Our ref: PJA\AJT\02 1383 8501
Your ref: 51693
Partner: Peter Armitage
Direct line: +61 2 9258 6119
Email: peter.armitage@ashurst.com

Ashurst Australia
Level 36, Grosvenor Place
225 George Street
Sydney NSW 2000
Australia

GPO Box 9938
Sydney NSW 2001
Australia

Tel +61 2 9258 6000
Fax +61 2 9258 6999
DX 388 Sydney
www.ashurst.com

13 August 2013

BY EMAIL

PUBLIC REGISTER VERSION

Ms Hayley Parkes & Ms Marie Dalins
Assistant Director / Director
Australian Competition & Consumer Commission

Dear Ms Parkes and Ms Dalins

Authorisations A91379 & A91380

We refer to your letter of 30 July 2013 seeking further information from the Applicants in relation to the above authorisation applications.

The purpose of this letter is to provide the information requested by the ACCC.

Please note that this letter contains information which is confidential to the Applicants. The confidential information is marked with square brackets and the text "CONFIDENTIAL TO [VISA / MASTERCARD] as appropriate. A non-confidential version of this letter will be provided to the ACCC for placing on its public register.

In the remainder of this letter we have adopted the ACCC's numbering in its letter of 30 July 2013.

1. **A COPY OF THE MANDATE ISSUED BY VISA ON 28 FEBRUARY 2013, OR ANY UPDATED MANDATE**

Please see:

- Annexure A: Visa Business News dated 28 February 2013- announces updates to PIN requirements in Australia; and
- Annexure B: extract from Visa International Operation Regulations-indicates rules that were amended to reflect updates to PIN requirements outlined in Annexure A.

These documents are **CONFIDENTIAL TO VISA**. Visa requests that the ACCC treat these documents as confidential and not place them on its public register or provide them to MasterCard.

2. **INFORMATION ON THE TECHNOLOGY UPDATES REQUIRED TO SUPPORT MANDATORY PIN@POS & WHETHER THESE WOULD ALTER THE PROCESSES AND PROMPTS FOR OTHER CREDIT CARDS**

What is in place today

Optional PIN was introduced by Visa, MasterCard, American Express and Diners in Australia in 2008. In Australia today, acquirers (through their terminals) and issuers currently support both signature and PIN as cardholder verification methods (**CVM**).

CVM currently takes place in the following ways:

(a) customer swipes their card (older terminal technology) and either signs or enters a PIN;

(b) in the case of a newer terminal, customer inserts their chip card and signs or enters a PIN or, for lower value transactions not requiring PIN or signature, holds their chip card near a contactless reader.

Terminals which support the chip card verification methods in (b) are known as "EMV compliant". EMV stands for Europay, MasterCard, Visa, and is a global payment industry standard for interoperability between chip cards and terminals to enable payment. It is important to note that EMV compliant terminals still allow non-chip cards to be swiped, but chip cards must be inserted or held to the reader.

The roll out of EMV compliant technology has been taking place for some time by acquirers, but some terminals have not yet been upgraded.

In time for the PIN@POS requirements in March 2014, all terminals where the acquirer is a member of either Visa or MasterCard[1] will be upgraded to enable chip cards to be processed as described in (b) above, making the terminal EMV compliant. (The process in (a) will still be available for non-chip cards on upgraded terminals).

"EMV compliance" deals with chip card processing, but does not specify how verification of chip transactions must take place (ie, PIN or signature). As a result, **EMV compliant terminals currently allow PIN entry to be by-passed**, which means that the cardholder can provide a signature instead of a PIN, even though the PIN is the preferred CVM on the card. **This will change with the introduction of mandatory PIN@POS**. Mandatory PIN@POS will require a PIN to be entered in domestic POS chip transactions on MasterCard and Visa cards.

Mandatory PIN@POS will build upon the security of EMV by enforcing PIN on chip transactions thereby reducing fraud by preventing fraudulent POS transactions verified with signature (e.g. lost and stolen cards).[2] Non-chip transactions will continue to be verified as described in (a) above, even on upgraded EMV compliant terminals.

What changes are necessary during the period of joint advertising of voluntary PIN@POS?

