Security Roadmap

Australia
2025–2028

Contents

As-Is Disclaimer

Case studies, comparisons, 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. Visa Inc. neither makes any warranty or representation as to the completeness or accuracy of the information within this document, nor assumes any liability or responsibility that may result from reliance on such information. The Information contained herein is not intended as investment or legal advice, and readers are encouraged to seek the advice of a competent professional where such advice is required.

Executive summary

The payments ecosystem has changed more in the past 5 years than in the previous 50.

In a rapidly evolving technological landscape, businesses need to adapt quickly to grow sustainably. This shift isn't just about technology; it's about meeting the new expectations of digital-savvy consumers who seek personalised, convenient and secure experiences. Companies must be quick to respond to new trends and technologies, be it in data analytics or artificial intelligence (AI). This means making strategic investments and ensuring their workforce is skilled to make the most of these tools.

While the democratisation of technology – and most recently AI – has benefited people and businesses, it has also emboldened bad actors. The incentive for criminal activity in the digital domain has never been easier and more enticing than it is today. The consumerisation of cutting-edge technologies and the proliferation of new payment assets have also given rise to a new generation of cyber criminals, where hacking can now be a side hustle.

Executive summary continued

AI is also part of the solution. Visa has pioneered AI models in fraud protection since 1993, and today, our technology platform is among the most powerful examples of the tangible benefits of AI. Visa has over 150 AI and machine learning models in production, powering products that help to solve longstanding challenges and pain points for consumers, merchants and financial institutions.

The development and release of secure technologies, such as tokenisation and authentication, have established a new foundation for digital payments security. This latest Visa Security Roadmap looks at the biggest challenges facing the payments ecosystem in the coming three years and the steps we can take together to minimise the impact on consumers, merchants and other participants.

In this Roadmap we will look at:

- Preventing the growing frequency of enumeration attacks
- Sustaining investment in secure technologies to balance fraud management with improved customer experience
- The shift to a data-driven risk based approach
- Building resilience against unauthorised payments fraud and scams (authorised fraud) in the era of AI
- Enhancing the cyber security posture of ecosystem participants
- Securing the digital payment experience by integrating best-in-class security protocols.

Visa is committed to connecting the world through the most innovative, convenient, reliable and secure payments network, protecting the payments ecosystem and facilitating global commerce for consumers, financial institutions, businesses, fintech partners and government entities.

Our network spans:

MORE THAN
200
COUNTRIES AND TERRITORIES

APPROXIMATELY
14.5k
FINANCIAL INSTITUTIONS

MORE THAN
130m
MERCHANT LOCATIONS

4.5bn
PAYMENT CREDENTIALS

US$15tn
IN TOTAL VOLUME

296bn
TOTAL TRANSACTIONS
in its fiscal year 2023[1]

[1] Visa Fact Sheet, June 2024, https://corporate.visa.com/content/dam/VCOM/corporate/documents/about-visa-factsheet.pdf

The journey

Since the previous two Visa Security Roadmaps for Australia were published in 2017 and 2021, the payments and threat landscapes have transformed significantly.

Visa has worked continuously across the industry to strengthen the ecosystem, with the development and adoption of secure technologies establishing a new standard for online purchases, one that ensures security at every stage of the transaction lifecycle. These developments have included:

Tokenisation – laying foundations for the future

Tokenisation is fast becoming a critical part of secure and user-friendly digital payments, not only protecting payments data but also false declines. The ecosystem has adopted tokenisation through Visa Token Service (VTS), which replaces the 16-digit debit or credit card number with a unique identifier called a token that only Visa can unlock. These benefits, coupled with ease of use across devices, lead to an improved consumer experience and reduction of fraud.

Adoption of secure and seamless authentication

Over the past year, the adoption of EMV® 3DS in Australia has increased by more than 4 times[2]. As the global industry standard for cardholder authentication in eCommerce, EMV® 3DS enables businesses to enhance security while providing a seamless user experience. In response to the evolving threat landscape, there has been a shift away from static authentication and SMS One-Time Passwords (OTPs) toward more dynamic multi-factor authentication strategies, such as biometrics, for stronger security.

Preventing Card-Not-Present (CNP) fraud

We have been vigilant in protecting the ecosystem from large-scale attacks, particularly as Australia continues to be a target for criminals in the Asia Pacific region. This vigilance has led to the introduction of Visa requirements for acquirers to implement risk controls to curb enumeration, the criminal practice where fraudsters use automation to test and guess payment credentials, which can then be used in fraudulent transactions.

Reducing disputes and chargebacks

Visa's introduction of the Compelling Evidence 3.0 rules in April 2023 has helped tackle first-party misuse. 'Friendly fraud', as it's known, occurs when a cardholder disputes a legitimate charge and claims it is fraudulent. The new rules marked a significant step forward in enhancing the integrity of the ecosystem, as more than three-quarters (77%) of merchants report successful dispute outcomes using these rules[3].

Previous Visa Security Roadmaps have significantly shaped risk and security standards in Australia's payments ecosystem. As new risks emerge with new opportunities in the era of generative artificial intelligence (GenAI), we look to the role that AI can play in secure technologies for the future. **Visa has already invested US$3 billion globally in AI and data infrastructure over the past decade**[4].

[2] VisaNet data on authentication penetration for transactions acquired in Australia, 12 months ending August 2024, VisaNet, August 2023 to August 2024

[3] Cybersouce, Global Fraud Report 2024, https://www.cybersource.com/content/dam/documents/campaign/fraud-report/global-fraud-report-2024.pdf

[4] Visa, Rajat Taneja, Visa: 30 years of AI and counting, September 2023, https://usa.visa.com/visa-everywhere/blog/bdp/2023/09/13/30-years-of-1694624229357.html

A changing world

The rapid change playing out in payments is the reflection of a changing world.

The COVID-19 pandemic was a catalyst in the evolution of eCommerce, resulting in a substantial increase in online retail activities in Australia and establishing this channel as a fundamental part of everyday life for Australians. The number of households shopping online has grown by 16% and 18% in metro and rural areas respectively since 2019, with Australians making more frequent online purchases and spending A$63.6 billion online in 2023[5]. The increase in eCommerce adoption is expected to continue, with projections suggesting a compound annual growth rate of 8.33% in eCommerce revenues from 2024–2028[6].

These changing consumer behaviours, combined with the rise in artificial intelligence, machine learning technologies and the ongoing expansion of online business models, have created new opportunities for cyber criminals to exploit weaknesses and vulnerabilities. This poses significant threats to businesses and consumers alike. Cyber attacks, payment fraud, and scams have inflicted substantial losses across the ecosystem, underscoring the need for all participants to actively engage in mitigating these threats.

In 2023 losses from card-not-present (CNP) fraud escalated to

A$688m[7]

and scam losses reached

A$2.7bn[8].

Meanwhile, data security breaches emerged as one of the most significant privacy risks for Australians[9].

[5] Australia Post, Ecommerce Industry Report: 2024 Inside Australian Online Shopping, 2024, https://auspost-report.s3.ap-southeast-2.amazonaws.com/eCommerce+Industry+Report+2024+-+Trends+in+eCommerce+section.pdf

[6] Commission Factory, Key Ecommerce and Online Shopping Statistics in Australia in 2024, 6 March 2024, https://blog.commissionfactory.com/ecommerce-marketing/australia-ecommerce-statistics

[7] AusPayNet, 2024 Australian Payment Fraud Report, https://www.auspaynet.com.au/resources/fraud-statistics/2023-Calendar-year

[8] ACCC, National Anti-Scam Centre, Targeting Scams Report 2024, April 2024, https://www.nasc.gov.au/system/files/targeting-scams-report-2023.pdf

[9] Office of the Australian Information Commissioner, The Australian Community Attitudes to Privacy Survey 2023, 8 August 2023, https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2023#:~:text=Eight%20in%20ten%20(82%25),use%20of%20their%20personal%20information.

Understanding the new threat landscape

The democratisation of technology has made tools and knowledge easier for people to access and, while this has delivered numerous social and economic benefits, it has also empowered cyber criminals, providing them with more opportunities and new channels for digital crime.

Compounded with Australia's eCommerce growth and the variety of available payment options, the threat landscape has become increasingly complex. Visa's Payment Ecosystem Risk & Control teams have tracked several trending tactics repeatedly over the past 24 months[10]:

Increased adoption of AI by malicious actors, leading to sophisticated phishing, social engineering, creation of deepfakes, scams and malware campaigns.

