Visa's Future of Security Roadmap: Australia

VISA

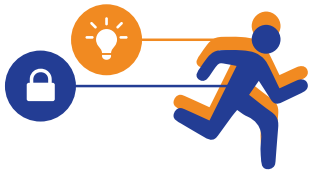
Contents

- Executive Summary
- Changing Fraud Landscape
- Roadmap
  - 3-Domain Secure 2.0
  - Biometrics
  - Tokenisation
  - EMV Chip Technology
  - Expanding Mobile Acceptance
- Additional Tools for Enhancing Security
  - Mobile Geo-location
  - Transaction Controls and Alerts
- Call to Action

Disclaimer

Case studies, statistics, research 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. You should consult with your legal counsel to determine what laws and regulations may apply to your 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. 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. 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.

Executive Summary



At Visa, we believe that security must move at the speed of innovation.

For nearly 60 years, Visa has been a leader in payments security, and as technology advances and fraud moves to the weakest points in the ecosystem, our innovations have kept pace. This has helped to keep fraud rates at historic lows.

We are guided by the principle of **responsible innovation.** This means any new capabilities we develop must also be secure. It is our responsibility to balance security with the need to reduce friction in the payment experience; we can't have one and not the other. Therefore, at Visa we continue to invest to **drive security** across the payments ecosystem, while improving the payments **experience for consumers.**

To date, Visa has worked with our industry partners on delivering a 7-point security plan for Australia, which focused on chip technology (EMV), PIN and Payment Card Industry (PCI) Compliance. We've come a long way since that was introduced. In just a few short years, together we have made EMV Chip technology near-ubiquitous, mandated PIN enablement and collaborated on a number of other initiatives to enhance industry-wide security.

But many of these solutions are focused on securing payments using technology specific to the environment, like chip technology in the face-to-face environment or password authentication in the e-commerce environment. It's no longer that black and white.

The boundaries between the accountholder being present or being remote to conduct a payment are now blurred. For example, remote payments are happening in the face-to-face environment through in-app purchases. As a result, payments will increasingly be based on a digital account rather than the physical card – which is why you will hear us use the term 'accountholder' instead of cardholder more and more. This blurring of boundaries introduces a new paradigm in how we must protect payments, but it's always based on the fundamentals of Visa's multiple layers of security, designed to work together to ensure payments are reliable, secure and convenient. This is critical to maintaining and strengthening consumer trust in every transaction.

This plan outlines Visa's evolved security roadmap, and is focused on four strategic pillars:

1. **Devalue data** by removing the sensitive data from the ecosystem and making stolen account details useless.
2. **Protect data** by implementing safeguards to protect personal data as well as account details.
3. **Harness data** by identifying potential fraud before it occurs and increase confidence in approving good transactions.
4. **Empower everyone,** including accountholders and merchants, to play an active role in securing payments.

Changing Fraud Landscape

For nearly 60 years Visa has worked collectively with the industry to bring fraud down and keep it down.

Technology has played a large part in that decline – from online authorisations to the global adoption of chip. While fraud remains low, the global fraud mix continues to shift to the Card Not Present (CNP) channel, which is fraud conducted on transactions that have taken place over the phone or online.

In 2016:

CNP fraud accounted for 78%

of all fraud perpetrated on Australian accounts.[1]

81% of fraud losses at Australian merchants

were perpetrated in the CNP channel, with 74% of these losses occurring on Australian-issued accounts (domestic fraud).[2]

1, 2 Australian Payments Network, 2016 calendar year: http://www.apca.com.au/payment-statistics/fraud-statistics/2016-calendar-year

Roadmap

Visa's Future of Security Roadmap: Australia

Objective: Drive security across the payments ecosystem. We are guided by the principle of responsible innovation: optimising the balance between risk and innovation.

2017

Commence education on 3-Domain Secure 2.0 (3-DS 2.0)

Publish standards for biometrics (CDCVM)

Drive early adoption of credential-on-file (COF) tokenisation

2018

Achieve 100% EMV chip acceptance

Begin 3-DS 2.0 implementation

Continue to utilise learnings from ongoing PIN on Mobile pilot to inform global standards

2019

Drive merchant enrollment in 3-DS 2.0

Mass adoption of credential-on-file (COF) tokenisation

2020 +

Achieve 100% tokenisation of all accountholder data held outside of financial institutions

Harness Data

3-Domain Secure 2.0

Where we are now

3-Domain Secure (3-DS) is a tool that enables consumers to directly authenticate their account with their financial institution when shopping online. The objective of 3-DS is to improve security by preventing unauthorised use of online accounts.

To date, 3-DS has had a very low rate of merchant adoption in Australia due to friction in the online shopping experience. Addressing this is a good example of what we mean by responsible innovation: Enhancing security but in a way that empowers consumers and improves the overall payment experience.