Assuming the period of joint advertising of voluntary PIN@POS is from approximately now through to March 2014, there are no changes to terminals or the issuer host for PIN@POS during this period.

The 'period of joint advertising' represents a time when issuers and acquirers will plan and budget for and test what is required to implement mandatory PIN@POS. This planning phase includes scoping the changes, forecasting costs, securing the funds internally, testing then executing the changes. The time it takes for this planning and testing varies between financial institutions.

There will be no changes made to the terminals or to the issuer host, until mandatory PIN@POS takes effect (either jointly through authorisation, or individually).

What changes are necessary for the introduction of mandatory PIN@POS?

The changes that are required on both sides (ie, terminals and issuer hosts) are to prevent Visa and MasterCard domestic POS chip transactions from occurring without a PIN. Changes will be made to prevent this at terminal level, but also at issuer host level.

---

1 Assuming authorisation is received

2 The mandatory PIN@POS changes will not require any amendment to the EMV standard.

Terminal changes would be conducted by the acquirer and or their terminal vendors (which may be between one and many parties) and the issuer host changes would be conducted by the issuer or the issuer's processor (such as First Data).

Terminal changes

As described above, the roll-out of chip-reading technology in terminals is taking place independently of mandatory PIN@POS. Visa estimates approximately 95% of terminals now accept chip transactions.

The introduction of mandatory PIN@POS will mean further changes to the already EMV-compliant terminals, to remove the option of signature for chip-initiated transactions.

At the terminal, the screen prompt will be changed when a PIN is required (ie, in chip transactions) to read "Enter PIN" instead of "Enter PIN or OK" (**Terminal Changes**). In this way, the terminal will be changed to prohibit a Visa or MasterCard domestic chip transaction that does not contain a PIN.

Acquirers will be able to make the Terminal Changes to some terminals remotely, such that on March 17th, 2014 the Terminal Changes will be implemented with immediate effect. The financial institutions forecast that 40-55% of all terminals will be changed remotely in this way on March 17th, 2014.

The remaining 60-45% of terminals will be upgraded by swapping them out for terminals that already have the Terminal Changes made to them over the 12-24 months following March 2014. The swap out of terminals will mean a large investment by acquirers and should Visa and MasterCard not implement PIN@POS at the same time but one after the other, the swap out would need to be repeated for those terminals that cannot be updated remotely.

Cardholders will be notified, through joint public marketing communications (if authorised), that Visa or MasterCard domestic chip transactions that do not contain a PIN will be declined at POS terminals from 17 March 2014 onwards.

Issuer host changes

The term issuer host in this context is the system by which an issuer receives transactions from the cards that they issue. The issuer host therefore receives all scheme and EFTPOS cards that are issued by that financial institution. The changes to the issuer host would involve declining all Visa and MasterCard domestic chip transactions that do not contain a PIN. In response to a Visa or MasterCard domestic chip transaction that does not contain a PIN, the issuer host will send a message back to the terminal that reads "DECLINED".

The issuer host changes will all be made on one day, 30 June 2014, without exception[3]. This will mean that all Visa and MasterCard domestic POS chip transactions will be declined without a PIN from 30 June 2014 onward (regardless of whether the Terminal Changes have been made). These changes are effectively a "second line of defence" / best practice, to ensure maximum security for cardholders.

Visa and MasterCard intend that the Terminal Changes be implemented first and in significant numbers so that the terminal drives the transaction.

[3] Assuming authorisation is received

(a) Is the technology specific to Visa and MasterCard cards?

The technology updates to support mandatory PIN@POS (namely, to make the Terminal Changes and altering the response by issuer hosts for Visa and MasterCard cards[4]) will be specific to Visa and MasterCard, or any other participating card schemes.

The changes required for mandatory PIN@POS will not alter the prompts at the terminal or the response by the issuer host for other cards which are not from participating card schemes.

(b) What terminal prompts will be visible for cards which are not Visa or MasterCard?

Following the introduction of PIN@POS[5], there will be no changes to the terminal prompts for cards which are not Visa or MasterCard cards (unless they belong to schemes which are also participating).

