SECURING THE COMMERCE ECOSYSTEM

in Australia

VISA

Contents

Visa Security Roadmap 2021-2023

2021

Program changes to incentivise adoption of tokenisation and EMV® 3DS

Best Practices to prevent Enumeration Attacks

Payment Intelligence sharing on indicators of compromise

VisaNet ecosystem resilience capabilities

2022

Performance frameworks effective for tokenisation and EMV® 3DS

Anti-enumeration requirements come into effect

Payment Card Industry Data Security Standard **(PCI DSS) v4 released**

2023 AND BEYOND

Support for contactless ATM access on Visa cards

Visa will continue to publish best practices and intelligence alerts as the threat landscape continues to evolve.

Executive Summary

As the trusted engine of commerce, Visa's mission is to connect the world through the most innovative, reliable and secure payment network – enabling individuals, businesses and economies to thrive.

We are a network working for everyone, facilitating digital payments across more than 200 countries and territories among global consumers, merchants, financial institutions, businesses, strategic partners and government entities through innovative technologies. At Visa, we are focused on understanding the unique needs of everyone engaged in commerce, then designing solutions that open doors to new possibilities for all. Our advanced global processing network, VisaNet, is capable of handling more than 65,000 transaction messages a second and we are committed to delivering leading-edge emerging technologies and state-of-the-art security that enable the secure movement of money.

As a global leader in the payments industry for over 60 years, Visa continues to be at the forefront of innovation and security. Fraud rates are at an all-time low globally and in Australia have been on a steady decrease for the past several years.

Card fraud in Australia increased by

0.6%

in calendar year 2020 to AU$467.6M, driven by a 3.8% increase in Card Not Present (CNP) fraud, which accounts for 87% of fraud losses[1].

Overall growth in spend in this CNP channel far outweighed the growth in fraud, with an increase in online spend at

44%

in 2020[2].

Visa's Artificial Intelligence (AI) technology has helped prevent over

$350M

in fraud from impacting Australian businesses in the past year[3].

1 AusPayNet Payments Fraud 2021, Fraud Statistics Jan 2020-Dec 2020 https://auspaynet.com.au/resources/fraud-statistics/2020-Calendar-year
2 NAB Online Retail Sales Index: December 2020 https://business.nab.com.au/nab-online-retail-sales-index-december-2020-44500/
3 12 months ending 30 April 2021, VisaNet, May 2020 – April 2021

The COVID 19 pandemic has had a significant impact on how Australian consumers and businesses pay and are paid for goods and services.

The accelerated shift to digital payments has driven changes in behaviour and preferences that are likely to continue well beyond the pandemic. But as these digital habits have taken hold, fraudsters have also adapted their attack vectors to take advantage of these changes and to further scale existing threats.

Visa's latest Security Roadmap outlines the steps Visa has taken and will be taking into 2022 and beyond across six key areas to continue to secure digital payments:

1

Driving adoption of secure technologies

2

Securing digital first payment experiences

3

Ensuring ecosystem resilience

4

Preventing enumeration attacks

5

Enhancing the cybersecurity posture of ecosystem participants

6

Preventing Australian consumers and businesses from becoming victims of scams

The Journey

Since Visa launched our previous Future of Security Roadmap in August 2017, the payments landscape in Australia has changed significantly. We are proud that, alongside our payment system stakeholders, Visa has achieved what we set out to deliver.

The 2017 Security Roadmap set out to advance the instances of acceptance that had not yet migrated to EMV® chip technology for face-to-face payments and outlined the foundational requirements for adoption of a new standard for authentication for online and mobile purchases, as payments have increasingly become digital.

- Visa actively worked with acquirers to migrate remaining merchant terminals and unattended parking meters, vending machines and ticketing machines to EMV® chip acceptance and ensure they were on the latest contactless specification that set them up to accept biometric authentication in lieu of PIN for transactions above $100.
- Visa worked closely with participants in the ecosystem to enable 100% of eligible issuing products to use the **EMV® 3-D Secure (EMV® 3DS)** standard, which enables seamless and secure ecommerce checkout experiences for Australian consumers and businesses.
- Through our leadership in EMVCo, Visa has ensured the new EMV® 3DS standard has been modernised to provide a better authentication experience for online shopping by moving away from static methods of authentication and enabling the mobile shopping experience.

