VISA

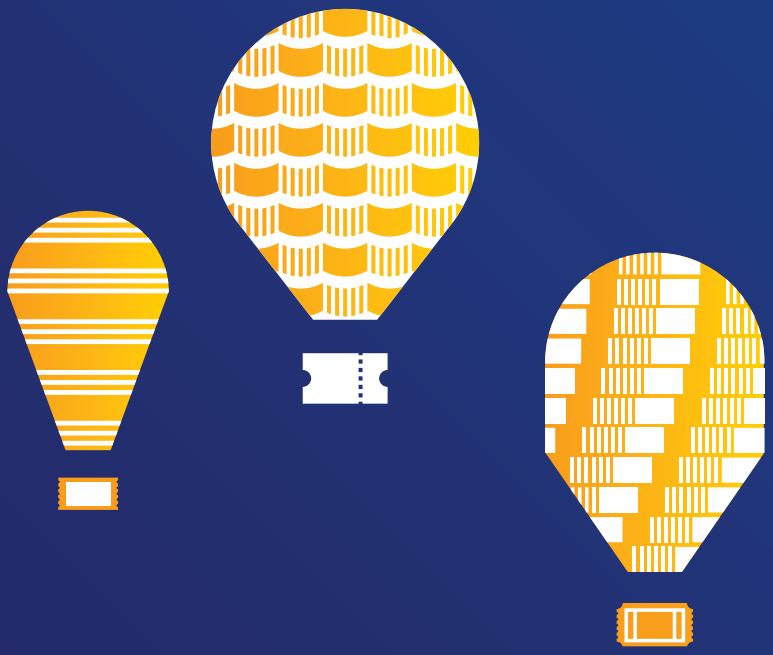
Tokenisation:

Why Australia, why now

Contents

Foreword

It is an exciting time to be in business



Foreword

It is an exciting time to be in business. Technology is fundamentally changing the relationship between consumers and the businesses that serve them. It has led to significant market and industry disruption and the payments industry is no exception.

In particular it is the rise of digital payments including mobile and online that presents the most opportunity and challenge in 2015.

This region has continually had one of the greatest adoption rates of smartphones in the world and our relationship with our mobile is deepening. Now, it is primed as a key source for multiple payment methods.

This white paper discusses tokenisation, a new layer of security for digital payments, because as technology evolves, payment security must evolve with it.

Tokenisation, while a largely invisible part of the payment process to consumers, will provide the foundation for future innovation. It will open up opportunities for new ways to pay and be paid – on the mobile, PC, tablet, and across future devices, whatever they may be.

Our experience tells us transformation will occur at a rapid rate. When we introduced Visa payWave, our contactless payments technology, we were confident Australians would enthusiastically take it up. The phenomenal growth we've seen over the last 12 months has exceeded expectations and confirmed that Australians are a nation of early adopters when it comes to payments.

Consumers are ready for the next phase of digital payments innovation and our investment in tokenisation will help enable that.

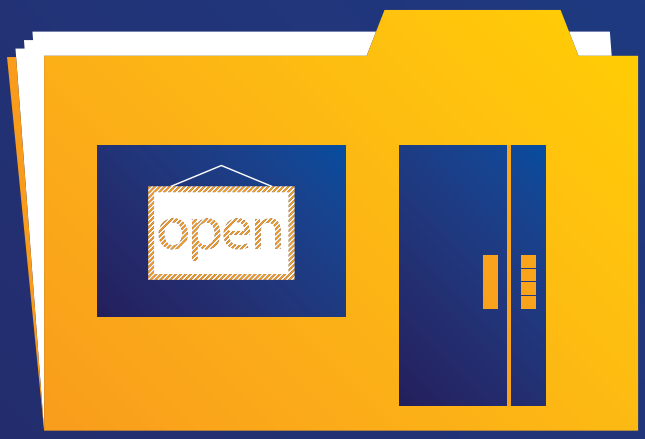
At every level of Australian business, from the corner store to the big institutions, 2015 will herald a change in the way Australians pay.

We hope the insights provided in this white paper will prove useful as we move forward into a challenging and transformative year.

Stephen Karpin
Group Country Manager, Australia, New Zealand and South Pacific, Visa

Executive Summary

The digital revolution has created an almost unlimited ability to participate in commerce



Executive Summary

The digital revolution has created an almost unlimited ability for companies – from start-ups to the world's largest – to participate in commerce by creating new experiences through mobile, tablets, PCs and future connected devices. As these new payment experiences evolve, so must the security measures that protect consumers' confidential account information.

This white paper explains tokenisation, a new layer of security for digital payments, and the challenges and opportunities it will present for merchants, financial institutions and consumers in Australia in 2015.

There are a number of factors driving the need for tokens, in particular the shift to mobile. The smartphone is our social media manager, personal assistant, DJ and GPS. It is already at the centre of commerce in Australia today.

The rapid rise of contactless payments has set the scene for a shift to mobile payments in-store.

The right infrastructure is in place, and with more acceptance points for mobile, the more we are likely to see consumers using their phone to transact.

The mobile is also a gateway to shopping online and mCommerce is increasing, but consumers remain concerned about leaving their card details with different merchants over the web.

Tokenisation will bring an added layer of security to mobile and digital payments without adding friction to the shopping experience.

It's a new layer of security that is needed now.

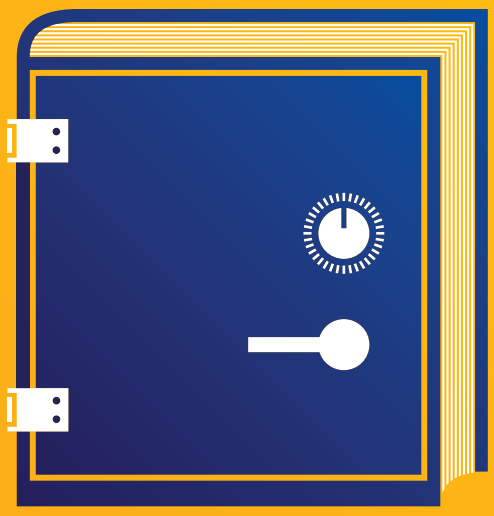
Technological change is hard to anticipate, the impacts are difficult to predict and its effects on society are often unclear. This white paper is a discussion on tokenisation and why its impacts are important for Australia's payments industry in 2015.