Unprecedented speed and scale of attacks, using advanced tools and infrastructure to execute sophisticated operations, evident in high-speed enumeration attacks and purchase return authorisation attacks.

Consumers are often targeted in the payment security flow through sophisticated scam campaigns, with threat actors using various payment methods, including non-traditional ones to monetise their schemes.

Synthetic identity fraud, with threat actors creating new identities to exploit merchant auto-onboarding processes and increase account-based fraud.

Exploitation of logical flaws or configuration gaps in the payment flow, leading to digital skimming attacks and harvesting of payment account data.

Data breaches and ransomware growth has slowed, but attacks still reached record levels in 2023.

[10] Visa, Biannual Threats Report, October 2024, https://corporate.visa.com/en/sites/visa-perspectives/trends-insights/documents/visa-pfd-biannual-threats-report-fall-2024.pdf

Both **unauthorised card fraud,** where transactions are made without a cardholder's consent, and **authorised fraud** (such as scams), where scammers deceive individuals or businesses into providing access to funds and payments credentials, present significant challenges.

In Australia, the total card fraud value (which includes both card-not present and card-present fraud, such as enumeration attacks, cyber attacks, malwares, skimming and counterfeit) rose by 32% to A$762 million, while the total value of card transactions increased 8% to A$1.1 trillion[11]. A significant portion of this was concentrated in the online, card-not-present space, with unauthorised card-not-present fraud seeing a 33% increase in 2023, reaching A$688 million[12]. This was driven by a sharp increase in cross-border fraud, where Australian-issued cards were used with overseas merchants. The Australian Bureau of Statistics' Personal Fraud Survey indicated that 8.7% of the population experienced card fraud in 2023[13].

Scams have also increased in various categories, with losses exceeding A$5 billion over the last two years, with investment and romance scams leading the charge[14]. With the advent of GenAI, it is increasingly attractive for threat actors to make use of these technologies to conduct elaborate scams. Threat actors use these capabilities to create highly realistic and convincing synthetic content, including text, images, audio, and video. This content can be used in sophisticated scams, such as generating personalised phishing emails, deepfakes that impersonate trusted individuals, and automated social engineering attacks.

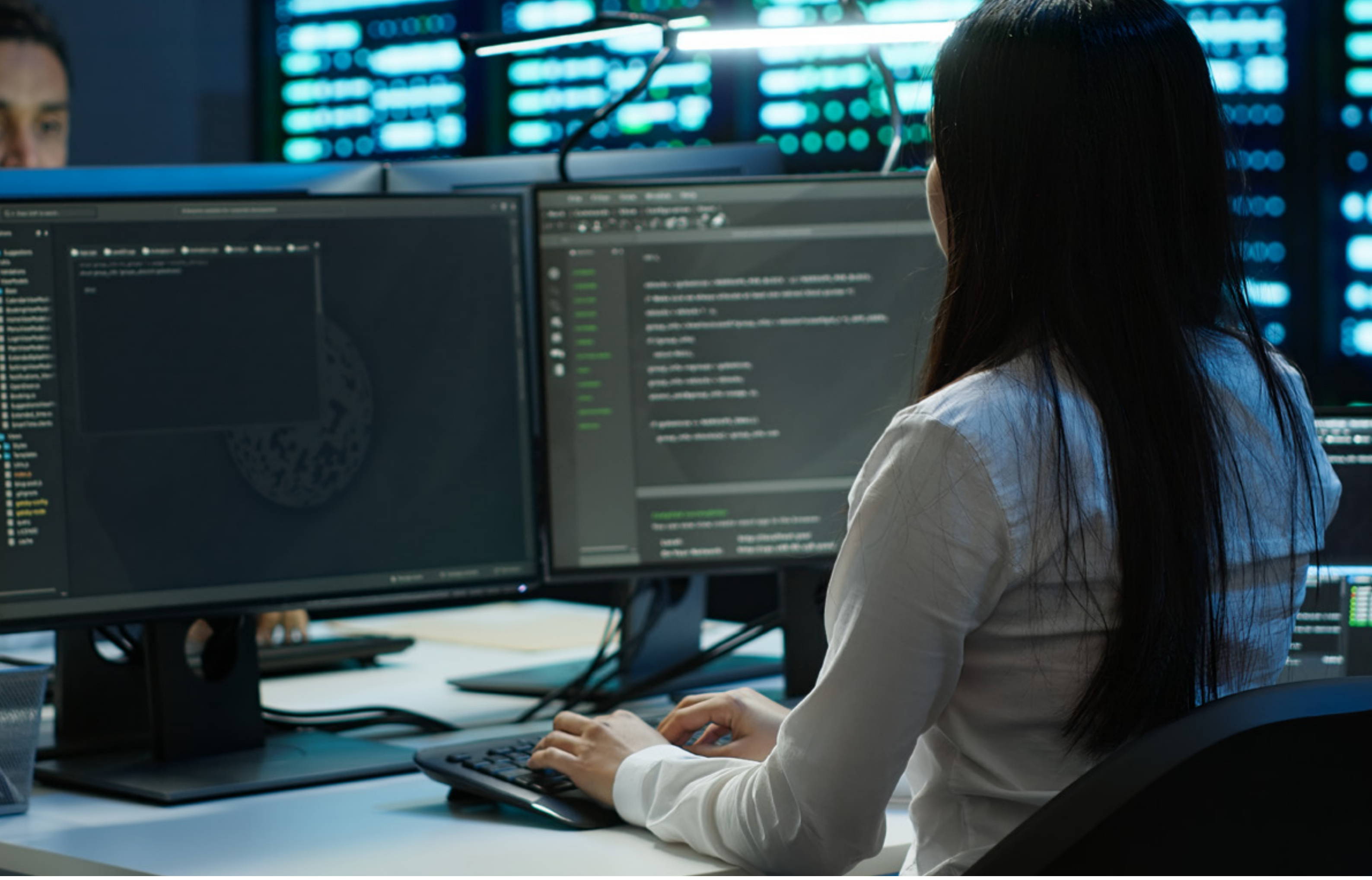
Data breaches add another layer of complexity to the threat landscape, given their far-reaching implications when sensitive information is compromised. The latter half of 2023 saw a 19% increase in reported breaches compared to the first half and 67% of these breaches resulted from malicious criminal attacks[15], highlighting the escalating threat of data breaches and the critical importance of robust cyber security defences.

[11,12] AusPayNet, 2024 Australian Payment Fraud Report, https://www.auspaynet.com.au/resources/fraud-statistics/2023-Calendar-year

[13] Australian Bureau of Statistics: Personal Fraud, March 2024, https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/latest-release

[14] ACCC, Targeting Scams: Report of the ACCC on scams activity 2022, April 2023 https://www.accc.gov.au/system/files/Targeting scams 2022.pdf & Targeting Scams: Report of the National Anti-Scam Centre on scams activity 2023, April 2024 https://www.accc.gov.au/about-us/publications/serial-publications/targeting-scams-reports-on-scams-activity/targeting-scams-report-of-the-accc-on-scams-activity-2023

[15] OAIC, Notifiable Data Breaches Report July to December 2023, 22 February 2024, https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-july-to-december-2023



In response to these challenges, various initiatives have been launched across sectors in Australia that aim to combat fraud and scams and address data security issues. These include:

- Establishment of the **National Anti-Scam Centre** in July 2023[16] to enhance coordination between the Government, law enforcement, and the private sector in combatting scams.
- Launch of the **Scam-Safe Accord by the Australian Banking Association** in November 2023[17], which is a comprehensive suite of anti-scam measures focused on disruption, detection, and response, including the development of an anti-scam strategy and intelligence sharing across sectors.
- Draft legislation for the **Scams Prevention Framework (SPF)** in September 2024[18], which establishes scam prevention principles in legislation that will guide industry-specific, mandatory obligations on designated sectors.
- The new **Australian Cyber Security Strategy** and legislative reforms[19], which propose increased collaboration between the Government and businesses at all stages of cyber incidents, the establishment of a Cyber Incident Review Board and mandatory reporting of ransomware incidents.
- **AusPayNet's Card-Not-Present Fraud Mitigation Framework**[20], which aims to curb the growing instance of online card fraud in Australia.
- Launch of the **Australian Online Scams Code (AOSC)** developed by the Digital Industry Group (DIGI) in July 2024[21], a collective effort by leading tech companies to combat online scams in the digital industry.
- **Digital Identity legislation**, which focuses on creating a safe and inclusive digital environment that provides secure and convenient options for individuals to verify their identities[22].