What is 3-D Secure?

3-DS is a global industry protocol that provides the mechanism for cardholder authentication at the time of an eCommerce purchase. Visa, as a leader in payment security, is focused on providing best-in-class certified solutions that utilise this protocol.

One of the primary benefits of the EMV® 3DS is the increased data elements that allow for authentication based on this data, or frictionless flow, without the need to ask for further details from the consumer, for example, a one-time password.

With more online businesses in Australia using the new protocol each month, authorisation rates grew by 3-5%[4] on authenticated ecommerce vs. unauthenticated ecommerce and cart abandonment rates are now as low as 5%.

The prior roadmap also introduced the concept of "Responsible Innovation" which is how we optimise the balance between risk and innovation. In particular, through this lens, we focused on challenging traditional methods of authentication using a static PIN for a face-to-face chip transaction by updating our standards to allow for biometric authentication, for example through voice, face, fingerprint or iris. Visa focused on ways to securely replace the static PIN data that can be stolen in the mail or even forgotten, with a biometric – something that is inherent to a user. 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.

We also applied responsible innovation to expanding acceptance outside of a traditional payment terminal to a consumer-grade mobile device. Since 2017, when we introduced our minimum standards for biometric authentication on mobile wallets, Visa has seen more wallet providers attest to our standard and this has been foundational for the secure growth in mobile wallet transactions taking place in Australia.

On the acceptance side, the specifications for software encryption for PIN security was the foundation for the Software-based PIN on Consumer Off the Shelf (COTS) (SPoC) standard that the **Payment Card Industry Data Security Standard (PCI DSS)** published in January 2018. Since then, PCI DSS has also published a Contactless PIN on COTS standard, which leverages the NFC capabilities of an Android device as an additional way for business to expand acceptance of Visa credentials. Visa leveraged these standards for our Tap to Phone solution, which enables merchants to accept fast, secure payments from any contactless-enabled Visa card, device or wearable, which a customer simply taps to pay against the merchant's smartphone or tablet. Merchants download an app, supported by their acquirer, and after registering and selecting their participating bank, they can start accepting contactless and mobile payments in just a few minutes. Providing the same functionality and security as EMV® contactless, sellers who were limited by the expense and complexity of traditional point of sale (POS) have added flexibility with Tap to Phone.

As we take stock of the evolving payments landscape, new trends have emerged and this latest Security Roadmap outlines the steps Visa will take to lead the industry in driving trusted outcomes for Australian consumers and businesses across six key areas.

PCI DSS explained

The Payment Card Industry Data Security Standards represents a comprehensive set of international security controls for safeguarding payment account data. These set the technical and operational requirements for organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions.

4 VisaNet authorisation requests, includes approvals and declines by transaction count, Visa Secure Authentication requests for 6 months ended June 2021

Investment in secure technologies addresses evolving risks and balances the customer experience

Visa Token Service

When Visa first introduced tokenisation as a capability, one of the main drivers was to protect against a data compromise. By replacing the 16-digit account number with a 16-digit token that is bound to a channel and token requestor, the risk of that token being used for fraud is effectively addressed.

As the shift to digital commerce and experiences has driven massive adoption of tokens through Visa Token Service (VTS) with more than 2 billion tokens[5] issued, the secure foundations of this technology have also added some clear benefits to the consumer experience. These include:

- improving the checkout experience for online retailers who participate in Click to Pay; and
- ensuring a Visa cardholder's recurring payments continue when a new Visa credential is reissued – thus minimising lost sales for merchants due to lost cards or expiry dates.

What is Click to Pay?

Built on the EMV® Secure Remote Commerce (SRC) industry specification, click to pay enables shoppers to speed through the checkout process by eliminating the need to manually key-in personal account numbers and passwords. Click to pay is designed to be as easy and consistent an experience as when consumers tap to pay in a physical store. When click to pay is combined with Visa Token Service, it replaces the storage of Primary Account Numbers (PANs) and can help reduce fraud, as well as decrease the impact of merchant data breaches.

