial services companies in a complex set of relationships. The parties commonly involved will be enumerated here for further clarity.

Party	Description	Examples
Card Issuer / Issuing Bank	Cardholder's bank	ANZ, Amex, etc.

---

[11] Above n 2, Page 1.

[12] APCA Guidelines, 2.1(a) (http://www.apca.com.au/docs/default-source/guidelines/third_party_digital_wallet_security_industry_guidelines.pdf)

[13] https://www.apple.com/business/docs/iOS_Security_Guide.pdf see page 5. A7 Processors first appeared in the iPhone 5S.

[14] In order to conform to or exceed EMVCo's technical specification for credit card security, Apple stores a "Device Account Number" instead of the users' actual credit card number.

Card Acquirer / Merchant Bank	Best Burrito Company's bank	CBA, Westpac, ANZ, etc.
Card Scheme / Card Network	The ultimate transaction facilitator	VISA, Amex, MasterCard
Tokenisation Service Provider	Service responsible for exchanging credit card tokens for actual credit card numbers	VISA, MasterCard
Merchant	The vendor supplying the goods or services	Best Burrito Company, etc.
Cardholder	The consumer making the purchase	The general public

3.2.1.(a) Regular "insecure" credit card transaction

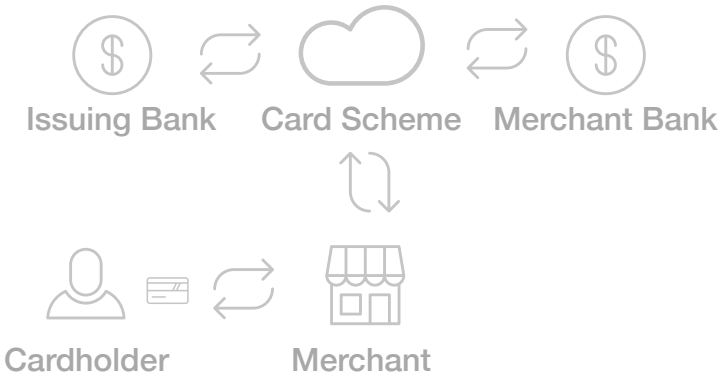

Figure 1. How a standard credit card transaction is processed

Regular credit card transactions begin with the Cardholder presenting the Card to the terminal located at the Merchant. The merchant terminal gathers the credit card number, which consists of a first digit to identify the Card Scheme, and then the Bank Identification Number (BIN) which tells the Card Scheme at which bank the account of the Cardholder exists. The final digits after the BIN allow the Card Scheme to communicate with the issuing bank to identify the account from which it will authorise payment. The merchant also sends the Card Scheme information about its own banking details. For example if a credit card number is:

3123 4567 8987 6543

Number	Denotation	Entity
3	Card Scheme	American Express
12345	BIN (Bank Identification Number)	An Australian Bank
6789876543	PAN (Personal Account Number)	Consumer's Bank Account ID

The problem with this type of transaction is that fraud can be committed when the credit card number is obtained by presenting a copy of the card number at another merchant. This can be

achieved inexpensively through various methods,[15] and costed Australia $460M in the 2015 calendar year.[16]

This problem is almost wholly alleviated by the process of tokenisation.

3.2.1.(b) Tokenised credit card transaction

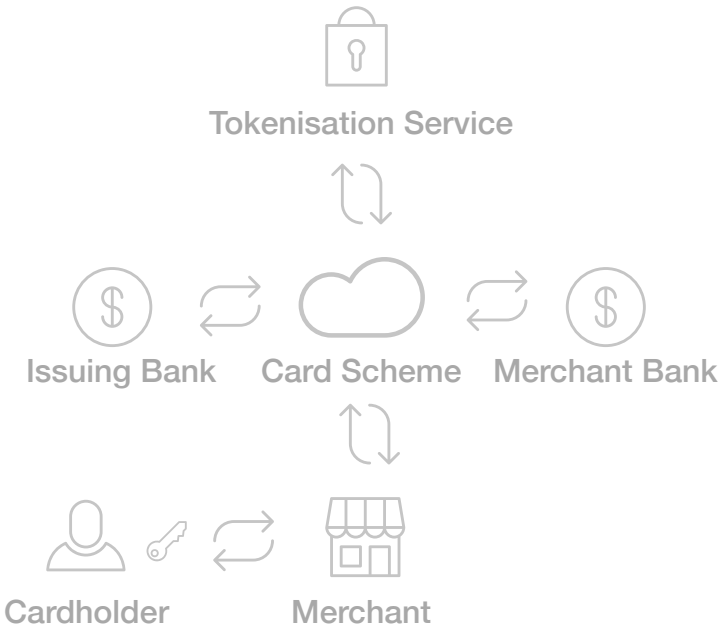

Figure 2. How a tokenised credit card transaction is processed

Tokenisation works by storing true credit card numbers in a Token Vault, and issuing cardholders (directly) a key or “token”. The transaction accrues the additional requirement of translating the token to a true credit card number after the Cardholder presents the tokenised card to the merchant terminal at the Merchant and before the transaction can proceed.