Where we're going

To achieve this, a new version of the 3-DS specifications has been published by EMVCo. The new version enables accountholders to more easily authenticate their identity in real-time, offering a balance of greater data exchange between merchants and financial institutions, and convenience for consumers.

2017: Commence education

2018: Begin implementation

2019: Drive merchant enrollment

EMVCo

EMVCo exists to facilitate worldwide interoperability and acceptance of secure payment transactions. EMVCo's work is overseen by its six member organisations including Visa and is supported by dozens of banks, merchants, processors, vendors and other industry stakeholders.

Harness Data

Biometrics

Where we are now

Mobile-initiated payments are ideal for incorporating a wide range of biometrics (e.g. voice, face, fingerprint, iris), given the ubiquity of smartphones and the ease of implementation for both in-store and in-app payments. The promise of eliminating passwords in exchange for a more convenient biometric solution addresses a universal problem shared by nearly all consumers.

Where we're going

The consumer device cardholder verification method (CDCVM) supports this innovation, allowing accountholders to self-validate transactions using their mobile phone or other device. CDCVM captures the cardholder verification method (CVM) on a mobile payment device, allowing a customer to verify quickly and securely that they are the legitimate user.

This is an exciting addition to secure the future of commerce. Visa is not selecting or actively promoting a single type of biometric, but we are working with industry associations such as the Fast Identity Online (FIDO) Alliance to certify products for biometric authentication.

2017: Standards published

2018 onwards: Continued collaboration with financial institutions and partners to enable CDCVM in Australia

Devalue Data

Tokenisation

Where we are now

In 2013, Visa helped to lead the global industry collaboration on payment tokenisation and was integral to the development of the EMVCo tokenisation specifications. Tokenisation is an industry-wide initiative that brings an added layer of security to mobile and digital payments – taking sensitive data out of the commerce ecosystem, preventing cross channel fraud without adding friction to the shopping experience. The security objective of any tokenisation process is to replace accountholder information such as account numbers and expiration dates with a unique digital identifier (a "token"). Such a token can be unique to a device, wallet provider or use case, such as credential-on-file.

Where we're going

Visa has deployed token services in Australia supporting mobile banking wallets, Apple Pay, Samsung Pay and Android Pay. We also have a roadmap to support credential-on-file, wearables and the internet of things. In 2017, we enabled tokenisation on the Visa Checkout platform – Visa's credential-on-file checkout solution. We have also made Visa Token Service Application Programming Interfaces (APIs) available in Visa Developer – a platform of APIs that anyone can access: https://developer.visa.com/.

Tokenisation is part of the CNP Fraud Roadmap of the Australian Payments Network. Visa actively participates in this program with the aim of ensuring all account data held outside of financial institutions is tokenised by 2020.

Credential-on-file

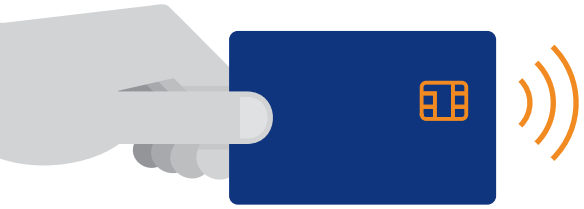
Growth in digital commerce and the emergence of new business models have led to an increase in consumer transactions where accountholders' payment credentials (e.g. account number or token) are held on file with a merchant, digital wallet provider or other service provider, so that those credentials can be used seamlessly for future transactions.

2017: Drive early adoption of credential-on-file (COF) tokenisation

2019: Mass adoption of COF tokenisation

2020+: Achieve 100% tokenisation of all accountholder data held outside of financial institutions

Devalue Data



EMV Chip Technology

Where we are now

The introduction of chip technology (EMV) enhanced security and paved the way for innovations like contactless and mobile payments. Chip cards generate a unique one-time code each time they're used in-store at a chip-activated terminal. This feature is virtually impossible to duplicate thereby preventing counterfeit fraud.

Where we're going

We are working with our financial institution and merchant partners to achieve 100% EMV-enabled terminals, ATMs and accounts issued in Australia.

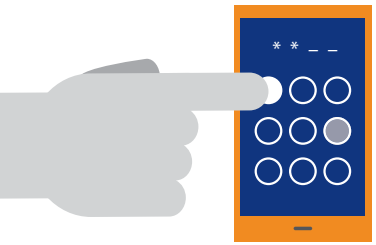
2018: Achieve 100% EMV chip acceptance

Visa's Zero Liability Policy

All Visa transactions today are safeguarded through Visa's Zero Liability Policy,[3] which protects Visa accountholders from being liable in the event of fraud.

3 Visa's Zero Liability policy covers Australia and New Zealand-issued cards and does not apply to ATM transactions, transactions not processed by Visa or certain commercial card transactions. Cardholders should notify their issuer promptly of any unauthorized Visa use. Please consult your issuer for additional details.

