



Security Road map

New Zealand
2025-2028

A decorative graphic element consisting of two horizontal bars, one blue and one yellow, stacked vertically.

Contents

Executive summary	3	Preparing for the future: Visa Security Roadmap 2025-2028	11
The journey	5		
A changing world	6		
Understanding the new threat landscape	7	1. Preventing enumeration attacks	12
Highlights of key security initiatives in New Zealand	9	2. Continued investment in secure technologies to balance fraud management and improved customer experience	14
		3. Shifting to a data-driven risk based approach	16
		4. Ensuring ecosystem resilience against unauthorised payments fraud and scams (authorised fraud) in the era of AI	18
		5. Enhancing the cyber security posture of ecosystem participants	24
		6. Securing digital payment experiences by integrating best-in-class security protocols	26
		Looking ahead	28

Confidentiality

This presentation is furnished to you solely in your capacity as a client of Visa and/or a participant in the Visa payments system. By accepting this presentation, you acknowledge that the information contained herein (the "Information") is confidential and subject to the confidentiality restrictions contained in the Visa Core Rules and Product and Service Rules or other confidentiality agreements, which limit your use of the Information. You agree to keep the Information confidential and not to use the Information for any purpose other than in your capacity as a customer of Visa or as a participant in the Visa payments system. The Information may only be disseminated within your organization on a need-to-know basis to enable your participation in the Visa payments system. Please be advised that the Information may constitute material non-public information under U.S. federal securities laws and that purchasing or selling securities of Visa Inc. while being aware of material non-public information would constitute a violation of applicable U.S. federal securities laws.

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

Reflecting a rapidly changing world, the digital payments ecosystem has changed more in the past 5 years than in the previous 50.



In this evolving technological landscape, businesses need to adapt quickly to protect themselves and thrive. This shift isn't just about technology; it's about meeting the new expectations of digital-savvy consumers and businesses who seek tailored, 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 consumers and businesses, it has also emboldened bad actors. The incentive for criminal activity in the digital domain has never been easier, nor more enticing, than it is today. The consumerisation of cutting-edge technologies and the proliferation of new payment methods have also given rise to a new generation of cyber criminals, where hacking can now be a side hustle.

Definitions of key terms used in this report:

Issuers: The cardholder's bank that provide payment cards like credit and debit cards, directly to consumers.

Acquirers: The merchant's bank that manages transactions and settlement on behalf of merchants.

Merchants: A business or individual that sells goods or services and accepts electronic payments from consumers.

Executive summary continued

AI is also part of the solution.

Visa has pioneered AI models in fraud prevention since 1993, and today, our technology platform is among the most powerful examples of the tangible benefits of its use. Visa has over 150 AI and machine learning models in production, powering products that help to solve longstanding challenges and pain points for consumers, businesses 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 digital payments ecosystem in the coming three years and the steps that can be taken to minimise the impact on consumers, businesses and other players in the payments ecosystem.

In this Roadmap we 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 digital payments ecosystem and facilitating global commerce for consumers, financial institutions, businesses (also known in the payments industry as Merchants), fintech partners and government entities. Our network spans more than 200 countries and territories, approximately 14,500 financial institutions, more than 150 million merchant locations and 4.7 billion payment credentials, enabling US\$15.9 trillion in total volume and a total of 310 billion transactions in Visa's fiscal year 2024¹.

Our network spans:



MORE THAN

200

COUNTRIES AND TERRITORIES



APPROXIMATELY

14.5k

FINANCIAL INSTITUTIONS



MORE THAN

150m

MERCHANT LOCATIONS



4.7bn

PAYMENT CREDENTIALS



US\$15.9tn

IN TOTAL VOLUME



310bn

TOTAL TRANSACTIONS
in its fiscal year 2024¹

¹ Visa Fact Sheet, September 2024, <https://corporate.visa.com/content/dam/VCOM/corporate/documents/about-visa-factsheet.pdf>

The journey

Since the previous two Visa Security Roadmaps for New Zealand were published in 2018² and 2022³, the payments and threat landscapes have transformed significantly.

Visa has worked continuously across the industry to strengthen the digital payments 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 managing 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.



Adoption of secure technologies:

Over the past two years, the adoption of EMV® 3DS in New Zealand has increased by 44%⁴. 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 or passkeys, for stronger security.



Preventing Card-Not-Present (CNP) fraud:

We have been vigilant in protecting the ecosystem from large-scale attacks, particularly as New Zealand continues to be a target for criminals in the Asia Pacific region. This vigilance has led to the introduction of Visa requirements for businesses 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 to be fraudulent. The new rules marked a significant step forward in enhancing the integrity of the digital payments ecosystem, as more than three-quarters (77%) of businesses report successful dispute outcomes using these rules⁵.



Previous Visa Security Roadmaps have significantly shaped risk and security standards in New Zealand'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 billion⁶ (NZ\$5 billion) globally in AI and data infrastructure over the past decade.**

EMV® 3DS is a protocol designed to enhance the security of Card-Not-Present (CNP) transactions by facilitating an additional layer of authentication between merchants and issuers. It helps prevent online fraud and ensures a more secure and seamless experience for all parties involved.