[16] ACCC, ACCC welcomes funding to establish National Anti-Scam Centre, 15 May 2023, https://www.accc.gov.au/media-release/accc-welcomes-funding-to-establish-national-anti-scam-centre

[17] Australian Banking Association, Banks unite to declare war on scammers, 24 November 2023, https://www.ausbanking.org.au/new-scam-safe-accord/#:~:text=Australian%20banks%20have%20joined%20forces,out%20of%20business%20in%20Australia.

[18] Australian Government, The Treasury, Scams Prevention Framework – exposure draft legislation, 13 September 2024, https://treasury.gov.au/consultation/c2024-573813

[19] Department of Home Affairs, 2023-2030 Australian Cyber Security Strategy, 22 November 2023, https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy

[20] Australian Payments Network, CNP Fraud Mitigation Framework, July 2023, https://www.auspaynet.com.au/insights/initiatives/CNP-Fraud-Mitigation-Framework

[21] Digital Industry Group Inc, Scams and Consumer Protection, 26 July 2024, https://digi.org.au/scams/

[22] Australian Government, Department of Finance, Digital ID Act 2024 legislation is coming, 28 November 2024, https://www.finance.gov.au/about-us/news/2024/digital-id-act-2024-legislation-coming

Visa has actively participated in the creation of different initiatives and tools, contributing to a safer digital environment in Australia. We continue to put our technology and expertise to work to enhance security, reduce fraud, and deliver seamless digital experiences for Australian consumers and merchants. In addition, Visa has invested over US$10 billion into technology and innovation in the last five years, to strengthen fraud prevention solutions and increase network security.

In 2024, we expanded Visa Protect, a suite of risk and identity products designed to safeguard consumers and businesses with new AI-powered solutions aimed at reducing fraud for transactions both on and off Visa's network. These include account-to-account and card-not-present payments. Key solutions within the Visa Protect suite include:

- Visa Advanced Authorisation (VAA), which utilises machine learning to provide real-time risk assessments for transactions, helping to identify and prevent fraud
- Visa Consumer Authentication Service (VCAS), which enhances security for online transactions by providing secure authentication methods such as biometrics
- Visa Provisioning Intelligence (VPI), which facilitates secure token provisioning to combat increasing token provisioning fraud
- Visa Protect Authentication Intelligence (VPAI), which leverages data analytics to optimise authentication processes, reducing friction for legitimate users while enhancing fraud detection; and
- Visa Protect for Account to Account (VPAA), which offers additional protection for account-to-account transactions.

VAA, for example, **has helped Australian financial institutions prevent A$714 million in fraud** from disrupting Australian businesses in a single year[23].

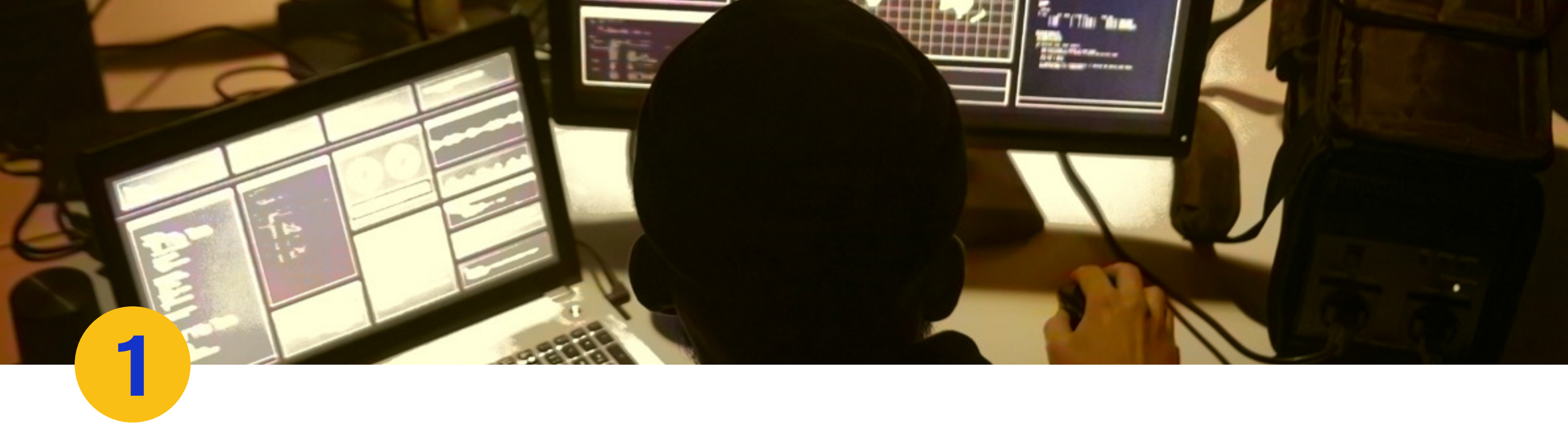
[23] Visa, 12 months ending March 2023, VisaNet, April 2022 to March 2023, https://www.visa.com.au/about-visa/newsroom/press-releases/visa-prevents-more-than-700-million-in-fraud-from-disrupting-australian-businesses.html

Preparing for the future:

Visa Security Roadmap 2025–2028

Taking this changing landscape into account, this latest edition of Visa's Security Roadmap outlines six focus areas to strengthen resilience in the payment ecosystem into 2025 and beyond.

1. Preventing enumeration attacks
2. Continued investment in secure technologies to balance fraud management and improved customer experience
3. Shifting to a data-driven risk based approach
4. Ensuring ecosystem resilience against unauthorised payments fraud and scams (authorised fraud) in the era of AI
5. Enhancing the cyber security posture of ecosystem participants
6. Securing digital payment experiences by integrating best-in-class security protocols



1

Preventing enumeration attacks

Enumeration attacks and account testing attacks are criminal practices where fraudsters use automation to test and guess payment credentials, which can then be used in perpetrating fraudulent transactions.

In these situations, threat actors target merchants with rapid, brute force, via card testing attacks, which involve the use of malicious scripts or code. They send thousands of low-value transaction attempts to test the validity of a primary account number, expiry date or Cardholder Verification Value (CVV2). Attackers adopt a variety of methods but mostly target online merchants that may lack adequate fraud controls, posing a significant risk in particular to Australian issuers, acquirers and merchants.

While such attacks contribute to less than 1%[24] of global card-not-present volume, they continue to be a popular vector for threat actors to validate compromised payment credentials, resulting in significant follow-on fraud.

40%[25] In the first six months of 2023, Visa saw a **increase in enumeration attacks** compared to the previous period.

These affect all parties in the payment ecosystem. Issuers suffer substantial fraud losses – in the year 1 October 2022 to 30 September 2023,

enumeration attacks led to US$1.1bn globally in fraud losses[26].

Merchants and acquirers face operational costs, losses from fraudulent transactions, and risk exposures, including compliance, regulatory, and reputation risks. To mitigate this, parties are advised to adopt preventive measures, such as the use of authentication controls, anomaly detection, real-time monitoring, and setting velocity thresholds. Additionally, acquirers should also require CVV2 for unsecure transactions (untokenised or unauthenticated transactions) and monitor for retries with different values, which indicate account testing behaviour. Collaboration and information-sharing among all parties involved are pivotal in combatting these attacks as per best practice guidelines for merchants.

Visa monitors and responds to these attacks via our Risk Operations Centre (ROC), a 24/7, real-time fraud detection and mitigation system operated by our fraud and security experts. From January to June 2024, the Visa ROC team collaborated with financial institutions and other partners to oversee and address large-scale fraud incidents worldwide, implementing pre-emptive targeted blocks in coordination with affected organisations on 68% of these incidents to prevent fraud without disrupting genuine transactions. These instituted blocks of presumed fraudulent transactions resulted in over

51 million declined fraudulent transactions[27].

To counter these attacks, Visa continues to invest in new technology, such as Visa Account Attack Intelligence (VAAI), to detect large-scale attacks with machine learning, using VisaNet insights.