This paper includes new research conducted by UMR Strategic Research on behalf of Visa. The Visa/UMR Strategic study, conducted in November and December 2014, identifies the views of 1,000 consumers and over 200 merchants to understand their views on payments and technology and their appetite for change.

Tokenisation Explained

This technology, and the associated standards, are exciting new developments for the payments industry

Tokenisation Explained



Before we explain what tokenisation is and how it works, it is crucial to note that this technology, and the associated standards, are exciting new developments for the payments industry. And like any new technology, tokenisation will continue to evolve based on the needs of consumers and the dynamics of the Australian marketplace.

While some of the concepts outlined here are **real and happening**, others are an articulation of the possible, based on what we know. This is a dynamic industry and Visa is committed to staying at the forefront and adapting to the needs of Australian consumers, issuers, acquirers and merchants, as we bring digital payments into the everyday.

Tokenisation Explained

What is tokenisation?

Tokenisation replaces cardholder information such as account numbers and expiration dates with a unique series of numbers (a "token") that can be used for payment without exposing a cardholder's more sensitive account information.

Payment tokens provide improved protection against potential misuse, because they are connected to a specific device or application. Today, in the chance that a shopper's customer account details are captured during a data breach, they may be used to conduct a fraudulent transaction in other online environments. With tokenisation, the account details are hidden and protected from a potential fraudster.

Tokenisation Explained

Why tokenisation

As digital payments accelerate and grow, confidential account information is increasingly placed in environments that are not as secure as the face-to-face environment, where we use our chip-enabled cards. In the future, people will transact in digital environments more and more, across multiple devices and applications. Tokenisation hides the consumers' confidential account information during digital transactions, making digital payments more secure for everyone, everywhere.

Tokenisation Explained

Creating an industry standard for tokenisation

Tokenisation works in different payment contexts. In fact, it exists today in different forms. For example, payment gateway providers offer online merchants a service that tokenises their cards on file. The tokens are specific to that gateway provider, who uses the token to initiate the transaction. Where this differs from new tokenisation technology however, is that the token is converted back to the customer's primary account number (PAN) during the actual payment process, therefore not hiding the sensitive account information. In tokenisation, the payment token is used throughout the payment process.

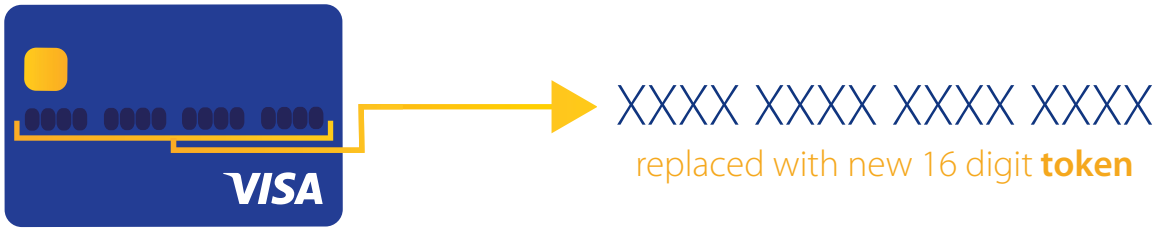
Now, tokenisation is being elevated to the entire payments ecosystem. These industry-wide tokens behave just like a PAN and can therefore be understood and used by card schemes, banks and merchants. **This is a major step forward for payments security.**

In 2013, Visa, along with MasterCard and American Express, developed a tokenisation framework for the payments industry. One of the key drivers for this was to evolve how PANs are managed in an expanding digital ecosystem. Consumers want the convenience of using their cards in emerging channels and environments, but as payment technology evolves, security solutions must keep pace. In the digital world, the key to reducing fraud is devaluing the sensitive account information, thereby reducing its appeal to fraudsters. Tokenisation hides this data by removing the PAN from the payment environment.

Tokenisation Explained

How tokenisation works

The basic explanation behind tokenisation is that the 16 digit card number is replaced with another 16 digit number called **a token**. This token, or digital account number, is used to complete the transaction.



But simply replacing the card number with a token is only the beginning.

Tokens can be ring-fenced to specific environments and to specific use cases, such as mobile. If anyone attempts to use a token in a different environment, the transaction will be flagged immediately as fraudulent and will be declined. This ability to restrict where and how tokens can be used limits the impact of fraud.

For example, if a fraudster was to get hold of a token that has been provisioned to a mobile device, and then try to use it for an online eCommerce transaction, the transaction would be declined. This creates an additional layer of security by limiting the ways in which a criminal could use stolen account information.

Tokenisation Explained

Tokenisation in action

Tokenisation can be split into two main components:

1 Provisioning:

This is a one-time step that happens before payment can take place. The consumer's PAN is linked to a token and the token is then provisioned to the device or wallet.

2 Token transaction processing:

This takes place during the payment.