Tokens will be the standard through which we participate in ecommerce and POS-based transactions, digital currency and cloud-based payments in the future.

Visa believes that the strength of the entire ecosystem amplifies as all participants lift their standards for network performance and deploy new capabilities as they become available. It is important that we as an ecosystem move in unison to adopt standards and capabilities that set us all up to participate in the opportunities that lie ahead.

5 Visa Token Service Factsheet April 2021 https://usa.visa.com/content/dam/VCOM/global/products/documents/visa-token-service-fact-sheet-april-2021.pdf

EMV® 3-D Secure

In the prior roadmap we introduced the new EMV® 3DS specification that is the basis of the Visa Secure solution for authentication. As Visa issuers in Australia have enabled Visa Secure, the benefits of the additional data available to authenticate an online transaction have been realised. Domestic transactions have experienced an uplift in approval rates and a reduction in fraud. In addition, the Non-Payment Authentication feature to authenticate a Visa cardholder outside of the transaction has proven useful in cases such as ride hailing and fuel dispensing where the transaction occurs after the goods or services are provided.

Visa has announced our plans to sunset 3-D Secure version 1 by October 2022, as EMV® 3DS has scaled globally and offers a better customer experience for authentication during online shopping.

After this date, merchants will not be able to use 3DS version 1 for authentication. Solution providers will need to work with their merchants who are using the legacy protocol to migrate them to an EMV® 3DS solution before October 2022 to gain the benefits of using an additional method to authenticate their customers for online and mobile purchases.

Secure digital experiences are the new normal

With cash in Australia expected to account for only 2.1% of sales at the point of sale by 2024[6], digital payment experiences will drive how Australians pay and are paid for goods and services well into the future.

As tokenised Visa credentials can be used to bind a device and a token, issuers can offer their customers instant access to a new or replacement digital Visa card for immediate use. Digitally savvy customers can even take advantage of transaction controls and alerts as part of the set up of their digital card, making them empowered stakeholders in the process. Another benefit of a digital card is that there is no risk of the card being lost or stolen, which accounts for most of the fraud in the face to face to environment.

Visa has also recently announced that by October 2022, newly-issued or replacement contactless cards and contactless payment devices must be configured to support contactless ATM transactions and by October 2030, this requirement will apply to all contactless cards and contactless payment devices. Removing the need for a physical card to be inserted at an ATM will address the risk of skimming that occurs, with fraudulent spend at other locations subsequent to the magnetic stripe data being compromised. **In calendar year 2020, counterfeit/ skimming fraud accounted for $11.1 million[7].**

This change will make it more prevalent for issuers to enable mobile wallets to be used at the ATM, removing the need for the physical card to access cash.

Global standards are the backbone of the payments industry. They both enable interoperability and scale, and are often developed in response to emerging risks. As more experiences shift to digital and we see authentication becoming a target for fraudsters as part of account takeover and fraudulent application attempts, Visa reiterates the importance of how to secure digital experiences that are tied to a payment credential in a secure manner whilst maintaining a frictionless user experience to foster digital trust. With Australia's Consumer Data Right (CDR) gaining momentum and more data requestors and data holders being accredited, authentication and consent will become central to the use cases for which Australians will leverage the CDR.

The **Fast Identity Online (FIDO) Alliance** is an open industry association with a focused mission on developing authentication standards to help reduce the world's over-reliance on passwords. As a Board-level member of FIDO, Visa works across the payment industry and alongside other technology leaders to develop standards that enable biometric authentication wherever a consumer is asked to identify themselves online. Thinking of responsible innovation and how Australian consumers and businesses may avail themselves of the benefits promised by the CDR, leveraging standards like FIDO for authentication should be at the forefront of the providers developing those solutions to balance the security and frictionless experience of their customers.

About FIDO Alliance

The FIDO Alliance promotes the development of, use of, and compliance with standards for authentication and device attestation. The FIDO Alliance is working to change the nature of authentication with open standards that are more secure than passwords and SMS one-time passwords, simpler for consumers to use, and easier for service providers to deploy and manage.