[24] Visa, Biannual Threats Report, December 2023, https://usa.visa.com/content/dam/VCOM/regional/na/us/run-your-business/documents/pfd-biannual-threats-report-december-2023.pdf

[25] Visa, Getting Payments – What is an enumeration attack, February 2024, https://www.linkedin.com/pulse/what-enumeration-attack-visa-cac2c/

[26] Visa, Introducing the Visa Acquirer Monitoring Program, August 2023, https://usa.visa.com/visa-everywhere/blog/bdp/2024/08/29/introducing-the-visa-1724958906425.html

[27] Visa, Biannual Threats Report, Fall 2024, October 2024, https://corporate.visa.com/en/sites/visa-perspectives/trends-insights/documents/visa-pfd-biannual-threats-report-fall-2024.pdf

Introducing

Visa Acquirer Monitoring Program (VAMP)

Due to the rapidly evolving payment ecosystem, Visa has also updated and strengthened acquirer risk controls for the new Visa Acquirer Monitoring Program (VAMP)[28].

VAMP has the potential to address

4x THE AMOUNT OF FRAUD GLOBALLY, ACCOUNTING FOR MORE THAN US$2.5BN IN LOSSES,

compared to previous programs and will help acquirers prevent fraudulent activities.

VAMP, effective 1 April 2025, creates more seamless controls and processes for acquirers and merchants to effectively deter fraud and enumeration and manage disputes, contributing to a more secure environment. The changes include:

- **Retiring the existing fraud and disputes monitoring program** to create globally-aligned fraud thresholds for both domestic and cross border card-not-present transactions.
- **Incorporating new enumeration criteria** based on the number of enumerated authorisation transactions and the enumeration rate identified by the VAAI Score, which provides increased coverage on enumeration monitoring.
- **Launching the new risk technology tool Visa Ecosystem Risk Control (VERC),** a case management tool that allows for independent portfolio performance monitoring and improves operational efficiency.

[28] Visa, Introducing the Visa Acquirer Monitoring Program, 30 August 2024, https://usa.visa.com/visa-everywhere/blog/bdp/2024/08/29/introducing-the-visa-1724958906425.html

2

Continued investment in secure technologies

Tokenisation replaces a 16-digit debit or credit card number with a unique identifier, a token, that only Visa can unlock. Visa tokens secure the payment credential, enabling the transfer of enhanced data, which can help to improve payment success rates and lower fraud rates. These benefits, coupled with ease of use across devices, lead to an improved consumer experience. The token devalues sensitive card data as it has no intrinsic or exploitable value and cannot be mathematically reversed to reveal the original card number. This remains one of the most secure ways to protect against card data compromise by removing it from the transaction flow, and limits the risk exposure in a breach.

As of April 2024, Visa has issued

1Billion[29]

tokens in the Asia Pacific region

boosting digital payments while enhancing security.

Asia Pacific's digital economy experienced an uplift of more than US$2 billion in 2023 due to Visa Token Service (VTS) adoption, with merchants who have adopted VTS for their digital payments experiencing a higher payment success rate or authorisation uplift and payment fraud rates reduced by more than half (58%)[30].

Token provisioning challenges

Tokenisation benefits all parties, but its security depends on effective token provisioning risk management. However, tokens may be illegitimately provisioned to bad actors. Provisioning related fraud is defined as fraudulent transactions occurring after a token's activation, primarily impacting device-bound tokens. At present, token provisioning fraud to digital wallets manifests as the rapid monetisation of tokens by threat actors in a use-and-lose pattern, with little attempt to incubate the fraudulent credential[31]. Visa found that token provisioning fraud losses reached an estimated US$450 million globally in 2022 alone[32]. Issuers should counter this by using tools, such as Identification and Verification (ID&V) methods, and the use of various data sources for risk assessment and post provisioning monitoring.

Visa Provisioning Intelligence is an AI-based solution designed to combat token provisioning fraud at its source, which uses machine learning to rate the likelihood of fraud for token provisioning requests. This helps financial institutions prevent fraud in a targeted way and enables more seamless and secure transactions for Visa cardholders. Available in Australia since October 2023, Visa Provisioning Intelligence is designed to help reduce overall ecosystem fraud and increase the number of valid token provisioning requests.

[29] Visa, The transformative impact of tokenisation on commerce in Asia Pacific, March 2024, https://www.visa.com.sg/partner-with-us/payment-technology/visa-tokenisation/unpacking-payment-tokenisation.html#:~:text=The%20transformative%20impact%20of%20tokenisation%20on%20commerce%20in%20Asia%20Pacific&text=Across%20Asia%20Pacific%2C%20consumers%20have,up%20from%203.8%25%20in%202019%C2%B9.

[30] Visa, Visa tokens bring USD2 billion uplift to digital commerce in Asia Pacific, March 2024, https://www.visa.com.ph/about-visa/newsroom/press-releases/visa-tokens-bring-usd2-billion-uplift-to-digital-commerce-in-asia-pacific.html#:~:text=Asia%20Pacific%E2%80%99s%20digital%20economy%20experienced%20an%20uplift%20of,the%201%20billion%202%20milestone%20in%20Asia%20Pacific.

[31] Visa, Biannual Threats Report, June to December 2023, December 2023, https://usa.visa.com/content/dam/VCOM/regional/na/us/run-your-business/documents/pfd-biannual-threats-report-december-2023.pdf

[32] Visa Provisioning Intelligence launches to combat token provisioning fraud, December 2023, https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.20251.html

Authentication (EMV® 3DS) enhances payment security and user experience by promoting frictionless authentication for online transactions. Its advanced risk-based decisioning and the availability of additional data elements in EMV® 3DS makes it superior to its predecessor (3DS 1.0). The transition to newer protocols – version 2.2.0 – ensures seamless, enhanced user experiences across applications and device channels and provides more data for authentication and security.

While secure technologies are crucial for payment ecosystem security, threat actors exploit weaknesses in identity verification. With the rapid increase in phishing scams, sole reliance on the step-up via One-Time-Passwords (OTP) presents vulnerabilities to Identification and Verification (ID&V) methods:

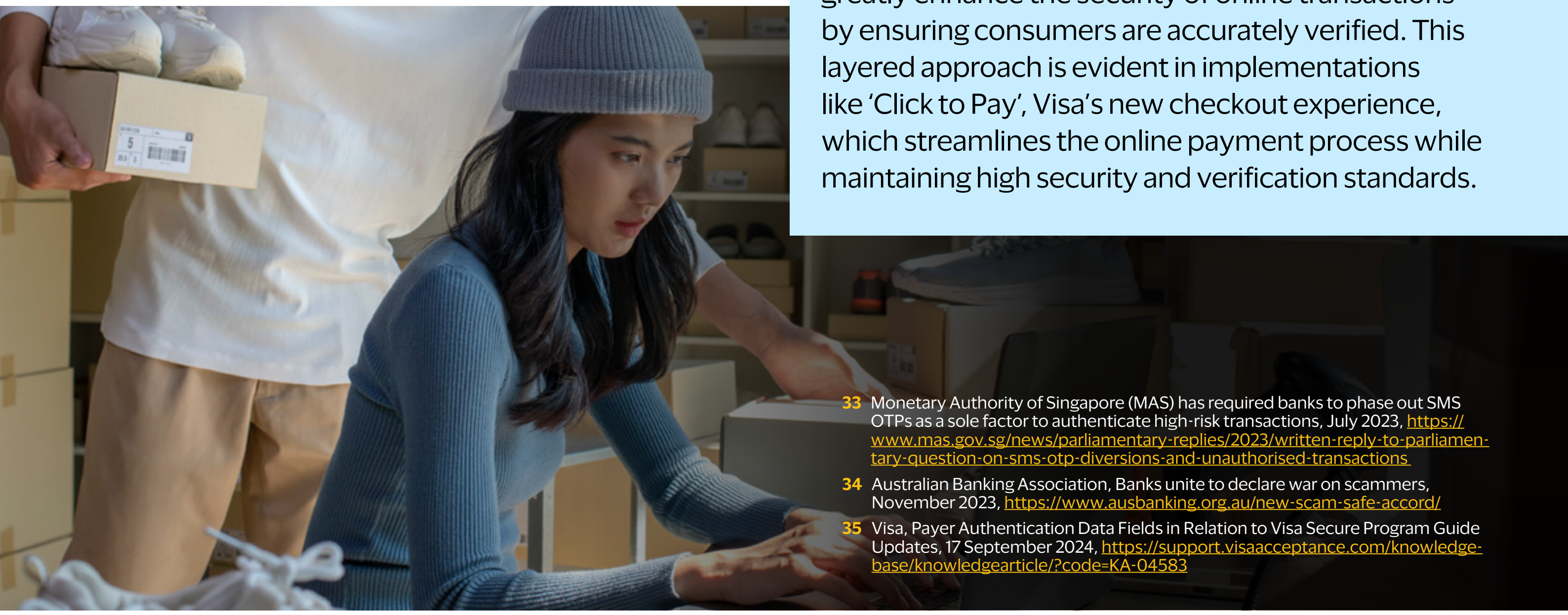
- **OTP Bypass Scams:** Threat actors can exploit OTPs to fraudulently provision payment accounts to their digital wallets or authenticate online transactions.
- **Relay Schemes:** In OTP relay schemes, the OTP is intercepted and used by fraudsters to authenticate transactions.
- **Rapid Monetisation:** Provisioning fraud often manifests as rapid monetisation of fraudulently provisioned tokens by threat actors, which creates a steep fraud curve.