3. COUNTERFACTUAL – MASTERCARD WOULD IMPLEMENT ITS MANDATE

(a) Evidence of the business rationale for MasterCard implementing mandatory PIN@POS following Visa (including any relevant supporting documents)

In the event that authorisation was not granted by the ACCC, MasterCard would issue its own mandate in relation to PIN@POS. We note that it is likely that any separate MasterCard mandate would be at a later date to the effective date of Visa's current mandate. In this regard, it was not submitted in the counterfactual that MasterCard would implement its mandate at a similar time and on similar terms.

The introduction of mandatory PIN@POS is expected to reduce fraud in card-present transactions at POS. MasterCard is supportive of mandatory PIN@POS and wishes to put this fraud-prevention measure in place for cardholders, as a matter of best practice.

The reason MasterCard has not done so to date and did not include mandatory PIN@POS in its 2011 Roadmap, is that it generally takes a consultative approach with regard to changes which affect its members. In 2011, its members were not supportive of the introduction of mandatory PIN@POS.

Since 2011, the position has changed and the appetite amongst MasterCard's member financial institutions to introduce PIN@POS has increased. MasterCard intends to change its approach to implementing mandatory PIN@POS, partly in response to this change by the financial institutions. In this regard, MasterCard expects that with Visa mandating PIN@POS MasterCard's members will seek to have MasterCard also mandate PIN@POS to ensure a consistent cardholder experience across the card schemes.

In addition, MasterCard anticipates that in the event that it did not implement its PIN@POS mandate but Visa had done so, those perpetrating fraud on signature cards would shift their focus to MasterCard cards, with the result that fraud on MasterCard cards would increase. From a business perspective, it would be unacceptable for MasterCard to be in this position for any significant period.

Further, MasterCard would also look to mandate PIN@POS to avoid any consumer perception that its brand may be less secure than Visa.

---

4 Assuming authorisation is received

5 Assuming authorisation is received

(b) What are the specific costs that would be incurred by MasterCard if MasterCard was to separately implement mandatory PIN@POS?

There are two types of costs that would be incurred if MasterCard was to separately implement PIN@POS. They are: separate marketing costs and separate technology upgrade costs.

In relation to marketing costs, MasterCard would need to support on a stand-alone basis, and implement, its own marketing strategy and would lose the synergies created by combined industry messaging. The financial institutions would not be able to achieve the efficiency of a combined campaign and would need to incur marketing expenses twice. The estimated additional cost to the financial institutions for marketing of a separate MasterCard campaign in relation to PIN@POS may be in the order of $5M.

On top of this, significant costs would be incurred in order to perform a MasterCard-specific technology upgrade to the merchant terminal infrastructure and core credit card banking systems. This would involve acquirers and issuers implementing MasterCard-only changes of the nature set out above in response to question 2. For acquirers, this would involve a separate software upgrade (only in relation to MasterCard cards) and a hardware upgrade (ie, swapping out some terminals) again, only in relation to MasterCard cards. As these are costs that would be incurred primarily by the financial institutions implementing the changes, MasterCard is not able to provide an accurate estimate of these costs. However, MasterCard considers that the costs are likely to be at least $10 million across all the financial institutions that would need to implement these changes.

4. COUNTERFACTUAL – VISA WOULD STILL IMPLEMENT ITS MANDATE EFFECTIVE 17 MARCH 2014

(a) Evidence of the business rationale for Visa to proceed with its mandate in the absence of MasterCard implementing mandatory PIN@POS

In the absence of authorisation to proceed to implement PIN@POS jointly with MasterCard, Visa's position is that it would proceed individually to implement its PIN@POS mandate, for the reasons discussed below.

The business driver for Visa to introduce PIN@POS was a desire to seek to reduce card present fraud in Australia. Visa was motivated to move to mandatory PIN@POS based on the successful implementation of chip and PIN in Europe, and the corresponding drop in rates of card present fraud as a result of that program, as discussed in section 3.5 of the original supporting submission and in the document previously provided to the ACCC entitled "Chip and PIN in Europe".

Against this background, in 2008-2009 Visa initiated a number of client and government consultations regarding its seven point security plan, which included a proposal to move to mandatory PIN@POS. (The seven point plan is contained in Annexure D below). The plan was announced in December 2008. A key objective of the seven point security plan was to mitigate the growing trend of card fraud in Australia (see (6)(a) below), with a move to mandatory PIN@POS being a key component of this initiative. Please see:

- Annexure C: Visa's Strategic Direction (February 2009); See page 20 regarding mandatory PIN@POS; and
- Annexure D: Seven Point Plan for Strengthening Security (February and March 2009). See page 10 regarding mandatory PIN@POS.