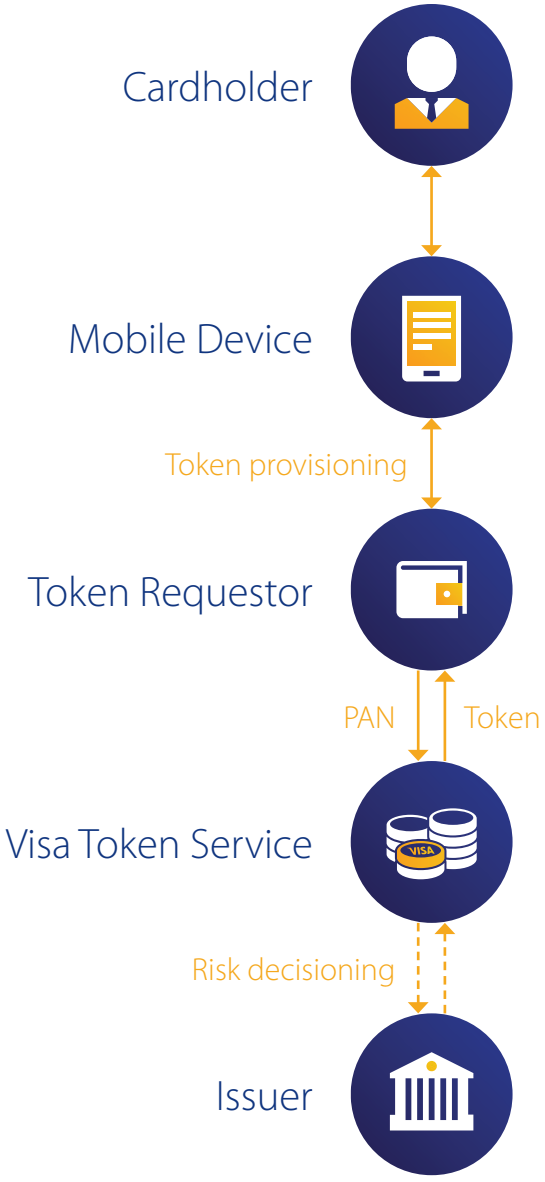
Tokenisation Explained

To explore how these components work, let's use a mobile phone as an example

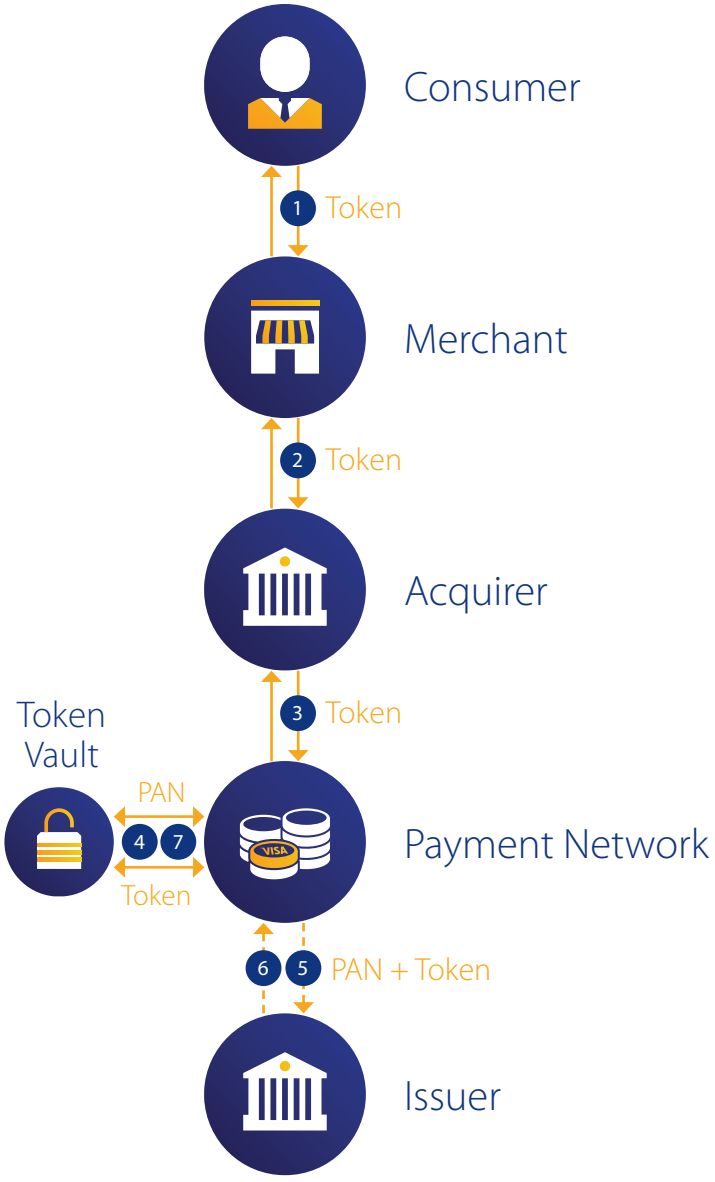
Tokenisation Explained

The cardholder starts the provisioning process by adding their card to their mobile phone. In this specific example, the handset provider is the token requestor, so in the case of Apple Pay, Apple is the token requestor. In future when tokenised solutions are available with other mobile payment devices, those handset providers will be the token requestor. Or, in an online retail example, a merchant could be the token requestor.

The token requestor initiates a request to the Visa Token Service. Visa Token Service confirms the card is eligible, generates the risk score, and delivers the information to the issuer to determine if the token request should be approved, declined or flagged for additional verification. If approved, Visa generates a new token and sends it to the token requestor. The token requestor provisions the token to the device and activates for payment. The token would then be stored in the consumer's mobile phone. In an online example, the token would be stored in the online merchant's database.



Tokenisation Explained



Let's continue with the mobile phone example and look at a proximity transaction at the point of sale. The consumer makes a payment using their phone at a Visa payWave-enabled terminal. Instead of the PAN going to the merchant's bank, the token is sent instead. The merchant's bank, also known as the acquirer, passes the token to Visa, where it is validated and de-tokenised back to the PAN so it can be identified by the issuer of the card. Visa provides the issuer of the card (i.e. the cardholder's bank) with the token and the PAN for authorisation. After the issuer authorises or declines the transaction, the token and PAN are passed back to Visa. Visa then re-tokenises the PAN and sends a response to the acquirer and merchant. This all happens in less than a second, and the consumer won't know that the tokenisation process has occurred in the background.

This is just one example of tokenisation in action. A consumer's PAN could be linked to many different tokens, with each token used in a different device or channel or at a different online merchant. Because each token is ring-fenced to a specific channel or merchant, if one token is compromised, the customer's card doesn't need to be replaced, only the token.

Tokenisation Explained

Tokenisation adds security without creating friction

Tokenisation is designed to be compatible with existing payment systems, which means bringing greater security but minimal disruption to issuers, acquirers, merchants and consumers. The payment experience can remain as frictionless as in the traditional face-to-face environment.

Issuers can focus on developing new and innovative mobile and digital payments services without worrying about how to store card credentials on mobile apps on networked devices. They also don't need to re-issue cards if only a token is compromised.

Merchants and acquirers will find in many situations that tokenisation is interoperable with their existing payment platforms, with some enhancements. Tokens behave just like primary account numbers. Yet merchants and acquirers will benefit from added protection and not having to store or manage confidential account information.