6 FIS Global Payments Report March 2021 https://worldpay.globalpaymentsreport.com/en/
7 AusPayNet Payments Fraud 2021, Fraud Statistics Jan 2020-Dec 2020 https://auspaynet.com.au/resources/fraud-statistics/2020-Calendar-year

The ecosystem's resilience is only as strong as its weakest link

Maintaining trust in the payments ecosystem requires continued investment in technologies that ensure availability and uptime across multiple stakeholders in the transaction lifecycle. Visa's technology platform comprises software, hardware, data centres and a vast telecommunications infrastructure, each with a distinct architecture and operational footprint wrapped with layers of security and protection technologies. Together, these systems deliver the secure, convenient, and reliable service that our clients, partners, consumers and merchants expect of the Visa brand.

All our data centres have high redundancy of network connectivity, power and cooling designed to provide continuous availability of systems. In addition, Visa has requirements in place for any entity directly connected to our network regarding the qualifications of personnel managing these connections along with ensuring the appropriate access controls, records, documentation, and logs are maintained. In the event a Visa issuer is unavailable to respond to authorisation requests, Visa can stand in to respond on their behalf. Last year Visa announced Smarter Stand-in Processing (Smarter STIP)[8] that uses real-time artificial intelligence to help financial institutions manage transaction authorisations when service disruption occurs.

Using deep learning to analyse past transactions, Smarter STIP generates informed decisions to approve or decline transactions on behalf of issuers if their systems go offline.

About Smarter STIP

Visa's Smarter STIP service builds on Visa's existing STIP capability by using deep learning to analyse past transactions down to the cardholder level. Thus the transaction decision that Smarter STIP provides is based on unique insights derived from the cardholder's past purchasing behavior, rather than solely on static rules applied across an entire card portfolio. With this added intelligence, Visa is able to provide a transaction decision on the issuer's behalf that more closely mirrors the issuer's own decision making process to help financial institutions manage transaction authorisations when service disruptions occur.

8 Visa Harnesses Real-Time Deep Learning to Enhance Transaction Processing, August 2020
https://investor.visa.com/news/news-details/2020/Visa-Harnesses-Real-Time-Deep-Learning-to-Enhance-Transaction-Processing/default.aspx

Enumeration attacks increasingly impact Australian merchants and issuers

Where we are now

One of the threats to emerge in the past 12-18 months is enumeration attacks.

An enumeration attack occurs when criminals target online retailers with scripted attacks that send thousands of low value transaction attempts with the aim to get an approval on a valid account number, expiry and CVV2 combination. These attacks generally lead to compromised accounts and account takeovers. However, the residual aspects of these schemes, while not always conspicuous, have additional negative effects on various ecosystem parties. These impacts include fees, operational inefficiencies, fraud and reputational risk for all parties involved.

At Visa, we take enumeration very seriously by investing in technology to inform, block and identify these attacks in flight. An example of this is Visa's Risk Operations Centre (ROC) – a 24/7, real-time fraud detection and mitigation system operated by our team of fraud and security experts. ROC analyses millions of transactions every day for known and emerging fraud threats.

Our capabilities are integrated with advanced Visa Account Attack Intelligence (VAAI) to identify and report enumeration quickly. VAAI uses machine learning to identify and score every Card Not Present (CNP) transaction processed through VisaNet, detecting these attacks.

However, we cannot prevent these fraud attacks alone. We need all stakeholders in the transaction lifecycle to employ anti-enumeration capabilities and account testing best practices, upgrade their infrastructure and continue investing in fraud management. Visa has also published best practices for merchants on what they can do to guard against these attacks, as well as some guidance on what issuers of Visa credentials could do to reduce the impact of enumeration.

Where we're going

As the threat of enumeration is expected to continue, Visa is introducing a requirement for ecommerce payment providers to ensure they invest in capabilities to identify and prevent enumeration attacks, effective October 2022.

Acquirers will need to be aware of the new rule and ensure that if they are the closest to the seller's payment page, they have the appropriate controls in place to identify, prevent and disrupt these attacks. If they work with Payment Gateways or Independent Solution Vendors, acquirers will need to ensure that these entities closest to the seller's payment page have the appropriate controls that meet Visa's requirements. Acceptable solutions include anomaly detection on authorisations, IP addresses, log ins or sessions, throttling or random pause on account checking and the ability to lock accounts after a certain number of log in attempts. For more details on the types of anti-enumeration capabilities available, please consult our best practices for merchants.