To stop adversaries simply copying the token from the Cardholder or at the Merchant, and “replaying” it at another Merchant, the TSP and the Cardholder agree on a shared secret which can be generated by the Cardholder and verified by the TSP (called a transaction cryptogram).

The token by itself is not enough information for a Card Scheme to find the Cardholder’s financial institution from the BIN or bank account from the PAN, so it is practically useless before it has been exchanged by the TSP for an actual credit card number. Before the TSP exchanges the token for the true credit card number, it checks the validity of the cryptogram and, if valid, returns to the Card Scheme (not the Cardholder or Merchant) the true credit card number, allowing it to continue settling the transaction with the Merchant Bank in the same way as a standard credit card transaction.

With respect to fraud risks, banks, card schemes and TSPs are considered ‘trusted’ parties, while Cardholders and Merchants are ‘untrusted’ because they cannot be assumed to keep the Cardholder’s true credit card numbers secret from adversaries.

---

[15] See ASIC’s moneysmart factsheet: https://www.moneysmart.gov.au/scams/banking-and-credit-card-scams/credit-card-scams#scams

[16] http://www.apca.com.au/payment-statistics/fraud-statistics/2015-calendar-year

This system of tokenisation is far superior to non-tokenised credit card transactions because the true credit card number is never revealed by the Cardholder to the Merchant where fraud takes place in practice.

However, the system is not perfect: there exists the risk that an adversary will be able to ascertain not just what the Cardholder's token is, but also *how* the cryptogram is generated — allowing that adversary to generate new cryptograms to exchange the leaked token for a true credit card number at a Merchant and fraudulently execute transactions on the Cardholder's behalf.

3.2.1.(c) Apple Pay transactions

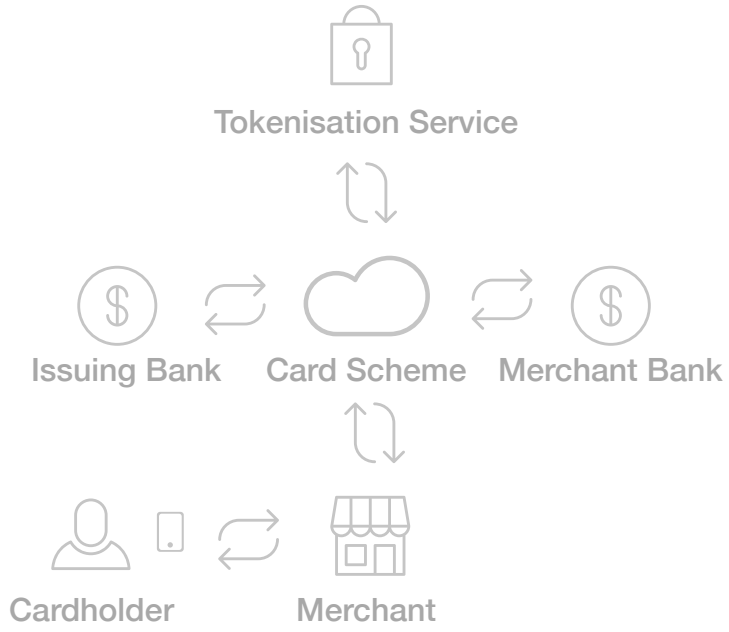

Figure 3. An Apple Pay transaction

This is where Apple Pay comes into its own. Apple Pay uses the secure enclave to store the token, *and* generate the cryptogram. Hived off from the rest of the iPhone, this secure enclave will never yield its contents or generate cryptograms *unless* a valid fingerprint has been registered against the iPhone's fingerprint reader, and is one of the most uncompromisable systems currently in existence in the world.[17]

Thus, by supplying a way of *securely* storing the token and generating the cryptograms, Apple has created a way to finance transactions with an exceedingly negligible risk of fraud.

3.2.1.(d) Conclusion in respect of APCA Guidelines

It can thus be seen that the mere "inclusion" of a secure element in a smartphone, does not alleviate the need for tokenisation to reduce fraud, nor achieve industry best practices.

---

[17] *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*

Therefore; while the APCA Guidelines do set out an industry standard, it is by no means the best practice industry standard. Moreover, this standard is self-serving at the cost of the Australian consumer for the benefit of the applicant banks.