Consumers won't see tokenisation happen and might not even know it exists. It will be a largely invisible part of the payment process, happening in the background. However, they will benefit from added security. Crucially, a token can be deactivated, reactivated or replaced without affecting the consumer's bank card. This means there is no need to reissue cards if a token is stolen – only the token needs to be replaced.

Why Australia

Australia is in a position to rapidly adopt new methods of digital payments, in-store and online

Why Australia

Although payment innovation is happening across the world, Australia is in a position to rapidly adopt new methods of digital payments, in-store and online. Powerful convergent influences are accelerating this change:

High smartphone penetration and use for online commerce

Adoption of Visa payWave and the shift to mobile Visa payWave

Growth in online shopping

High EMV chip adoption vs. magnetic stripe use in other markets

These factors combined place Australian consumers in a favourable position to continue their history of early adoption of innovative technology.

Compared to similar markets, including Canada, the United Kingdom, the USA and Singapore, Australia is ahead of the curve in the key areas which promote adoption of payment innovation both digital and in-person.

Australians have one of the highest rates of smartphone ownership and they are using their devices to transact online at higher numbers, with double the amount of smartphone shoppers than in the UK or USA. [1]

[1] See pages 21 – 22

Why Australia

Visa payWave is currently experiencing the highest levels of popularity in Australia, with double the adoption rate of one of the country's closest regional neighbours, Singapore.

Internet penetration exceeds that of Canada, USA, UK and Singapore and Australians shop online at rates higher than the other markets compared.

Further, the EMV chip technology standard has been successfully adopted by Australian financial institutions and rolled out to cardholders and merchants in this market. Elsewhere, like in the United States, it is currently being rolled out to over 575 million cards to lower the risk of fraud and speed up the adoption of contactless and mobile payments.[2]

It is these influences that give rise to the need for tokenisation in Australia.

[2] Gemalto, The Migration to EMV Chip Technology White Paper, 2011

Australia

60.4%

Adoption of Visa payWave has reached 60.4% of all face-to-face Visa transactions [3]

70%

Smartphone penetration has reached 70% [4]

Internet penetration in Australia is at 89% [5]

43%

of Australians shopped online using a smartphone in 2014 [6]

92%

of Australians have shopped online [7]

Canada

14.7%

Adoption of Visa payWave has reached 14.7% of all face-to-face Visa transactions [8]

55%

Smartphone penetration has reached 55% [9]

Internet penetration in Canada is at 83% [10]

20%

of Canadians used a smartphone to shop online in 2014 [11]

82%

of Canadians shopped online in 2014 [12]

UK

41M

41 million contactless cards [13]

71%

Smartphone penetration has reached 71% [14]

Internet penetration in the UK is at 84% [15]

14%

of Britons used a smartphone to shop online in 2014 [16]

67%

of shoppers in the UK have made a purchase online [17]

[3] VisaNet, January 2015
[4] Visa/UMR Strategic study, February 2015 (see appendix for more details)
[5] Nielsen Global eCommerce Report, August 2014
[6] Visa/UMR Strategic, The Future of Payments – Everywhere Commerce study, July 2014
[7] Visa/UMR Strategic, The Future of Payments – Everywhere Commerce study, July 2014
[8] VisaNet, September 2014
[9] Catalyst and Group MNext, Acting on the Evolution of the Canadian Smartphone User report, March 2014
[10] Nielsen eCommerce Report, August 2014
[11] The Ipsos Canadian Inter@ctive Reid Report, September 2014
[12] The Ipsos Canadian Inter@ctive Reid Report, September 2014
[13] VisaNet, September 2014
[14] Kantar Worldpanel ComTech, April 2014
[15] Nielsen Global eCommerce Report, August 2014
[16] Google Consumer Barometer report, November 2014
[17] Centre For Retail Research study, March 2014

USA

Smartphone penetration has reached 72.9% [18]

Internet penetration in the USA is at 78% [19]

of Americans use a smartphone to shop online in 2014 [20]

of Americans shopped online monthly in 2014 [21]

Singapore

Adoption of Visa payWave has reached to 21.5% of all face-to-face Visa transactions [22]

Smartphone penetration has reached 85% [23]

Internet penetrations in Singapore is at 75% [24]

of Singaporeans use a smartphone to shop online in 2014 [25]

of Singaporeans shopped online at least once a month [26]

[18] ComScore MobiLens® and Mobile Metrix®, October 2014
[19] Nielsen Global eCommerce Report, August 2014
[20] GfK FutureBuy study, October 2014
[21] PriceWaterhouseCoopers, Total Retail Survey United States (US), October 2014
[22] VisaNet, July 2014
[23] Google Consumer Barometer report, November, 2014
[24] Nielsen Global eCommerce report, August 2014
[25] Google Consumer Barometer report, November 2014
[26] GfK online shopping report, August 2014

Why Now

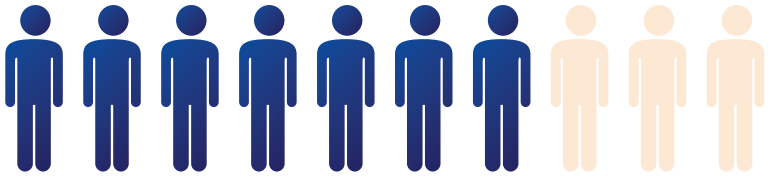
Tokenisation will bring an added layer of security to mobile payments without adding any friction

Why Now

Tokenisation will bring an added layer of security to mobile payments without adding any friction. It's a new layer of security that is needed now, given the smartphone is already at the centre of commerce in Australia today.

Mobile payments in-store

The rapid rise of contactless payments has set the scene for a shift to mobile payments in-store. The right infrastructure is already in place, as mobile proximity payments use the same technology as contactless-enabled cards.