In response to these threats, regulators in some regions have mandated the removal of SMS OTP, encouraging issuers to adopt methods less prone to social engineering[33]. In Australia, the Australian Banking Association (ABA) has recommended measures such as biometric checks for new account openings to help combat identity fraud[34].

To address the threats of social engineering and strike a balance with a risk-based approach, Visa is mandating issuers to move away from using SMS OTP as the sole factor for authentication by 2026.

Issuers are encouraged to migrate towards more secure authentication methods, such as biometric or in-app authentication, or newer methods like app-to-app and passkeys, which involve multi channels and/or devices providing higher confidence in the identification process.

For merchants and acquirers Visa introduced the Visa Secure minimum data requirements in August 2024 where merchants must provide required data in the authentication request[35]. Consistently high quantity and high quality data fields help enhance business outcomes for merchants and provide additional security for the cardholders. Incorporating biometric authentication with tokenisation can greatly enhance the security of online transactions by ensuring consumers are accurately verified. This layered approach is evident in implementations like 'Click to Pay', Visa's new checkout experience, which streamlines the online payment process while maintaining high security and verification standards.



[33] Monetary Authority of Singapore (MAS) has required banks to phase out SMS OTPs as a sole factor to authenticate high-risk transactions, July 2023, https://www.mas.gov.sg/news/parliamentary-replies/2023/written-reply-to-parliamentary-question-on-sms-otp-diversions-and-unauthorised-transactions

[34] Australian Banking Association, Banks unite to declare war on scammers, November 2023, https://www.ausbanking.org.au/new-scam-safe-accord/

[35] Visa, Payer Authentication Data Fields in Relation to Visa Secure Program Guide Updates, 17 September 2024, https://support.visaacceptance.com/knowledgebase/knowledgearticle/?code=KA-04583

3

Shifting to a data-driven risk based approach

Adopting a risk-based approach in payments is a key strategy for ensuring the security of the ecosystem. It not only mitigates fraud but reduces false positives, leading to a better customer experience.

While EMV® 3DS is often associated with this risk-based authentication, this approach should not be limited to the authentication flow alone. Data is available at various stages of the payments journey, and effectively utilising it can greatly enhance fraud mitigation strategies. This is reflected in various initiatives aimed at bolstering fraud mitigation strategies across the payment ecosystem:

APRIL ’21 ✓ **The Network Performance Drive (NPD)** was introduced in April 2021 to facilitate the adoption of flexible payment experiences and foster cardholder trust. It includes two key frameworks for secure and user-friendly customer experiences:

- **Secure Credential Framework (SCF)**, which focuses on payment credential security, and provides guidelines for safe handling, storage, and transmission of sensitive payment information in the digital environment.
- **Digital Authentication Framework (DAF)**, which centres around digital transaction authentication, and supports investment in low-friction, robust authentication methods[36].

APRIL ’24 ✓ The streamlined **merchant** Payment Card Industry Data Security Standard **(PCI DSS) requirements[37].**

AUGUST ’24 ✓ Updated **Visa Secure minimum data requirements** to support issuers’ authentication decision-making to determine whether a transaction should be frictionlessly approved or challenged[38].

OCTOBER ’24 ✓ Updated risk standards to support a more secure, efficient and collaborative environment for acquirers through the launch of **Visa Acceptance Risk Standards (VARS)** in October 2024[39].

[36] Visa, Why tokens hold the key to the future: de-risking the evolving payments ecosystem, October 2023, https://navigate.visa.com/cemea/trust-and-security/why-tokens-hold-the-key-to-the-future-de-risking-the-evolving-payments-ecosystem/

[37] Visa, Account Information Security Program and PCI, accessed November 2024, https://corporate.visa.com/en/resources/security-compliance.html#1 .

[38] Visa, Visa Payer Authentication Data Fields in Relation to Visa Secure Program Guide Updates, 17 September 2024, https://support.visaacceptance.com/knowledgebase/knowledgearticle/?code=KA-04583

[39] Visa, Visa Acceptance Risk Standards, 1 October 2024, https://usa.visa.com/dam/VCOM/download/merchants/visa-global-acquirer-risk-standards.pdf

In EMV® 3DS, the additional data elements underpin its value in reducing friction and fraud and improving the customer experience. The data providers (merchants) and recipients (issuers) play a complementary role in an everchanging landscape where threat actors employ advanced tactics to exploit vulnerabilities. By ensuring complete and accurate data, we can enhance the overall performance of EMV®3DS to achieve better business outcomes for merchants, cardholders and issuers.

The **Visa Protect Authentication Intelligence Score** – part of the Visa Protect suite – was launched in September 2023 to support issuer authentication decisioning. The Score uses machine learning from aggregated EMV® 3DS transaction data, historical Visa data and fraud data to help issuers evaluate transactions in authentication. This is aimed at helping issuers provide seamless payment experiences, with a reduced need to challenge, ensure fewer false declines and improve fraud-to-sales ratios with enhanced fraud detection. By doing so, consumers enjoy smoother and more secure transactions, while businesses benefit from increased customer satisfaction and reduced fraud-related losses.

Risk-based authentication in the Australian market has proven results, with one issuer seeing challenge rates decrease by 48%[40]

The revamp of the issuer's authentication strategy resulted in a smoother online checkout experience for cardholders and led to a reduction in abandonment rates by 113 basis points (bps).

Using a data-driven approach, the issuer was challenging fewer transactions, with a reduction in fraud rate by 6bps a testament to the benefits of striking a balance between customer convenience and robust fraud prevention.

✓ **Overall, Visa's direction for eCommerce is focused on enhancing security through new technologies, providing better data quality in transactions, and a layered approach to risk management.**

[40] CardinalCommerce Case Study, February 2024, An Australian Issuer's Journey from SMS OTP Only to Risk-Based Authentication (RBA), January 2024, https://cardinalcommerce.com/an-australian-issuers-journey-from-sms-otp-only-to-risk-based-authentication-using-vcas/

4

Ensuring ecosystem resilience against unauthorised payments fraud and scams (authorised fraud) in the era of AI

While the proliferation of Gen AI, combined with the expansion of the eCommerce landscape, is creating new threat opportunities, AI is also revolutionising the way we identify and prevent fraud and enable safer, more secure money movement.

The barriers to entry for bad actors have never been lower and continue to diminish, and therefore a comprehensive understanding of existing and emerging threats, and the evolving landscape spanning cyber security, fraud, and scams is paramount. This knowledge forms the cornerstone for developing relevant and effective strategies to mitigate risks and safeguard operations.

Artificial intelligence has been an integral part of Visa's operations for more than 30 years, and our commitment to ensuring ecosystem resilience against new threats in the era of AI is backed by our continued investment in this space. Back in 1993, Visa pioneered the use of AI in payments and became the first payments network to use neural networks for real-time, risk-based fraud analytics[41]. Today, our technology platform is among the most powerful examples of the tangible benefits of AI, with around 150 AI and machine learning models in production powering products that are helping to solve longstanding challenges and pain points for consumers, merchants and financial institutions. This knowledge forms the cornerstone for developing relevant and effective strategies to mitigate risks and safeguard operations.

[41] Visa, Rajat Taneja, Visa: 30 years of AI and counting, September 2023, https://usa.visa.com/visa-everywhere/blog/bdp/2023/09/13/30-years-of-1694624229357.html

Unauthorised fraud

In the realm of response and recovery, Visa has established a robust framework with its Zero Liability Policy to protect consumers from unauthorised fraud. Such fraud involves transactions conducted without the consumer's knowledge or consent. The Australian market has witnessed a significant surge in fraudulent activities, correlated with the rapid growth of eCommerce. As more consumers turn to online shopping, the increase in card-not-present (CNP) transactions presents an expanded opportunity for fraudulent activities to occur.

Visa has a robust set of scheme rules and a liability framework in place, backed by a long history of combatting unauthorised fraud.