Visa will continue its monitoring of enumeration attacks impacting the payment system and our analysis will identify acquirers with merchants and/or third-party providers that continue to have a significant number of merchants driving enumeration attacks, indicating they have not made the necessary investments in accordance with our requirements. In the future, Visa may implement a compliance program to formally identify these outliers and work with them on an approach that benefits all payment system participants.

Cyber attacks are big business

Where we are now

In the past year we've seen cyber incidents impact supply chains and infrastructure, governments, and large and small businesses in varying parts of the world. The nature and global reach made possible by our highly connected world, continue to keep cybersecurity a top concern for both the public and private sectors.

In 2020, 80% of breaches globally were executed by organised crime, with the two most common targets being bank account and card data[9].

In the first half of 2021, malicious or criminal cyber attacks remain the leading source of data breaches in Australia, accounting for 65% of notifications under the Notifiable Data Breach Scheme, with ransomware incidents increasing by 24%[10] from the prior six-month reporting period. Ransomware attacks and data breaches of supply chain vendors increased over the past year and sufficient protection of third-party service providers and supply chain vendors is increasingly critical in the Australian context.

Where we're going

Visa routinely identifies cyber threats to the ecosystem and updates our clients and the public through security alerts, intelligence alerts and our biannual threats report.

These publications include indicators of compromise along with best practices and recommendations to identify, prevent and remediate cyber threats. Whether it's ransomware, eSkimming, Distributed Denial of Service (DDoS) attacks, or changes in the cybercrime underground, basic data security hygiene is underpinned by global standards. The PCI DSS sets the technical and operational requirements to help organisations - merchants, financial institutions, payment processors, service providers and technology providers – keep their cyber defenses primed against attacks aimed at stealing cardholder data. As these trends evolve, so too does the PCI DSS, with the latest version 4.0 expected to be published in early 2022[11].

One of the primary changes we expect with version 4.0 is flexibility and support for additional methodologies to achieve security objectives outlined in the 12 core PCI DSS requirements. The change in approach to become compliant is based on industry feedback and seeks to support organisations as they use a broad range of controls and methods to meet the security objectives set out by the standard. As part of PCI's timeline, training to industry participants, especially Qualified Security Assessors, will become increasingly important in balancing the flexibility of the new approach related to alternate validation and maintaining the spirit of the requirements in securing the payments ecosystem.

In addition to the flexibility in the validation approach, PCI DSS is also making some changes related to multi-factor authentication requirements taking into consideration National Industry for Standards and Technology (NIST) Multi-Factor Authentication (MFA)/password guidance, monitoring requirements given advances in technology and broader applicability for encrypting cardholder data on trusted networks. Once version 4.0 is published, Visa will announce our timelines for ensuring compliance with the new standard to applicable payment system participants.

9 Verizon 2021 Data Breach Investigations Report www.Verizon.com/dbir
10 OAIC, Data breach report highlights ransomware and impersonation fraud as concerns, 23 August 2021 https://www.oaic.gov.au/updates/news-and-media/data-breach-report-highlights-ransomware-and-impersonation-fraud-as-concerns/
11 Updated PCI DSS v4.0 Timeline https://blog.pcisecuritystandards.org/updated-pci-dss-v4.0-timeline

Scams outpace the growth of fraud

Where we are now

Whilst card fraud in Australia has grown by less than 1% based on AusPayNet fraud data[12], scams impacting Australian consumers and businesses have been on the rise over the past two years.

Fraud occurs when a third party obtains unauthorised access to a consumer or business's payment credentials typically through a data compromise. A scam, on the other hand, occurs when a consumer or business owner is misled to provide their payment credentials to someone they believe to be a trusted entity. These credentials are then used to perpetrate account takeovers or for unauthorised payments or transfers. According to the Australian Competition and Consumer Commission (ACCC), Australians reported a record $211 million in losses to scams so far this year, an 89 per cent increase compared to the same period last year[13].

Visa's existing processes and rules aim to prevent the Visa system from being used by scammers to monetise credentials.