Currently 70%

of Australians own a smartphone,

providing a large potential user base for mobile payments.[27] This user base is ready to pay using their mobile device, with UMR Strategic Research for Visa finding that 53 per cent of Australians are interested in being able to use their smartphone to pay in store.[28]

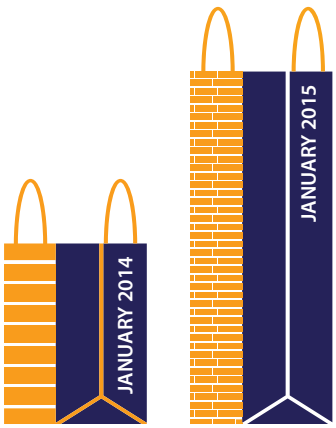
of Australians are interested in using smartphones to pay in store

[27] Visa/UMR Strategic study, February 2015 (see appendix for more details)
[28] Visa/UMR Strategic study, February 2015 (see appendix for more details)

Why Now

▼ Mobile payments in-store

Just as 2014 was the year contactless payments reached mass adoption in Australia, 2015 is poised to be a tipping point for mobile payments.



Use of contactless payments has almost doubled in the past year, with more than 70 million transactions a month now taking place with a simple 'wave and go'.[29] Consumers are choosing the convenience of contactless and the extension from cards to smartphones is a natural progression.

There are already mobile payment technologies available and they are gaining traction with consumers. Examples of existing mobile proximity payments in Australia and around the world include:

- Cuscal Redi2Pay
- Cash by Optus
- Westpac and The Commonwealth Bank of Australia (CBA) both providing apps for contactless smartphone payments
- Apple Pay, currently live in the US
- Zapp, currently live with five different banks in the UK

These examples all use different technologies for enabling payments on the phone. For instance Cash by Optus uses the USIM model, where payment data sits on the SIM to activate payment at the contactless terminal. Cuscal uses Host Card Emulation (HCE) where payment data is regularly updated from the cloud. The Westpac, CBA and Apple Pay models rely on the embedded secure element where the payment data sits on the device, or in CBA's case, on the device or on its PayTag, also known as a payment sticker.

[29] VisaNet, January 2015

Why Now

▼ Mobile payments in-store

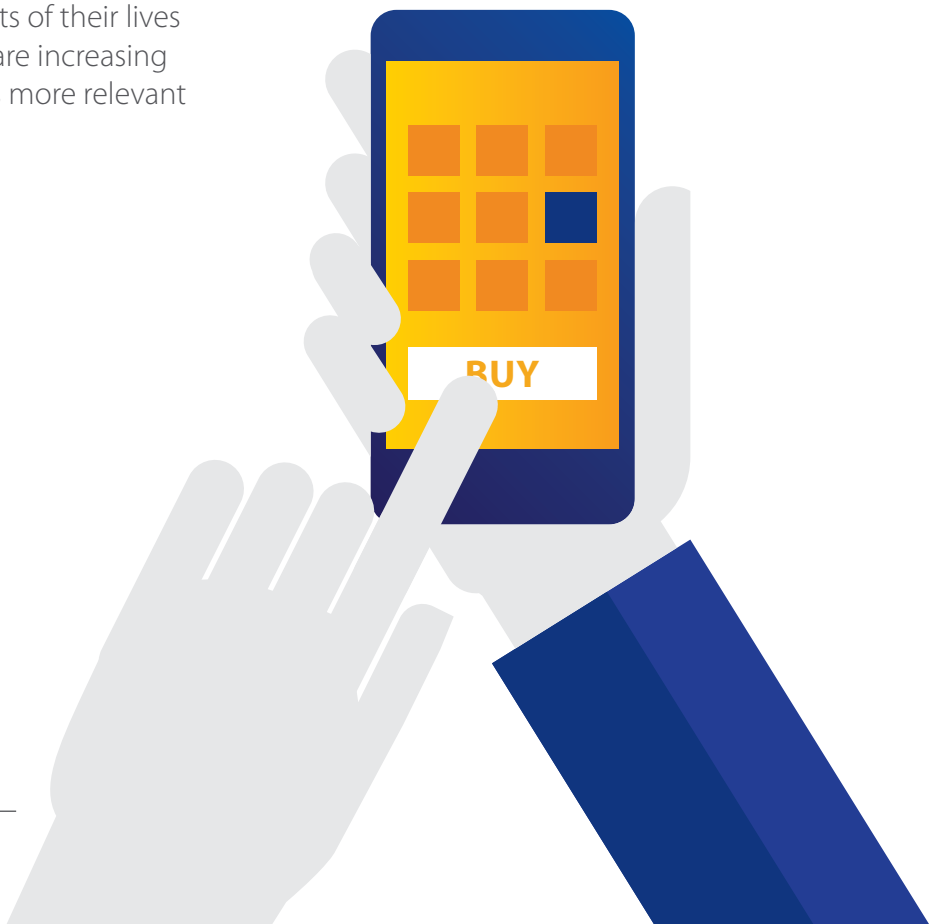
These technologies, while different, are all used to ensure mobile payment data is securely provisioned to the phone to enable mobile payment. Tokenisation then provides an additional layer of security to mobile payments technology, which is important because it opens up the potential to safely integrate cardholder information in a wider range of apps.

Tokens can be locked down to an individual's phone, meaning if the phone is lost or stolen the consumer's account information can't be used in a different channel. Because the consumer's account details wouldn't be compromised, they wouldn't need to get a new card if they have lost their phone. Only the token would need to be replaced.

Consumers increasingly prefer to use their smartphone in more aspects of their lives and banks and merchants are increasing their focus on making apps more relevant to today's consumer.

According to Capgemini's World Payments Report 2014, **mobile payments could increase by as much as 60 per cent worldwide, amounting to 47 billion transactions this year.**[30]

This highlights the stark need for tokenisation. It provides an additional layer of security to mobile payments technology, which will be beneficial as more Australians take up mobile payment solutions in 2015.