The Visa Protect suite contains several solutions that are designed to detect this. The fraud models harness the power of AI, along with VisaNet data, to help drive decision-making for issuers before authorising risky transactions and aid merchants in addressing lower card-not-present conversion rates and poor online experience.

3.6% of all accepted eCommerce orders in Asia Pacific today are fraudulent[42]. **In Australia, the fraud rate has been on a declining trend since 2018 but saw a resurgence in 2023, with 14% increase compared to 2022[43].**

The rise in fraud concentrated in both card-not-present domestic and cross border transactions, with cross border fraud growing more than **4 times faster** than domestic fraud. While the payments industry has made significant strides over the past decade, it's crucial to continue the investment into multiple tools and techniques for effective fraud management.

Data usage plays a central role in the fraud prevention strategies for issuers, acquirers and merchants. Tools such as anomaly detection, which identifies unusual behaviour patterns, and predictive analytics, which forecasts potential threats based on past trends and patterns, harness the power of data to help combat fraud. It is essential for issuers to conduct real-time velocity monitoring or perform a common point-of-purchase (CPP) analysis by inspecting the suspected merchant's eCommerce website and identifying any links between the eCommerce setup and the malicious domains. An additional layer to protect consumers from fraud is also via the use of CVV2 or dynamic CVV2. There is a requirement for merchants to capture the CVV2 in authorisation for all unsecure ecommerce transactions (non-authenticated and non-tokenised). Performing a name and address verification could help reduce exposure to fraud and scams in CNP transactions.

Expanding **Account Name Inquiry (ANI)**[44], which enables an online merchant to verify that the name provided by a cardholder matches the name held by their issuing bank, and **Address Verification Service (AVS)**, which verifies whether a billing address matches the address of a credit card cardholder, to select countries in the Asia Pacific region will provide ecosystem participants with more data, enhancing their ability to verify cardholder identities and make informed decisions.

[42] Visa, 2024 Global eCommerce Payments & Fraud Report, 25th Edition, https://www.cybersource.com/content/dam/documents/campaign/fraud-report/global-fraud-report-2024.pdf

[43] Visa, 12 months comparison ending December 2023, VisaNet, January 2022 to December 2023

[44] Visa, Visa Account Name Inquiry, accessed December 2024, https://corporate.visa.com/content/dam/VCOM/regional/na/us/support-legal/documents/account-name-inquiry-onesheet-merchant-version.pdf

Introducing
Fraud Reporting and Control Program (FRECOP)

As part of Visa's continued efforts to secure the payments ecosystem, the new Fraud Reporting and Control Program (FRECOP) was launched to help ensure accurate and complete fraud reporting from all issuers globally.

Fraud reporting is essential for controlling fraud, mitigating risks across the ecosystem, enhancing payment security and meeting regulatory expectations regarding fraud mitigation. Through accurate fraud reporting, financial institutions and merchants receive actionable insights to optimise their payments and deliver a secure customer experience.

Introducing
Visa Integrity Risk Program (VIRP)

Visa Payment Fraud Disruption identified an increase in fraud associated with threat actors exploiting weak or inadequate merchant onboarding practices to establish fraudulent merchants[45]. Threat actors posing as legitimate merchants attempt to apply for payment services with the intent to commit fraud once granted access to the payment system. They often use synthetic or stolen identities obtained through data breaches, social engineering, or in cyber crime underground marketplaces. In addition to the threat of illegitimate merchants, there is also a risk posed by certain business types that, while legal, may process transactions for illegal activities if proper controls are not in place.

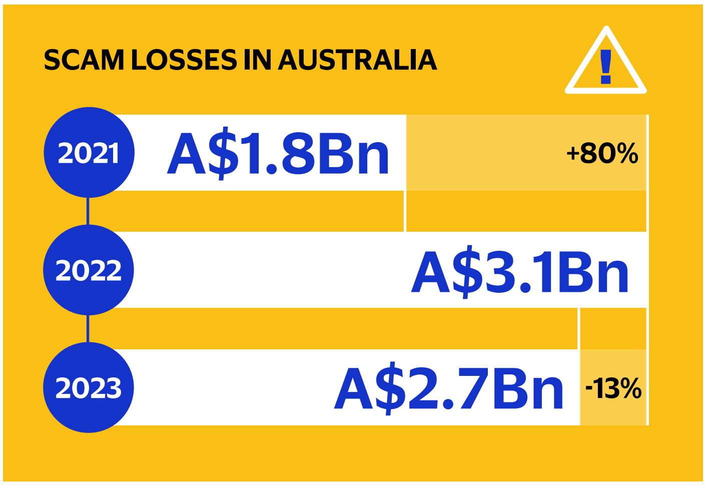
The Visa Integrity Risk Program (VIRP)[46] was launched in April 2023 to safeguard the Visa payment system's integrity. Its main aim is to protect acquirers, issuers, and cardholders from transactions that may involve illegal goods or services, contravene Visa product and service rules for Visa members (Visa Rules), or adversely impact the goodwill of the Visa payment system. The VIRP ensures that acquirers, and their agents, that support High Integrity Risk Merchants maintain proper controls and oversight of processes to identify and deter illegal transactions from entering the Visa payment system.

[45] Visa, Payment Fraud Disruption, The Pr3ssure Gauge, March 2023, https://corporate.visa.com/content/dam/VCOM/corporate/visa-perspectives/documents/protecting-the-integrity-of-the-visa-network.pdf

[46] Visa, Protecting the integrity of the Visa network, 6 April 2023, https://corporate.visa.com/content/dam/VCOM/corporate/visa-perspectives/documents/protecting-the-integrity-of-the-visa-network.pdf

Authorised fraud (scams)

There is an increasing level of attention on scams as they continue to be a growing concern for all participants in the Australian payment ecosystem.



In 2022, scam losses in Australia grew by 80% from the previous year, leading to a loss of **A$3.1 billion**[47] and, as referenced in our overview of the threat landscape, while total scam losses dipped by 13% (to **A$2.7 billion**) in 2023, the overall **scam reports lodged by Australians increased by 18.5% to a staggering 601,000**[48].

In the same period, the Personal Fraud Survey by the Australian Bureau of Statistics (ABS) revealed that more than half a million Australians fell victim to scams[49]. This dramatic rise and broad reach of scams highlights the pressing demand to bolster cyber security across the nation, as well as for continued vigilance and countermeasures to protect consumers and businesses.

Drawing on decades of experience in fraud prevention, Visa is now expanding its capability across to Real-Time Payment (RTP) rails, with the aim of helping financial institutions detect and deter scams on RTP networks and Authorised Push Payment (APP).

Visa Protect for Account to Account (VPAA) leverages our extensive experience from Visa Advanced Authorisation (VAA) and incorporates deep learning AI detection models to score account-to-account transactions in real-time. In other regions, this solution was launched in collaboration with payment operators in the United Kingdom and Latin America. Results from the pilot in the UK revealed Visa identified 54% of fraudulent transactions which had already passed through the banks sophisticated fraud detection systems, suggesting Visa's proven predictive **AI technology is an important contribution to this growing space and could potentially help save £330 million (A$639 million) for UK consumers**, businesses and the economy[50].

In late September 2024, Visa announced it has signed a definitive agreement to acquire Featurespace, a developer of real-time artificial intelligence (AI) payments protection technology that prevents and mitigates payments fraud and financial crime risks. The acquisition of Featurespace will complement and strengthen Visa's portfolio of fraud detection and risk-scoring solutions used by financial institutions around the world to grow and protect their businesses[51].