These documents are **CONFIDENTIAL TO VISA**. Visa requests that the ACCC treat these documents as confidential and not place them on its public register or provide them to MasterCard.

ashurst

These presentations were given to various clients of Visa, and government bodies. Visa notes for completeness that subsequent to these presentations, Visa altered its mandate as described in section 4.8 of the original supporting submission, including to limit it to chip transactions only (not magnetic stripe transactions as outlined in these documents).

Visa considers that the implementation of mandatory PIN@POS, is consistent with its objective of reducing card fraud in Australia - by preventing fraudulent POS transactions verified with signature. Accordingly, in the event that authorisation is not granted, Visa intends unilaterally to implement the mandate for PIN@POS regardless of whether MasterCard also intends to itself individually implement a PIN@POS mandate.

5. ADDITIONAL INFORMATION ON THE PENORPIN CAMPAIGN IN 2008

(a) Reasons for the rate of conversion to PIN under this campaign. (Section 11(b) notes this is presently at 55 percent)

MasterCard participated in an Industry Working Group formed in 2007 by MasterCard customers, major retailers, other card schemes (including Visa and Amex) and their customers. In 2007-8, Australia was still a magnetic stripe market, and MasterCard anticipated PIN support to be a stepping stone to support EMV with PIN on credit, while Visa utilised the Pen or PIN campaign as a stepping stone to introduction by it of mandatory PIN at a later date.

The main objective of the Pen or PIN campaign in 2008 was customer choice. The campaign highlighted the option of replacing signature with PIN at Point of Sale. As a result of no card scheme enforcement and no major marketing activities, there was no significant rise in PIN usage.

The purpose of the campaign was educational in nature, and was to create awareness that PIN could now be used at all merchants in Australia as an additional option to signature. The campaign was of a very limited nature and cost. However, despite the fact that there has not been further communication focused on increasing PIN usage since the Pen or PIN campaign, the number of transactions that contain a PIN is approximately 55% today.

(i) Was there PIN usage before 2008 (ie prior to the PenorPin campaign) and, if so what was the rate of uptake of PIN before and after the campaign?

There was PIN usage before the campaign and the change in PIN usage after the campaign was insignificant due to the level of marketing funding.

(ii) Between 2008 and now, what factors have influenced the uptake of PIN in this period? There may include the PenorPIN campaign, customer preference, other factors.

Between 2008 and now, the migration to EMV has increased the usage of PIN at Point of Sale. Card issuers have moved to issuing EMV-compliant cards (ie, with chips) and have configured those cards for the use of PIN as the preferred CVM.

Issuers have also enhanced how their cardholders can update their PIN, and most now offer Cardholder Self Select PIN. The enhancements include PIN change via Interactive Voice Response (IVR) and/or bank call centres or other web-based methods, instead of the traditional PIN mailer. These have improved the cardholder experience and have helped to boost the PIN usage as cardholders can now remember their own PIN.

(iii) Is there now or was there previously a strong preference for some consumers for signature over PIN?

To date, PIN or signature has been the customer's choice although chip cards have helped to drive cardholder behaviour towards PIN. There is still a misconception by some cardholders that it is unsafe to enter PIN at point of sale due to potential fraud.

Marketing campaigns and education materials that will be developed as part of the current PIN initiative will assist to correct this incorrect assumption.

Current PIN and signature behaviours are driven by habit rather than conscious customer choice. Additionally, many merchants do not offer the choice of PIN at the time of payment even though the functionality exists. Many people who sign know their PIN but are not given the choice by the merchant; rather they are automatically given the payment slip to sign.

(iv) Is MasterCard expecting push-back from consumers in relation to mandatory PIN?

Based on the UK experience, no.

(v) Why would MasterCard mandate PIN individually when prior to its involvement in the steering committee MasterCard would have had a rationale for not mandating PIN? For example, in its 2011 Business Roadmap, MasterCard did not include a mandate for PIN@POS. What has changed such that in the absence of authorisation, it would now pursue mandatory PIN@POS?