[30] Capgemini World Payments Report, October 2014

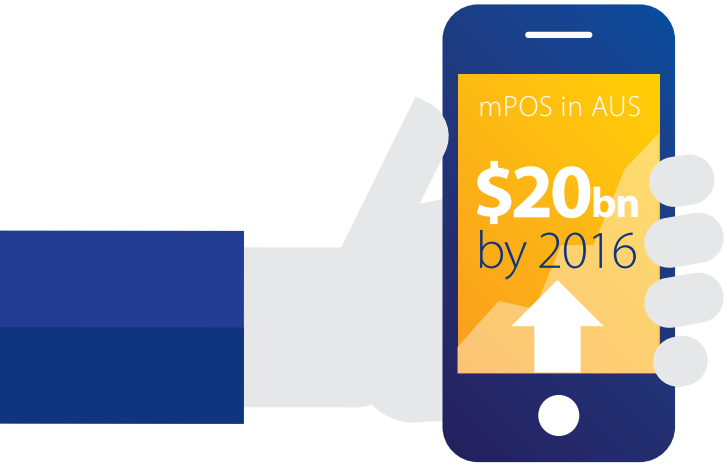
Why Now

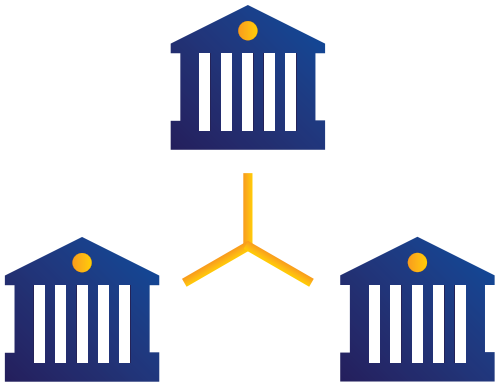
The mobile merchant

The smartphone is also opening up a new category of merchants.

mPOS, or mobile point of sale, creates opportunities for merchants of all sizes, even the door to door salesman, to accept electronic payments using a mobile terminal or device plugged into their mobile phone.

As a category, mPOS is growing rapidly and reducing the barrier for merchants to enter the digital payments landscape.[31] It has opened up the opportunity for new players on the payments side as well. Technology companies such as Mint Wireless, Square and Amazon have either entered the Australian market or are operating in similar overseas markets. mPOS provider Mint Wireless has estimated the value of mPOS transactions in Australia has the potential to grow to US$20 billion by 2016.[32]





Similarly, Australian banks are innovating, competing with technology companies big and small who provide mPOS technologies to the market. ANZ's FastPay and Westpac's PayWay are just two examples of technology which the banking sector has deployed in this space.

It's important to highlight this trend because the more acceptance points for mobile, the more we are likely to see the consumer using their phone to transact.

[31] PYMTS.com article, August 2014
[32] Start Up Daily article, January 2014

Why Now

Mobile offers

The GPS capability of smartphones provides opportunities for merchants to connect with consumers in new ways. For example, merchants can provide offers and notifications to their customers' smartphones via a Bluetooth low energy (BLE) signal[33] whenever they are in close proximity to a store. This is a growing marketing technique, which we expect to see more of in 2015, and it is important because it again places the smartphone at the centre of commerce.

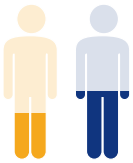
There is strong evidence from abroad that using geofencing to reach customers and convert purchases works, with specialist company Placecast delivering Kiehl's, a US cosmetics retailer, a 73 per cent purchase success rate with customers who signed up to receive text message alerts upon entering the store's geofenced zone.[34]

But consumers need to opt in to receive these notifications, otherwise the investment by merchants in the technology will yield no results.

UMR Strategic Research for Visa outlined:

32% **of Australian merchants** surveyed are either already or very likely to adopt geo-marketing.

However, the type of business and its consumer demographics will be crucial to the success of the activity.[35] Fifty-seven per cent (57%) of Australians would try to block a merchant who targeted them with geo-marketing, but the sentiment of those who find the tactic worthwhile and exciting falls clearly within generational lines.[36]



Only 25% of 30-49 year olds agree that geo-marketing is worthwhile, **while 42%** of 18-29 year olds would embrace the tactic.[37]

As the spending power of the 18-29 demographic increases, the opportunity to profit from geo-marketing will improve accordingly. Again, we see the smartphone at the centre of commerce.

[33] Business Insider article, June 2014
[34] Smarter Business Ideas article, January 2015
[35] Visa/UMR Strategic study, February 2015 (see appendix for more details)
[36] Visa/UMR Strategic study, February 2015 (see appendix for more details)
[37] Visa/UMR Strategic study, February 2015 (see appendix for more details)

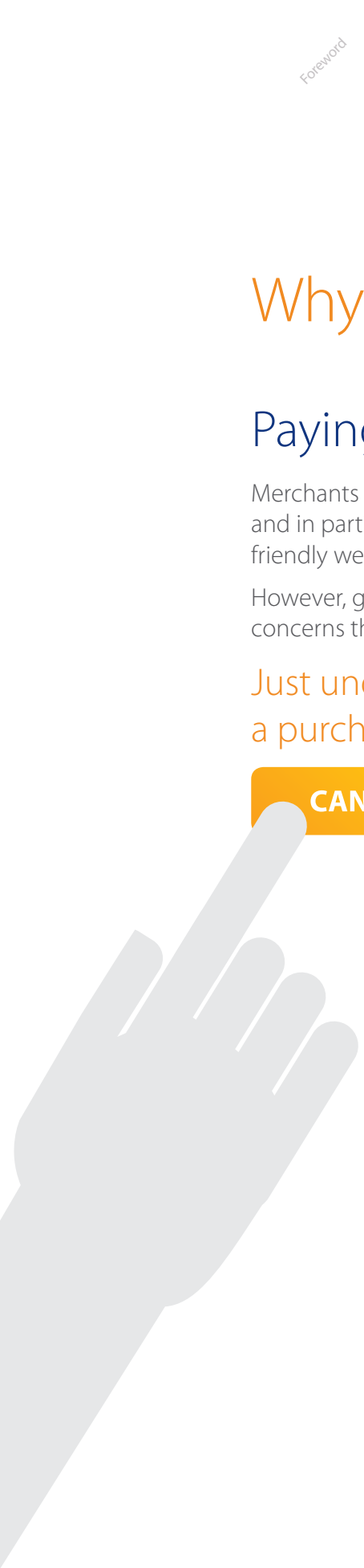
Why Now

Paying online

Merchants in Australia are well aware of the growth of online shopping and in particular the rise of mobile commerce, with 53% saying a mobile-friendly website is important for their business.[38]

However, growth in online spending is under threat by the security concerns that many Australians feel when they shop online.