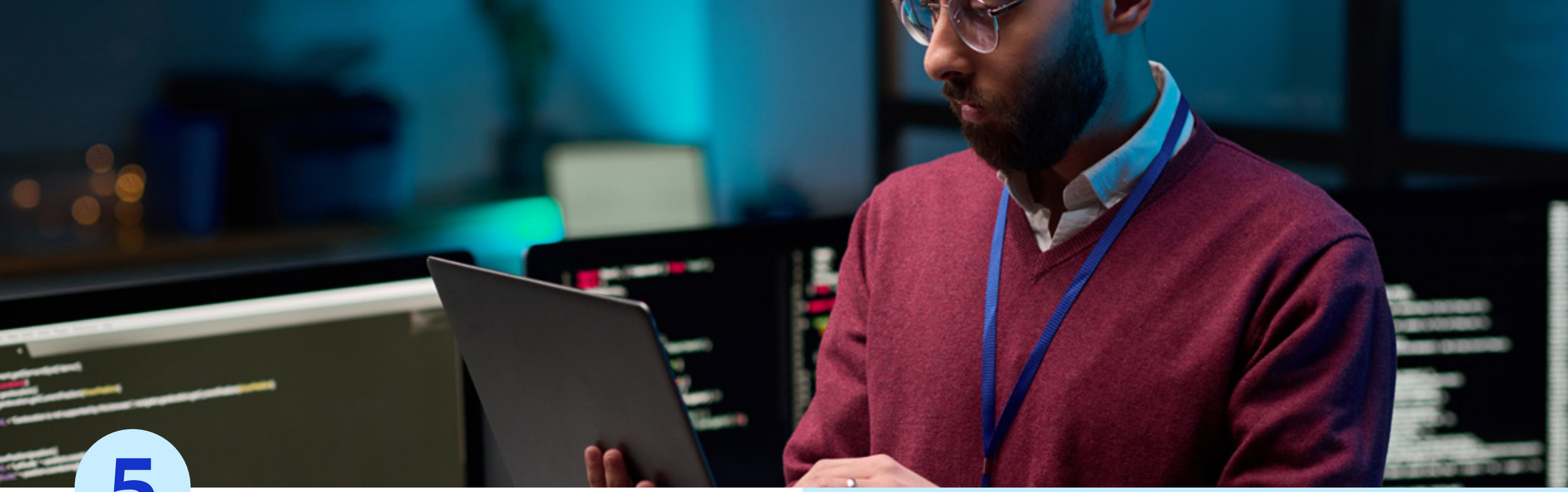
[47] ACCC, ACCC calls for united front as scammers steal over $3bn from Australians, 17 April 2023, https://www.accc.gov.au/media-release/accc-calls-for-united-front-as-scammers-steal-over-3bn-from-australians#:~:text=The%20latest%20Targeting%20Scams%20report%20has

[48] ACCC, Targeting Scams: Report of the National Anti-Scam Centre on scams activity 2023, April 2024, https://www.accc.gov.au/about-us/publications/serial-publications/targeting-scams-reports-on-scams-activity/targeting-scams-report-of-the-accc-on-scams-activity-2023

[49] Australian Bureau of Statistics: Personal Fraud, March 2024, https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/latest-release

[50] Visa, Visa's new AI tool for Faster Payments could help save UK over £330m a year on fraud and APP scams, 30 May 2024, https://www.visa.co.uk/about-visa/newsroom/press-releases.3326480.html

[51] Visa, Visa to acquire Featurespace, 26 September 2024, https://investor.visa.com/news/news-details/2024/Visa-to-Acquire-Featurespace/default.aspx



5

Enhancing the cyber security posture of ecosystem participants

The evolving threat landscape presents numerous challenges, with data breaches being a significant concern for Australians.

During the second half of 2023, there was a marked increase in reported breaches, totalling 483 incidents[52]. This represents a 19% increase compared to the first half of the year, where the health and finance sectors emerged as the most impacted areas. Cyber security incidents, including phishing, compromised or stolen credentials, and ransomware, accounted for 44% of the breaches.

Globally the Visa Payment Fraud Disruption team identified a 12.3% decrease in the number of ransomware and data breach attacks that were opportunistic in exfiltrating data, as compared to the prior six-month period. However, of note, is a trend wherein the number of overall incidents slightly decreased, but the breaches that are occurring are becoming more impactful. Additionally, although the total number of incidents tracked and cases opened both decreased slightly from the prior six-month period, threat actors show a continued interest in targeting third-party service providers[53].

Threat actors appear to persist in their targeting of critical infrastructure, which includes financial institutions among other essential service entities. These actors often resort to prevalent methods, such as social engineering, phishing, ransomware, and Distributed Denial of Service (DDoS) attacks.

In response to these cyber threats, the Australian government is proactively taking measures to bolster its cyber security, starting with conducting comprehensive consultations to devise robust strategies to mitigate these escalating risks.

Visa's commitment to cyber security and resilience

As a payment network, Visa is committed to maintaining the highest level of security of transactions throughout the industry, which is underpinned by several protective measures. At the core of these measures is board-level accountability that aligns risk management with Visa's vision, business strategy and objectives. Visa routinely identifies cyber threats, keeping the ecosystem and the public updated through security alerts, intelligence alerts, and threat reports. The Visa Biannual Threats reports provide an overview of the top payment ecosystem threats observed globally every six months.

Compliance with the global Payment Card Industry Data Security Standard (PCI DSS) is mandatory for all entities storing, processing, or transmitting Visa cardholder data. PCI DSS provides the technical and operational requirements for financial institutions, merchants and service providers to protect against attacks aimed at stealing cardholder data.

[52] OAIC, Notifiable Data Breaches Report July to December 2023, 22 February 2024, https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-july-to-december-2023

[53] Visa, Biannual Threats Report, Fall 2024, October 2024, https://corporate.visa.com/en/sites/visa-perspectives/trends-insights/documents/visa-pfd-biannual-threats-report-fall-2024.pdf

Across the payment ecosystem, there is an increasing trend for organisations to use third-party vendors or agents (TPAs) to scale their business. Visa's **Third-Party Agent (TPA) Registration Program** plays a vital role in ensuring adherence to Visa's rules and policies when TPAs are involved. These standards are pivotal in managing TPA relationships across the ecosystem, ensuring compliance, promoting integrity, and minimising risk.

DURING 2022–23,

millions of Australians

had their private information compromised through significant data breaches,

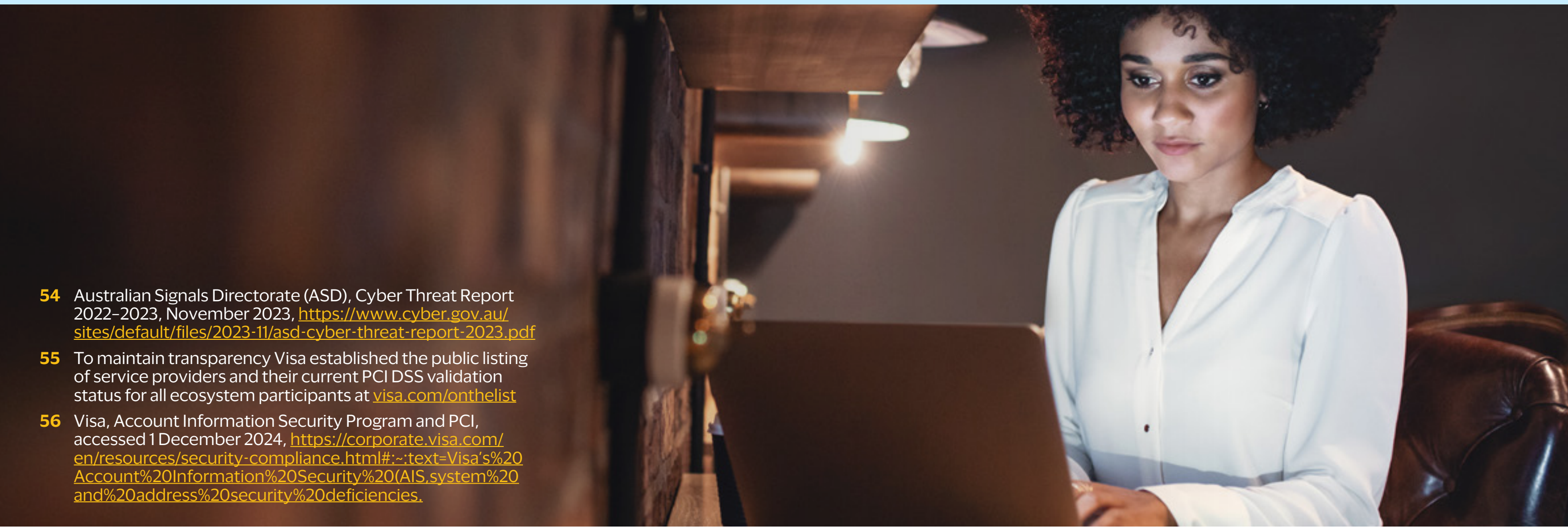
and some Australians were exposed to multiple breaches[54].

The rise in the number of data breaches highlighted the ongoing third-party vendor risks. As a result, stakeholders in the ecosystem are encouraged to conduct requisite due diligence and register TPAs with Visa[55].

