Visa's Future of Security Roadmap: The South Pacific

Contents

Disclaimer

Executive Summary

Together with our partners and by drawing on the strength of our global expertise gained over six decades – Visa is proud to deliver, for the South Pacific, its Future of Security Roadmap.

For 60 years Visa has been a leader in payments security. 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 without the other. This is why at Visa we continue to invest to drive security across the payments ecosystem, while improving the payments experience for consumers.

Visa has worked with our industry partners on delivering targeted security initiatives across the South Pacific Region, primarily focused on the adoption of EMV® chip technology which is less attractive to criminals, and Payment Card Industry Data Security Standard (PCI-DSS) compliance.

These are both critical steps to enabling contactless technology – the gateway to innovative payments technology which enable consumers to pay using mobile and wearable devices.

Executive Summary

Contactless technology will boost the region's thriving tourism sector, estimated to generate over $US3billion annually.

Australian and New Zealand visitors account for a 52% share of the total tourist arrivals[1], and these countries rate as among the highest for consumer uptake of contactless.

With more than four million mobile subscribers in the South Pacific Region, more than 18,000 contactless enabled Point of Sale terminals and three million annual visitors, the region requires a solid plan to ensure innovative, convenient and secure payments for locals and visitors alike.

Foundational to the security of contactless payments into the future is tokenisation – a process which removes sensitive data from the payments ecosystem and replaces it with a unique digital identifier (a 'token').

We've come a long way in just a few short years. Together we have made great strides in driving EMV® Chip issuance and terminalisation, PCI-DSS compliance, Verified by Visa adoption and we have collaborated on a number of other initiatives to enhance industry-wide security.

These solutions are focused on securing payments using technology specific to the environment, like chip technology in the face-to-face environment or secondary authentication in the e-commerce environment. The boundaries of commerce have blurred between face-to-face, in-app and online purchasing. This is why Visa believes it is so necessary to support, and be part of, a robust payments ecosystem.

This Future of Security Roadmap is focused on four strategic pillars:

1. Devalue data by removing the sensitive data from the ecosystem and making the remaining data useless if stolen.

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 genuine transactions.

4. Empower everyone, including accountholders, third party providers and merchants, to play an active role in securing payments.

Visa's Zero Liability Policy

Consumers can transact on their Visa cards with confidence as their transactions are safeguarded through Visa's Zero Liability Policy*, which protects Visa accountholders from being liable in the event of fraud.

*Visa's Zero Liability policy covers South Pacific-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.

1 South Pacific Tourism Organisation, Annual Review 2016

Roadmap

Visa's Future of Security Roadmap: The South Pacific

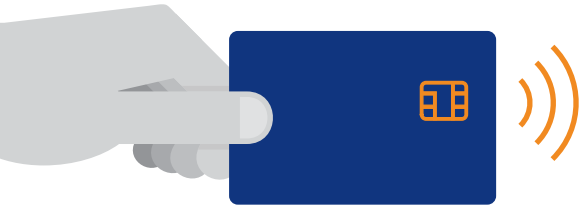
Objective: Drive security across the payments ecosystem. We are guided by the principle of responsible innovation: optimising the balance between risk and innovation.

Existing	2019	2020
Progress chip issuance and acceptance, including latest contactless specification (VCPS 2.1.3 or above), enabling biometric authentication through Consumer Device Cardholder Verification Method (CDCVM)	Compliance to Visa Rules requiring 100% chip issuance and acceptance	Issuers support 3-D Secure 1.0 and EMV® 3-D Secure (2.0) specifications Merchants consider support of EMV® 3-D Secure (2.0) as part of their fraud management suite of tools

Foundational elements:

PCI-DSS compliance • Real time fraud monitoring solution • Tokenisation is foundational for the future

Devalue Data



EMV® Chip Technology

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

2018

Progress Chip issuance and acceptance, including support for the latest contactless specification (VCPS 2.1.3 or above)

2019

Compliance to Visa Rules requiring 100% chip issuance and acceptance

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.

Devalue Data

Tokenisation

In 2013, Visa helped to lead the global industry collaboration on payment tokenisation and was integral to the development of the EMV® Payment 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 and 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.

> Tokenisation is part of Visa's long-term strategy of securing digital payments with the aim of ensuring all account data held outside of financial institutions is tokenised.

Protect Data

PCI-DSS Version 3.2.1

PCI-DSS compliance is the foundation of Visa's Data Security and Compliance programs and is critical to protecting sensitive accountholder data from compromise.

PCI-DSS sets minimum technical and operational requirements to help organisations - merchants, financial institutions, payment processors, service providers and technology providers – keep their defences primed against attacks aimed at stealing accountholder data.

The PCI-DSS is routinely updated to provide clarifications on new requirements and address emerging threats to payment information. Companies that store, process or transmit accountholder information should ensure compliance with the most current version of PCI-DSS to prevent, detect and respond to attacks that can lead to breaches.

Harness Data

Real Time Monitoring System

> As the card business has matured, so have fraudsters' techniques. This means issuers and acquirers have to constantly review and improve their fraud management capabilities.