Just under half of Australians (46%) have stopped a purchase when shopping online because they didn't trust a merchant with their card details.[39]



Although price is the number one influence on purchase decisions in-store, security is the most important when deciding where to shop online.[40]

Consumer concern regarding security is something merchants are aware of and are responding to as a priority. UMR Strategic Research for Visa shows that 87 per cent of Australian merchants rate keeping customer credit card details secure as important for their business, over and above other important aspects like a mobile optimised website.[41]

[38] Visa/UMR Strategic study, February 2015 (see appendix for more details)
[39] Visa/UMR Strategic study, February 2015 (see appendix for more details)
[40] Visa/UMR Strategic study, February 2015 (see appendix for more details)
[41] Visa/UMR Strategic study, February 2015 (see appendix for more details)

Why Now

▼ Paying online

In this era of high-profile data breaches, trust and security are paramount for consumers, particularly when they're shopping on their phone or tablet. The introduction of tokenisation will add a new layer of security in payments, placing greater confidence in shopping over the web. Tokens also offer the potential to prevent disruptions to web and other card on file merchants caused by changes in the underlying card account information. Currently, if an online merchant stores a consumer's card information on file, any changes to the cardholder's underlying card information (such as expiry date changes or the issuance of a new PAN) will cause subsequent transactions to fail.

Merchants are forced to contact the customer to obtain the updated card information, a significant cost to merchants and an inconvenience to consumers. With tokens, updates to the card account are automatically applied in the token vault, ensuring uninterrupted payment for merchants and uninterrupted service for consumers.

This is one of the reasons Visa launched Visa Checkout, a quick and easy payment service that enables Australian consumers to pay for goods online, on any device, in just a few clicks.

Why Now

Future ways to pay

Our personal arsenal of networked devices is set to grow beyond smartphones, tablets and laptops to incorporate many of the objects used in day-to-day life. From wearable technology to car dashboards, these devices will be linked to each other and to the cloud. In a world where everyday devices add greater automation and convenience to consumers' lives, it's a reasonable expectation that people will want to use these connected devices to pay for goods and services, anywhere and at any time. The key to safely and securely opening up this ecosystem of previously unimagined payment devices and experiences will be tokenisation.

Wearable computing technology is set to explode in growth. US Research analyst BI Intelligence projects that by 2019 more than 148 million wearables alone will be shipped globally annually, up from 33 million units in 2014.[42]

Apple and Google have both entered the smartwatch market. Given their dominance in mobile platforms (over 90% of the market), they're expected to ignite demand for wearables, starting with smartwatches and expanding from there.[43]

Likewise, the Internet of Things is opening new avenues for payment innovation. Cisco has predicted that there will be 25 billion connected devices in the world in 2015, which is set to double to 50 billion by 2020.[44]

[42] BI Intelligence ,The Wearable Computing Market Report, November 2014
[43] BI Intelligence ,The Wearable Computing Market Report, November 2014
[44] Cisco Internet Business Solutions Group infographic, April 2011

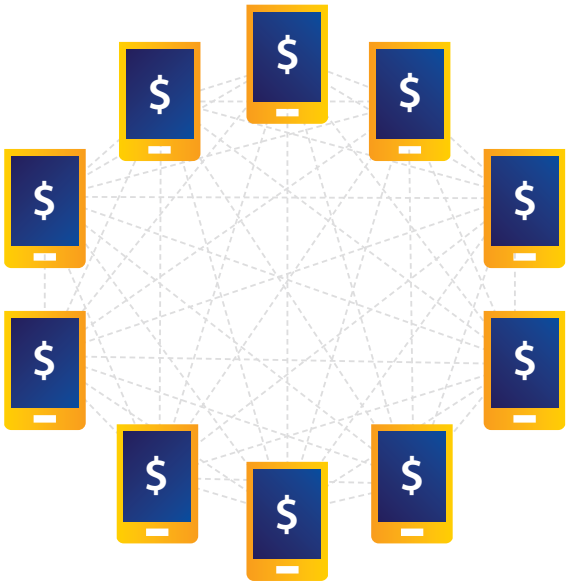
Why Now

▼ Future ways to pay

This movement will mean connected devices have the ability to connect to a payment process, potentially opening many new devices to joining the digital payments ecosystem.

SAP's proof of concept at Mobile World Congress 2014 is a powerful example. By connecting vending machines to smartphone applications, which allow for payments, gamification and connection to social networks, the consumer's experience is deepened and enriched.[45]

This is the power of tokenisation. By avoiding the need to disclose the cardholder's most sensitive account information, tokenisation has the ability to transform any device into a secure vehicle for commerce.



Other potential examples of payments in the Internet of Things include a connected car, or a connected refrigerator. A car with payments capability embedded in the dashboard and made secure using tokenisation could be used to pay for petrol at the pump, without needing to pull out a card. The refrigerator of the future could be equipped to allow consumers to scan items as they run out, generate a shopping list based on these items and place an order for delivery, paying securely and automatically.

As with the strong desire to use smartphones to make payments online and in-store, opening up the payment ecosystem to new devices and experiences will deliver previously unimagined payment possibilities. Tokenisation breaks down the barrier of risk that has existed around putting a consumer's PAN into more devices.

[45] Citeworld article, March 2014

The Challenge in 2015

The possibilities are exciting and difficult to measure, but the opportunity is clear

The Challenge in 2015

At the moment, Australian businesses risk missing out on opportunities, especially as consumers continue to embrace new technology. The shift to contactless and mobile payments is accelerating; however:

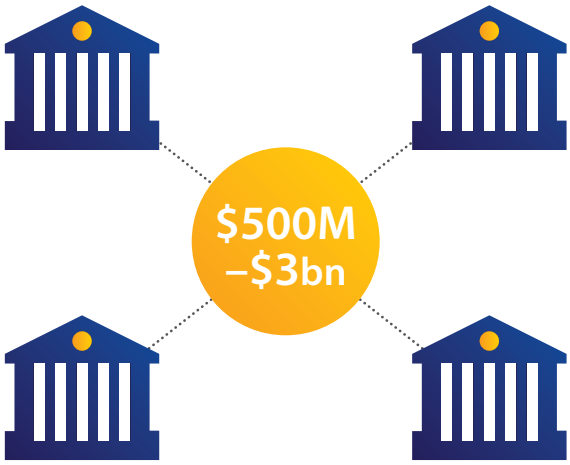
23 per cent of merchants haven't upgraded their in-store payment terminals and have no plans to do so.[46]

Research from Macquarie Group has predicted that $27 billion worth of market share is currently under threat from digital disruptors in the Australian banking sector's key payments and lending markets.[47]

In response to the risk the big four banks are reportedly planning on spending between $500 million to $3 billion to upgrade their core banking systems over the next four years.[48]

It is this focus on investing in technology that will power the sector's ability to be competitive, now and into the future. Fundamentally, providing the easiest path to purchase is key. Consumers are actively looking for the best experience across in-store and online.