Visa's **Account Information Security Program (AIS)** is a global compliance program dedicated to maintaining the safety and integrity of the Visa payment ecosystem[56]. This is achieved through monitoring compliance and addressing security deficiencies to prevent compromise of Visa account data. As mentioned previously, Visa is transitioning to a more streamlined merchant PCI DSS compliance reporting approach. The shift is designed to help provide acquirers with greater control and autonomy in overseeing and managing their merchants' compliance with PCI DSS requirements. Visa will shift its focus to non-compliant merchant cases and will continue to work with acquirers that have merchants under remediation.

Visa is also enhancing its network capabilities to support **Advanced Encryption Standard (AES)** by 2030 across a wider set of technology interactions than we do today. This will provide each transaction with a strengthened unique signature, verifying its authenticity. Getting ready for the migration to AES is critical to ensure that our partners are equipped to make use of a more secure solution, fostering a safe and resilient ecosystem.

Part of Visa's consulting arm aids issuers in identifying system weaknesses through the **Visa Payment Threats Lab (VPTL)**. This solution proactively detects potential vulnerabilities within payment systems, ideally before they are targeted by malicious actors. Typically, such security gaps only come to light following a fraudulent incident, but with VPTL, issuers can recognise and rectify gaps and vulnerabilities in advance.



[54] Australian Signals Directorate (ASD), Cyber Threat Report 2022–2023, November 2023, https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf

[55] To maintain transparency Visa established the public listing of service providers and their current PCI DSS validation status for all ecosystem participants at visa.com/onthelist

[56] Visa, Account Information Security Program and PCI, accessed 1 December 2024, https://corporate.visa.com/en/resources/security-compliance.html#:~:text=Visa's%20Account%20Information%20Security%20(AIS,system%20and%20address%20security%20deficiencies.

6

Securing digital payment experiences by integrating best-in-class security protocols

Advancements in digital payments will continue to shape the way Australians make and receive payments.

Amidst this transition, Visa remains committed to ensuring that every solution introduced prioritises security while balancing seamlessness. Visa has recently unveiled a variety of new payment experiences designed to enhance consumer convenience while maintaining trust and security.

One such innovation is **Click to Pay (CTP)**. By addressing challenges like cart abandonment, security concerns, and removing friction from the online check out experience, CTP optimises the payment process by eliminating the need for passwords, manual card entry, tedious form fills and various step ups. Instead of relying on traditional Primary Account Number (PAN) entry, CTP uses tokenisation, enhancing both security and convenience for consumers and merchants alike. With CTP consumers can access all their payment cards by entering their phone number or email address, then selecting their preferred card for payment. This consistent experience works across devices, allowing users to complete transactions securely with a few clicks. For merchants, it ensures authenticated payment credentials without requiring consumers to input PANs or passwords. Built on EMV Secure Remote Commerce standards, the CTP standards are compatible with technologies that enable cardholder verification and tokenisation.

With CTP

consumers use a single profile, across multiple devices and merchants

for cards from participating networks, leveraging existing secure technology standards to reduce friction and improve overall shopping experience.

In the increasingly complex digital world, identifying a person has become a challenge, with online payment fraud now seven times higher than in-person payments.

Globally, Visa seeks to address this issue with the Visa Payment Passkey (VPP) Service[57], built on the latest Fast Identity Online (FIDO) standards.

Using passkeys, cardholders can authenticate online transactions using biometrics in place of passwords or OTPs. This will be integrated across Visa's existing product suite and programs to offer a consistent, seamless and secure user experience for cardholders. Visa is currently testing VPP and will begin conducting pilots in the second quarter of 2025 in select Asia Pacific markets.

Globally, Visa has also announced the introduction of **Visa Flex Credential**, which seeks to revolutionise the payment experience for cardholders. This new solution allows cardholders to toggle between payment methods via just one single payment credential. Cardholders will have the flexibility to select from their preferred methods and set predefined preferences for each transaction.

With over six billion mobile devices worldwide, consumers are equipped with versatile near field communication (NFC) enabled devices for "tap" transactions. **Visa's Tap to Pay penetration has doubled since 2019, reaching 65% globally, reflecting its popularity[58].** Visa plans to enhance this service with new Tap to Everything features – transforming any device into a point-of-sale with Tap to Pay, ensuring secure online shopping with Tap to Confirm, enhancing card security with Tap to Add Card, and Tap to Accept enabling banking apps to support acceptance for nano merchants. All these innovations are underpinned by robust security protocols, including EMV chip security or dynamic data encryption for contactless transactions. Each tap transaction generates a unique, one-time code, which reduces the risk of counterfeit fraud. These features offer a fast, convenient and secure payment acceptance in the SMB space and will foster growth and innovation of Australia's 2.5 million small businesses[59].

[57] Visa Payment Passkey Delivers a Modern Authentication Solution, August 2024, https://corporate.visa.com/en/products/visa-payment-passkey.html

[58] Visa Reinvents the Card, Unveils New Products for Digital Age, May 2024 https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.20686.html#:~:text=Today%20at%20the%20annual%20Visa%20Payments

[59] Australian Government Small Business Statement 2024–2025, https://budget.gov.au/content/factsheets/download/factsheet-sml-bus.pdf

Looking ahead

Visa will continue to engage our stakeholders and partners to meet the evolving needs of consumers and businesses, working together to secure the payment system in Australia and globally.

Trust remains at the core of everything we do, and our collective responsibility is to continue to earn that trust by protecting individuals and businesses as the commerce landscape and threat environment evolves, driving security alongside payment innovation as we enable new and exciting ways to pay.

Considering these expectations of the Australian threat landscape in the coming years, Visa has mapped the steps we are already taking with ecosystem partners during 2024 and into the coming three years to highlight the critical areas for action.

2024

- Continued adoption of secure technologies
- Best Practices to prevent Enumeration Attacks
- Rollout of Visa Integrity Risk Program (VIRP)
- Release of PCI DSS v4
- Third-Party Agent (TPA) Registration
- Account Information Security (AIS) Program

2025

- Visa Program changes come into effect (VAMP, FRECOP)
- New guidance on Visa Acceptance Risk Standards (VARS)
- Further expansion of secure technologies – Click to Pay
- Support for contactless ATM access on Visa credentials
- Network Performance Drive 3.0

2026-2028

- Shift from SMS OTP to more secure authentication methods (biometrics, in-app)
- Preparation for the migration to Advanced Encryption Standard (AES)
- Visa's take on Digital Identity with Visa Payment Passkeys

Visa collaborates with its partners and industry stakeholders to keep payments secure and prevent fraud. The deployment of a multi-layered security approach has kept fraud rates low despite significant growth in the volume of digital payments. All parties in the ecosystem have a shared responsibility, and the table below lists how each stakeholder can play their part:

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
- Do not share any sensitive log in or authentication information with anyone, including someone claiming to be from your bank or another trusted source

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 www.visa.com/onthelist
- Offer fraud and risk management solutions for payments based on global standards, including authentication (through biometrics) as well as tokenisation

Merchants

- Implement risk solutions to prevent card-not-present and card present fraud, enumeration attacks, and cyber attacks
- Increase your approval rates and reduce your fraud rates through the usage of secure technologies: tokenisation, authentication, and Click to Pay
- Prevent account takeover fraud by utilisation of biometrics and ensure secure and seamless onboarding
- Make use of frictionless and risk-based authentication by providing additional data elements in transactions
- Enhance your dispute management processes by using Compelling Evidence 3.0 to reduce first party fraud
- Monitor the cyber health of your third-party providers as well as your organisation and have a contingency plan in place in case of a data breach

Acquirers

- Follow risk management practices for seamless and secure onboarding
- Equip your merchants with guidance and education for enumeration attacks defence, fraud prevention and dispute management by using real-time transaction decisioning tools
- Educate your merchants on the risk monitoring programs (VAMP, VIRP) and frameworks (SCF, DAF)
- Work with your gateways to ensure proper risk management processes, payment authentication and tokenisation
- Work with merchants to tokenise credentials, use secure technologies such as Click to Pay with EMV3DS
- Work with your merchants to provide required data points for seamless and frictionless transactions
- Monitor the cyber health of your third-party providers as well as your organisation and have a contingency plan in place in case of a data breach

Issuers

- Provide guidance and education to account holders 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, and biometric authentication)
- Provide an alternative form of authentication for ID&V other than SMS OTP
- Utilise fraud management techniques to reduce token provisioning challenges by utilisation of additional data points
- Use real-time transaction decisioning tools to combat enumeration attacks and increase approval rates
- Secure other payment rails, such as account to account, with the utilisation of card data to prevent scams

For more information, please contact your Visa Risk Manager or visit visa.com/security