Visa maintains the Global Acquirer Risk Standards (GARS) that outline requirements for acquirers to manage the risks to their business and the greater ecosystem across onboarding, monitoring and working with third parties. This includes capabilities to identify merchants who may be driving scam activity or even when their merchants have become victims of scams. For investment related scams in particular, issuers may be able to use Dispute Code 13.5 Misrepresentation in the event their customer is not able to withdraw funds to which they are entitled.

Visa's global fraud and dispute monitoring programs will help to identify and remediate any outlier merchants that may be driving these scams or where fraud because of scam activity is occurring.

Where we're going

Despite these controls, Visa recognises that an industry approach through education and awareness is best to help prevent Australian consumers and businesses from becoming victims of scams.

Visa actively works with law enforcement agencies and across industry groups to drive messaging on what to look out for as well as common scams sources through our Payment Intelligence alerts. Consumers and businesses can also stay up to date with the latest updates to protect themselves at visa.com.au.

12 AusPayNet Payment Fraud 2021, Fraud Statistics Jan 2020-Dec 2020 https://auspaynet.com.au/resources/fraud-statistics/2020-Calendar-year
13 ACCC Scamwatch, losses reported between 1 January and 19 September 2021 https://www.scamwatch.gov.au/news-alerts/losses-reported-to-scamwatch-exceed-211-million-phone-scams-exploding

Looking Ahead

As we look to the future and the payments landscape continues to evolve with new technologies, Visa expects the threat landscape will continue to change.

Fraudsters can adapt very quickly, leveraging new technologies to carry out their attacks. As an industry, we need to be just as nimble in disrupting them.

With increased adoption of digital only cards, the safeguards Visa and the industry have worked for so many years to secure the physical card will need to shift. This includes how we think about the static authentication data, especially as it relates to non-reloadable prepaid cards, PINs, and CVV2.

Will these products shift to digital only offerings in the next five years? Or will the industry still see a need to maintain the physical card to ensure interoperability and access?

As sellers are able to adopt mobile technology for secure payment acceptance and the blurred lines between in person and remote payments continue, there may be some consideration given to removing key entry at the point of sale as a legacy mechanism to take mail or telephone orders (MOTO). These transactions typically have a higher propensity for fraud as there is little authentication data passed in such a transaction.

As always, Visa will continue to engage our stakeholders and trusted partners in securing the payment system, as the network working for everyone, to discuss how we can continue to maintain trust and meet the evolving needs of consumers and businesses in how they pay, are paid and move money.

Call to Action

Visa collaborates with its partners, industry stakeholders 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 digital payments. However, we all have a shared responsibility to continue to secure the commerce ecosystem. Here's how you can help.

Consumers

- **Ensure your contact details are up to date** with your bank
- **Enrol in mobile alerts** to take control of how your Visa credentials are used
- **Read the security alerts** provided by your bank and stay up to date with recent scam activities
- **Don't share any sensitive log in or authentication information** with anyone, including someone claiming to be from your bank or another trusted source

Merchants

- **Get educated** on the risks associated with accepting digital payments
- **Talk to your provider** to understand your options to prevent fraud, enumeration, and cyber-attacks. Tokenisation and 3DS are important starting points
- **Implement risk-based solutions** to manage fraud
- **Ensure incident response plans are in place and tested** Review Visa's What To Do If Compromised Guide for further details

Third Party Service Providers

- **Ensure compliance** with the latest PCI DSS for protecting payment data
- **Register with Visa** as a Third Party Agent. Compliant Providers are on Visa's Global Registry of Service Providers at www.visa.com/onthelist
- **Offer fraud and risk management solutions** for payments based on global standards like tokenisation and EMV® 3DS

Acquiring Banks

- **Provide guidance and education to merchants** for best practices on payment security
- **Work with merchants to enable tokenisation** for transactions where the payment credential is held on file with a merchant or other provider use cases
- **Enable merchants on payments solutions based on global standards** like tokenisation and EMV® 3DS

Issuing Banks

- **Provide guidance and education to cardholders** for best practices on payment security and avoiding scams
- **Provide mobile banking apps and digital wallets with optional security features** (e.g. transaction controls, alerts, biometric authentication)
- **Continue to invest in secure technologies** and a layered approach to authentication