Protect Data



Expanding Mobile Acceptance

Where we are now

Mobile devices, including smartphones and tablets, with specialised attachments (e.g. dongles) that can accept payments have recently entered the market. This technology is known as mobile point of sale or 'mPOS'.

mPOS helps extend the benefits of electronic payments to small and micro merchants by providing secure, low cost payments acceptance infrastructure.

As mPOS has evolved, new solutions have emerged supporting the entry of PINs directly onto the smartphone or tablet. These solutions are referred to as Software-Based PIN Entry on Consumer-Off-The-Shelf devices, commonly known as 'PIN on Mobile'.

Globally, and in Australia, mPOS devices are growing in popularity and as such, Software-Based PIN Entry is becoming more commonplace.

Where we're going

Software-Based PIN Entry necessitates a change in how PIN security is managed. Traditionally, PIN security has been governed via hardware, but with new technology such as mPOS, we need to also consider software-based security standards for PIN.

In 2015, Visa first developed standards for Software-Based PIN Entry and launched a pilot with partners in early 2016 to monitor the security performance of this technology. As a member of the Payment Card Industry Security Standards Council (PCI SSC), we shared these standards and learnings for industry review and use.

Recently, PCI SSC completed a feasibility study on its own and is now proceeding with the development of global standards.

2015: Pilot Standards published

2016: Pilot launched

2017 onwards: Continued collaboration with the PCI Security Standards Council

Empower Everyone

Additional Tools for Enhancing Security

Mobile Geo-location

Suspicious transactions are normally declined in order to prevent fraud, however not all these transactions are fraudulent. To prevent fraud but also unnecessary declines, **Visa's Mobile Location Confirmation** provides real-time geo-location intelligence about enrolled accountholders. It makes it possible to determine if the accountholder's device is proximate to the merchant location. With this technology, financial institutions can more confidently approve good transactions, helping to provide a seamless consumer experience as well as save operational costs associated with incorrect declines and pre-travel notification calls. Mobile Location Confirmation APIs are available in Visa Developer.

Transaction Controls and Alerts

Growing consumer preference for self-service banking and control over the way they pay has led to the creation of **Visa Transaction Controls**, where accountholders can define spending limits, impose channel restrictions (e.g. no e-commerce), prohibit international transactions or temporarily suspend their account if their card is ever misplaced, lost or stolen. Transaction Controls increase account security and help customers to better manage their account spending, while building trust and account preference. It is made available to customers through their financial institutions.

Visa's financial institution partners can also enable consumers to improve control and management of their expenses through **Visa Transaction Alerts.** Transaction alerts give accountholders a near real-time view of the transactions conducted on their enrolled Visa accounts, allowing them to catch fraudulent activity early. Accountholders can select the types of alerts and the threshold settings that will trigger personalised notifications to them via email and SMS. Visa's Transaction Controls and Transaction Alerts APIs are available in Visa Developer.

Call to Action

Visa collaborates with its partners, industry stakeholders, policymakers, law enforcement and consumers to keep payments secure and prevent fraud. We deploy a multi-layered security approach that has kept fraud rates low, despite significant growth in electronic payment volumes. However, we all have a shared responsibility to continue to secure the commerce ecosystem.

Here's how you can help.

Consumers

- Make use of security features from your financial institution such as alerts and mobile location controls. Read all security tips available
- Avoid exposing personal and payment data in insecure networks, public Wi-Fi and unknown apps

Third Party Providers

- Ensure validation of compliance with PCI DSS across all environments storing, processing or transmitting Visa account data
- Register with Visa as a Third Party Agent. Compliant providers are included on Visa's Global Registry of Service Providers at www.visa.com/onthelist

Merchants

- Ensure 100% of terminals are EMV chip enabled terminals
- Enable tokenisation
- Implement risk-based solutions to manage fraud, such as 3-DS 2.0
- Comply with current versions of PCI DSS and all other applicable security requirements
- Use Visa-registered providers for payments acceptance and fraud management
- Get educated and act on security tips to protect from fraud

Acquirer Bank

- Provide guidance and education to merchants on best practice payment security measures
- Enable credential-on-file tokenisation and processing
- Work with merchants to eliminate sensitive data and move to tokenised transactions
- Register all Third Party Providers handling Visa account data on their or their merchants' behalf

Issuer Bank

- Protect accountholder data with tokenisation and 100% EMV chip cards
- Provide guidance and education to accountholders on best practice payment security measures
- Provide banking apps with optional security features (e.g. alerts, transaction controls, mobile location)
- Enrol accountholders on the newest one-time risk-based authentication services
- Ensure minimum requirements for innovation in payments

Law Enforcement

- Drive awareness of new fraud trends in the payments industry
- Work with the industry to combat fraud


VISA