The potential for rapid consumer behaviour change is here, with mobile firmly at the centre of commerce. Tokenisation is the key enabler to drive this change forward and create new ways to pay and be paid, for everyone, everywhere.



[46] Visa/UMR Strategic study, February 2015 (see appendix for more details)
[47] Macquarie Group research, July 2014
[48] Macquarie Group research, July 2014

Key Findings at a Glance

Key Findings at a Glance

Australia is uniquely positioned to drive new ways to pay, online and in-store, and we all have a role to play in driving that transformation

The smartphone is at the centre of commerce and this is set to grow in 2015

Payment security is a key concern for consumers who want to shop online, from any device, anytime

Tokenisation is an added layer of security for digital payments

Tokenisation will open up opportunities for future ways to pay

Key Visa/UMR Strategic Research at a Glance

Consumer views[49]

70% of Australians
own a smartphone

43% of Australians shop online using a smartphone in 2014

92% of Australians have shopped online

Three in five Australians
shop online at least once a month

39% of 18-29 year olds
and
25% of 30-49 year olds
shop online at least once a week

84%

Security
is an important factor when shopping online, with 84% of respondents saying it was either important or very important

CANCEL

Almost half of all Australians (46%)
have stopped an online purchase because they did not trust the retailer with their card details

53% of Australians are interested in using smartphones to pay in store

Only 25%
of 30-49 year olds agree that geo-marketing is worthwhile,

while 42%
of 18-29 year olds would embrace the tactic

[49] Visa/UMR Strategic study, February 2015 (see appendix for more details)

Key Visa/UMR Strategic Research at a Glance

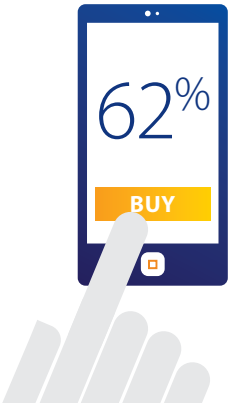
Merchant views[50]

of merchants prefer customers to pay by 'wave & go' such as Visa payWave

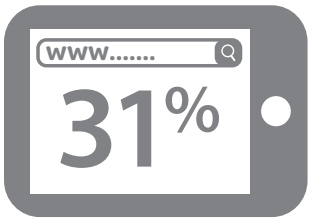
87%
of merchants rate 'keeping their customers' payment information secure' as important or very important

28%
of online merchants are only 'somewhat confident' or 'not confident' about the security of customers' payment information

84%
of merchants agree that developing new technologies that mean they will no longer have to collect and store customer card information is a good thing



of merchants are comfortable with consumers using smartphones to make payments in-store



of merchants have not, but would like to optimise their website for smartphones

33%
of online merchants have simplified their checkout process to make payment easier for customers

[50] Visa/UMR Strategic study, February 2015 (see appendix for more details)

Glossary of Terms

Glossary of Terms

Beacons	a small broadcasting device that allows other Bluetooth enabled devices, such as smartphones, to receive tiny amounts of information within a short distance of the beacon
Digital Account Number	another name for a token. The digital account number replaces the PAN in the tokenisation process
EMV	stands for Europay, MasterCard and Visa and is a joint effort to ensure the security and global interoperability of chip-based payment cards
Gateway Tokenisation	this describes the kind of tokenisation that is currently available in the market. The Visa Token Service elevates tokenisation to the ecosystem level making online and mobile payments more secure in more places
Geofencing	is a feature that uses the global positioning system (GPS) or radio frequency identification (RFID) or Bluetooth of devices to define geographical boundaries – a virtual barrier. It is most commonly used to allow an administrator to set up triggers so when a device enters or exits the boundaries of the geofence a text message or email alert is sent
HCE	stands for Host Card Emulation and is a technology that allows the presentation of a virtual and exact representation of a payment card using only software, by storing it in the cloud
mPOS	stands for mobile point of sale and is a smartphone, tablet or dedicated wireless device that performs the functions of a cash register or electronic point of sale terminal which is not hardwired
NFC	stands for near field communication and is a set of technologies that enables smartphones or other devices to establish a radio communication with each other or another device by bringing them into proximity with each other

Glossary of Terms

Primary account number (PAN)	also referred to as the payment card number is the 16 digit number on a payment card
Proximity payments	a payment made at a point of sale (POS) terminal, typically by a payment card or mobile phone
Remote payments	payment from a remote location such as one made over the phone or internet or via a mobile device
Secure element	a dedicated tamper-resistant platform such as a chip capable of securely hosting applications and their confidential and cryptographic data in accordance with the rules and security requirements set forth by EMV. The secure element resides in the handset and holds the payment data
Tokenisation	tokenisation replaces cardholder information such as account numbers and expiration dates with a unique series of numbers (a "token") that can be used for payment without exposing a cardholder's more sensitive account information. It is a new layer of security for digital payments
USIM	stands for universal subscriber identity module, or universal SIM card. They are the next generation of mobile phone SIM cards with more power and capabilities than other SIM cards. USIM allows e-payment, video calling, encryption of calls and data exchanges and other benefits. In the case of Cash by Optus, the USIM holds the payments data

Appendix

About the Visa/UMR Strategic Study

The research was conducted by UMR Strategic Research Pty Ltd. Fieldwork was carried out between 21 November and 15 December 2014. A nationally representative sample of 1,000 consumers and 200 merchants were interviewed online, all aged 18 years and over.

Disclaimer

The information and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.