MasterCard wishes to implement the increased security measure of mandatory PIN@POS, for the reasons set out in 3(a) above.

It wishes to put in place the current best practice fraud prevention measures for cardholders with the support of its financial institution members, which now exists. As noted above, in 2011 MasterCard's financial institution members were not supportive of the introduction of mandatory PIN@POS. This has since changed and they are now in favour of the increased security measures.

(vi) Is it possible MasterCard would not independently implement their mandate and would only do so if Visa was doing so?

As noted above, the introduction of PIN@POS is expected to reduce fraud in card-present transactions at POS. It is also now supported by its financial institution members.

For these reasons, MasterCard would implement mandatory PIN@POS independently of any actions Visa may be taking.

(vii) Could it be a competitive strategy for MasterCard to NOT mandate PIN and be more attractive to consumers who prefer to sign?

[CONFIDENTIAL TO MASTERCARD]

Those committing fraud will always look to find the weakest target. MasterCard anticipates that in the event that it did not implement its PIN@POS mandate but Visa did, those perpetrating fraud on signature would shift their focus to MasterCard cards, with the result that fraud on MasterCard cards would increase.

Accordingly, continuing to allow signature authorisation on MasterCard chip cards is not considered to be a viable option.

6. **ADDITIONAL INFORMATION ON THE URGENCY OF THE REQUEST FOR THE INTRODUCTION OF PROMOTIONAL MATERIALS TO SUPPORT VOLUNTARY PIN@POS. (THE SUPPORTING SUBMISSION NOTES THAT DELAYS MAY IMPACT FRAUD PREVENTION)**

As set out in the parties' supporting submission, the urgency of the request for the introduction of promotional materials results from the proposed timetable for the implementation of mandatory PIN@POS. A delay in the implementation of mandatory PIN@POS will impact fraud prevention. The data requested by the ACCC on fraud levels is set out below.

In order for mandatory PIN@POS to be introduced in a manner that results in the least confusion and disruption to cardholders and merchants it is important that the public communications strategy be able to commence as soon as possible. The public communications strategy is designed to raise public awareness of PIN@POS as a security measure and to promote the voluntary transition of cardholders from signature to PIN. In doing this, regardless of the outcome of the application for authorisation, the grant of interim authorisation will result in a public benefit through the increased awareness of PIN@POS as a result of the communications campaign. Apart from encouraging consumers to voluntarily adopt the use of PIN@POS, the grant of interim authorisation will not otherwise impact on the status quo.

(a) Please provide annual data on the incidence of fraud as a percentage of total credit card transactions since 2009 for all types of fraud in Australia

Please see Appendix A. The data in Appendix A sets out the incidence of fraud as a percentage of total credit card transactions (by number and value) for all types of fraud (as requested by the ACCC), as well as for those types of fraud that will be primarily impacted by the introduction of PIN@POS. Specifically, adopting the categories of fraud used by the Australian Payments Clearing Association, the categories of fraud that will be impacted by mandatory PIN@POS are:

(i) Lost/Stolen Card: fraud resulting from the loss or theft of an existing card and a transaction has taken place without the cardholder's consent or authority.

(ii) Card Never Received: fraud where a card has been intercepted (stolen) during delivery to the customer and used before it was received by the customer.

(iii) Counterfeit/Skimming: the use of altered or illegally reproduced cards including the replication/alteration of the magnetic stripe and changes to the details on the face of the card with intent to defraud. Skimming is a form of magnetic stripe counterfeiting where the magnetic stripe track information from a valid card is copied and this information is then encoded on a counterfeit or stolen card and used fraudulently.

Visa and MasterCard believe that mandatory PIN@POS will have a significant impact on the first two categories of fraud, namely lost/stolen card fraud and card never received fraud. As set out in the Supporting Submission to the application, the Financial Fraud Action UK estimated[6] that since the implementation of chip and PIN beginning in 2004, face-to-face card fraud declined by 69% (see Part 2 of Appendix 1 to the Supporting Submission).

It is also expected that mandatory PIN@POS will cause a significant reduction in the level of counterfeit/skimming fraud. As set out below in response to question 6(b), this was the experience in the UK.