Additionally, as the APCA Guidelines demonstrably do not reduce fraud below the levels currently experienced through non-tokenised physical credit card transactions, any submissions to the contrary are misrepresentative of the underlying technical facts.

If the applicant banks are allowed to collectively negotiate with Apple on data security standards, and they succeed, the public interest in avoiding credit card fraud will be subverted in favour of the applicant banks cost-cutting and status quo maintenance measures.

3.2.1.(e) ID&V and onboarding fraud

ID&V fraud is largely an artefact of the past. Although the *New York Times* article was published in March 2015, it serves as a case study for what a properly competitive environment can achieve: in the United States where ID&V fraud was initially a problem, the issuing banks and Apple were able to both identify a problem in the market (inefficient ID&V caused by lack of information sharing between issuing banks and Apple) and work together to solve the problem for the benefit of the market and the public interest — exemplifying how a properly competitive banking sector works together with its stakeholders to achieve a public benefit.

Any further regulatory fetter upon the market that already suffocates innovation and competition in the Australian banking sector would not yield the same outcome in Australia as occurred in the United States, and it is for this reason that ID&V fraud cannot be a ground upon which the authorisation is granted.

3.2.2. Independence of APCA questionable

Of APCA board members, all of the big four banks have an appointee,[18] including three out of the four banks in this applicant. The public interest in reducing credit card fraud is not likely to be served well where the applicant banks can exert the level of political pressure on a body charged with the responsibility for creating credible industry best practice standards as they currently do.

3.2.3. Consumers bear ultimate liability for unreported fraud

In Australia, there is an increasing pressure for the Australian public to migrate to credit card services as cash or cheque transactions become increasing infeasible. Credit card fraud impacts the public interest negatively by dishonestly transferring wealth across a society where the afflicted Cardholder is not at fault, has taken, nor is able to take any action.

Credit card fraud risks are controlled in the case of physical credit cards at two levels. The first level of protection is at the the issuing bank: an issuing bank that receives the authorisation request for a transaction can choose to selectively honour transactions against an account that would otherwise have sufficient funds to settle that transaction. This is desirable when an adversary obtains the credit card numbers of many cards, and attempts to submit transactions to issuing banks. In this case, an issuing bank may be able to conclude that some of these transaction are fraudulent. For example, if the transaction was submitted as a “card present” transaction in California at what would be the early hours of the morning in Sydney, and the issuing

---

[18] http://www.apca.com.au/about-apca/how-we-work/apca-board

bank knows that the consumer is not currently overseas, it can reject proactively the transaction to avoid fraud.

This type of fraud protection is what Apple's submission refers to as "the cure".[19] It is necessarily worse than "prevention" because it operates on a statistical basis, which is imperfect: if the adversary was able to time the transaction while the Cardholder was on holidays in San Francisco, the issuing bank would not be able to detect this unauthorised transaction.

Thus, while the Australian Bankers' Association Code of Banking Practice 2013 affords Australian banking customers the right to "chargeback"[20] a transaction, this effectively transfers the burden of detection onto the consumer whose credit card number is valid for a number of years, and hence vulnerable to *bank-undetected* fraud for that period of time. Tokenisation creates transaction-specific credit card numbers valid for periods of seconds, limiting the same vulnerability to prohibitively short timescales for credit card fraud.

4. Conclusion

The applicant banks have track record of resisting innovation, even where the benefits to themselves are great, such as is the case with the New Payments Platform. Where Apple Pay has been introduced, consumer demand has injected renewed efficiency into the market. To the extent that this trend continues, the market forces should be allowed to prevail unimpeded by the applicant banks.

Additionally, where the applicant banks have sought to use subterfuge and misconstruction of the technical factual matrix in relation to the status of tokenisation as industry best practices, they should attract censure — not authorisation to collude as a means of magnifying their bargaining power and obtaining the benefit of more desirable market conditions on their own behalf.

Thus it is of the utmost importance to the Australian public interest that the application for authorisation made under s 88 of the *Competition and Consumer Act 2010* on behalf of the applicant banks be rejected. Upon consideration of the factual with the counterfactual, it is clear that the future without authorisation will lead to a market with high allocative and dynamic efficiencies by operation of market forces themselves, while the counterfactual will simply lead to the converse.

---

[19] Authorisation applications A91546 & A91547 Submission by Apple, 26 August 2016, Page 12 [4.3].

[20] http://www.bankers.asn.au/Industry-Standards/ABAs-Code-of-Banking-Practice/Code-of-Banking-Practice-2013---Online-Version#1e22