Having the right fraud prevention tool allows issuers and acquirers to reduce fraud losses and increase authorisation throughput by improving fraud detection and confidently approving low-risk transactions.

Fraud prevention tools are a key component of an issuer's and acquirer's risk management strategy, and fostering consumer confidence in the payments system expands Visa card use for point-of-sale, e-commerce and mobile payment transactions.

Harness Data

3-Domain Secure 2.0

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 Visa accounts online.

Visa developed the original version of 3-DS in 1999, however technology in payments has advanced significantly since then. As a result, 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.

- **2020**

  Issuers support 3DS 1.0 and EMV® 3-D Secure (2.0) specifications. Merchants consider support of EMV® 3-D Secure as part of their fraud management suite of tools.

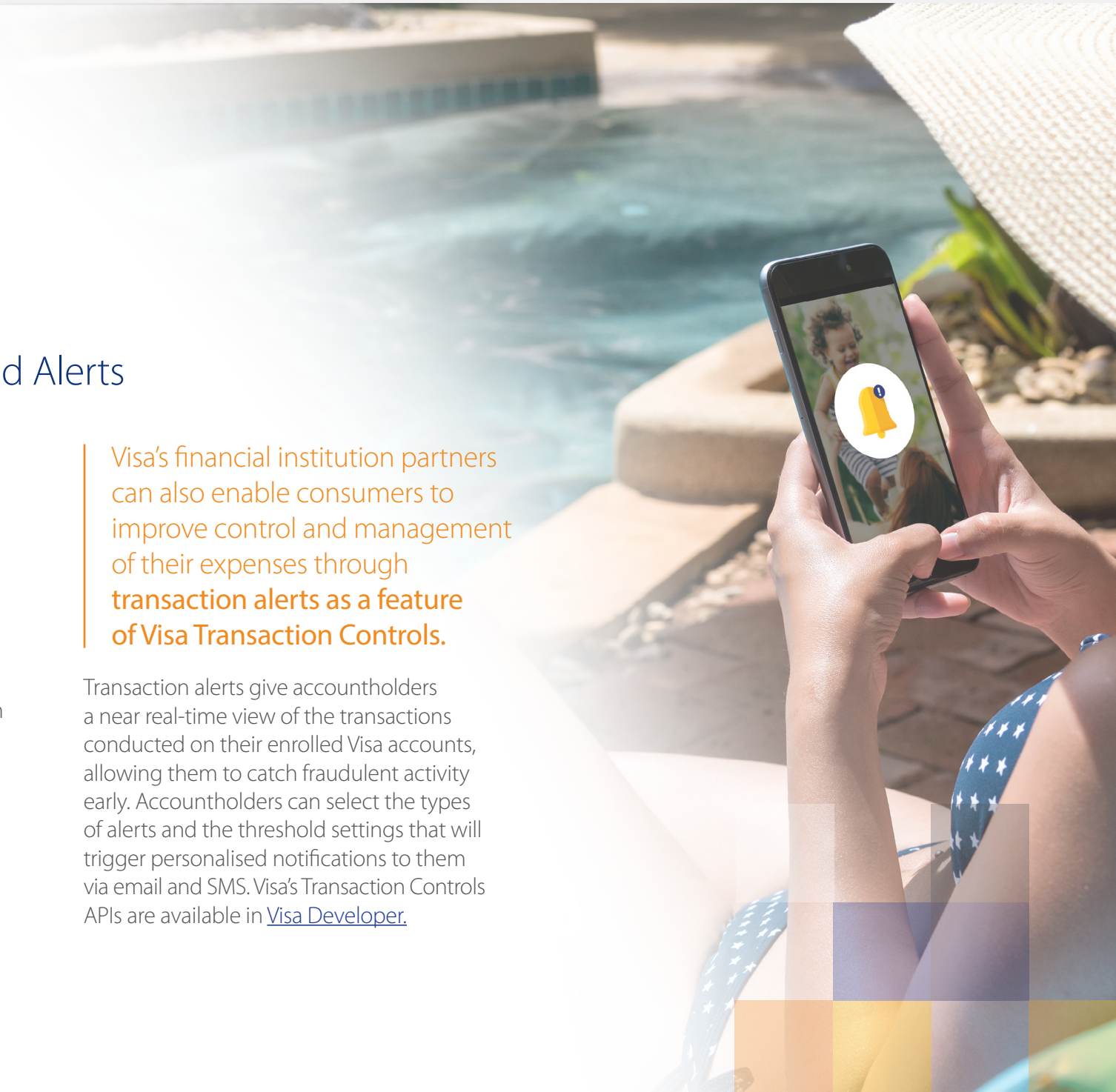
Empower Everyone

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 **transaction alerts as a feature of Visa Transaction Controls.**

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 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.

Contact us to discuss how we can work together to secure the payments ecosystem.

Andy McCowan
Head of South Pacific
+64 21 582 112
amccowan@visa.com

David O'Brien
Head of Visa Merchant Sales & Acquiring
+64 21 525 415
obriend@visa.com


VISA