---

6 In "Fraud, the Facts 2011"

The data set out in Appendix A indicate that the number and value of (i) lost/stolen card fraud transactions and (ii) card never received fraud transactions, have approximately doubled over the period from 2009 to 2012 in terms of both volume and value. The incidence of these types of fraud as a proportion of all transactions has also nearly doubled in the same period. In terms of counterfeit/skimming fraud, while the volume and value of this type of fraud has not changed significantly over the same period, it continues to be material.

(b) Section 3.5 of the submission refers to a reduction in the incidence of fraud based on the introduction of mandatory PIN@POS in the UK. Please provide data based on the UK experience for all fraud types for the use of credit cards in the UK.

For information on the UK experience following the introduction of mandatory PIN@POS the ACCC is referred to the Financial Fraud UK publication, *Fraud: The Facts 2012* (see: www.financialfraudaction.org.uk/publications). As set out in this publication, in the UK:

(i) counterfeit fraud losses have fallen by 72% since 2004; and

(ii) fraud losses at face-to-face transactions with UK retailers have fallen by 80% since 2004.

These reductions in fraud have been attributed to the introduction of "chip and PIN" in the UK 2004 which was then made mandatory in 2006. As set out in that report, the use of chip and PIN has led to a substantial reduction in lost/stolen fraud, mail non-receipt fraud (i.e. card never received fraud) and counterfeit fraud in the UK. Where in 2001 these types of fraud collectively accounted for approximately 74% of all "plastic card" fraud in the UK, by 2011 they accounted for only 29% of all plastic card fraud.

Please see this publication for further data and information on the UK experience.

Yours faithfully

Ashurst Australia

ashurst

APPENDIX A: FRAUD RATES IN AUSTRALIA ON AUSTRALIAN ISSUED CARDS

	2009		2010		2011		2012	
		PERCENTAGE OF FRAUDULENT TRANSACTIONS PER NUMBER/VALUE OF TOTAL CREDIT AND CHARGE TRANSACTIONS		PERCENTAGE OF FRAUDULENT TRANSACTIONS PER NUMBER/VALUE OF TOTAL CREDIT AND CHARGE TRANSACTIONS		PERCENTAGE OF FRAUDULENT TRANSACTIONS PER NUMBER/VALUE OF TOTAL CREDIT AND CHARGE TRANSACTIONS		PERCENTAGE OF FRAUDULENT TRANSACTIONS PER NUMBER/VALUE OF TOTAL CREDIT AND CHARGE TRANSACTIONS
TOTAL NUMBER OF DOMESTIC FRAUD TRANSACTIONS	202,405	0.0134%	274,308	0.0171%	393,706	0.0233%	514,804	0.0286%
TOTAL NUMBER OF LOST, STOLEN & NEVER RECEIVED	47,993	0.0032%	42,992	0.0027%	57,002	0.0034%	108,898	0.0060%
TOTAL NUMBER OF COUNTERFEIT / SKIMMING	30,625	0.0020%	30,164	0.0019%	41,804	0.0025%	37,484	0.0021%
TOTAL NUMBER OF CREDIT AND CHARGE CARD TRANSACTIONS	1,510,642,000		1,600,898,000		1,688,590,000		1,800,627,000	
TOTAL VALUE OF DOMESTIC FRAUDULENT TRANSACTIONS (A$)	$61,233,480	0.03%	$70,012,776	0.03%	$104,843,968	0.04%	$111,011,772	0.04%
TOTAL VALUE OF LOST & STOLEN, NEVER RECEIVED (A$)	$10,507,708	0.0047%	$9,502,688	0.0040%	$11,768,707	0.0047%	$21,195,036	0.0081%

ashurst

TOTAL VALUE OF COUNTERFEIT / SKIMMING (A$)	$15,527,781	0.0069%	$12,871,632	0.0054%	$16,469,564	0.0066%	$13,047,707	0.0050%
TOTAL VALUE OF CREDIT AND CHARGE CARD TRANSACTIONS (A$)	$225,764,000,000		$239,480,000,000		$249,644,000,000		$260,482,000,000	

Sources: Australian Payments Clearing Association Fraud Statistics 2009 – 2012 Calendar years and Reserve Bank of Australia Credit and Charge Card Statistics as at June 2013

ashurst