² Visa, Visa's Future of Security Roadmap: New Zealand, 2018, <https://www.visa.co.nz/content/dam/VCOM/regional/ap/newzealand/global-elements/documents/visa-future-of-security-roadmap-new-zealand.pdf>

³ Visa, Securing the Commerce Ecosystem in New Zealand, 2022, <https://www.visa.co.nz/pay-with-visa/security/future-of-security-roadmap.html>

⁴ VisaNet data on authentication penetration for transactions acquired in New Zealand, 24 months ending December 2024, VisaNet (Jan 2023 – December 2024)

⁵ Cybersource, Global Fraud Report 2024, <https://www.cybersource.com/content/dam/documents/campaign/fraud-report/global-fraud-report-2024.pdf>

⁶ Visa, Rajat Taneja, Visa: 30 years of AI and counting, September 2023, <https://corporate.visa.com/en/sites/visa-perspectives/innovation/thirty-years-of-ai-and-counting.html>

A changing world

The rapid change playing out in payments is reflected in 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 New Zealand; with many consumers discovering the ease and convenience of online shopping during lockdown. The number of online transactions increased by 5%⁷ in 2023 compared to 2022. Economic pressures led shoppers in New Zealand to adapt their spending behaviours, resulting in more frequent purchases in New Zealand but lower spending per transaction. In 2023, New Zealanders spent NZ\$5.8 billion online, which is 4% less than in 2022⁸. However, the increase in eCommerce adoption is expected to continue, with projections suggesting a compound annual growth rate of 9.21% in eCommerce revenues from 2025-2029⁹.

These changing consumer behaviours, combined with the rise in AI, 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 digital payments ecosystem, underscoring the need for all participants to actively engage in mitigating these threats.

In 2023 and 2024, New Zealanders reported nearly **NZ\$200 million** lost to scams each year¹⁰. Meanwhile, data security breaches emerged as the most reported incident type, with reports of phishing and credential harvesting seeing a 2% increase in 2023 from the previous year¹¹.

Credential harvesting is a cyberattack where criminals gather user login information, such as usernames, email addresses, and passwords, to access systems and steal sensitive data.

⁷ NZ Post, eCommerce Market Sentiments Report 2024, https://www.nzpostbusinessiq.co.nz/sites/default/files/2024-05/eCommerce_%20Market%20Sentiments%20Report_%202024.pdf.

^{8, 9} Digital Commerce - New Zealand, December 2024, <https://www.statista.com/outlook/emo/ecommerce/new-zealand>

¹⁰ Ministry of Business, Innovation & Employment, 198 million dollars lost to scams in the last year, 13 November 2023, <https://www.mbie.govt.nz/about/news/198-million-dollars-lost-to-scams-in-the-last-year>

¹¹ CERT NZ, 2023 Report summary, 2024, <https://www.cert.govt.nz/assets/Uploads/Quarterly-report/2023-q4/cert-nz-2023-report.pdf>

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 cybercriminals, providing them with more opportunities and new channels for digital crime.

Compounded by New Zealand's eCommerce growth and the variety of available payment options, the threat landscape has become increasingly complex. Visa's Payment Ecosystem Risk & Control (PERC) teams have been tracking several trending tactics repeatedly over the past 24 months^{12,13}:



Increased adoption of AI by malicious actors, leading to sophisticated phishing, social engineering, creation of deepfakes, scams and malware campaigns. Visa PERC continues to detect, investigate, and disrupt scam activity impacting the ecosystem. In the last twelve months, Visa PERC detected US\$357 million (NZ\$594 million) in fraud associated with scams and over 20K merchants involved in scams.



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. Enumeration resulted in around US\$1.1 billion (NZ\$1.85 billion) in follow-on fraud in a one-year period.



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. Visa PERC analysis identified a continued interest from threat actors in innovating fraud tactics, particularly in the use of social engineering, one-time passcode (OTP) bypass scams, and provisioning fraud.



Synthetic identity fraud, with threat actors creating new identities to exploit auto-onboarding processes for new business registrations and increase account-based fraud. For example, setting up a fraudulent merchant site to process eCommerce transactions which is registered to a fake business profile.



Exploitation of logical flaws or configuration gaps in the payment flow, leading to digital skimming attacks and harvesting of payment account data. Visa PERC identified a 7% increase in websites identified as infected.



Ransomware and data breach attacks that were opportunistic in exfiltrating data, with several thousand ransomware and data breach incidents tracked by Visa PERC over the past six months, a 51% increase from the prior six-month period.

Purchase Return Authorisation attacks occur when a merchant authorises a refund before the funds are settled, allowing the cardholder to exit the funds.

¹² Visa Public, Bi-Annual Threats Reports: Fall-2024, October 2024, <https://corporate.visa.com/en/sites/visa-perspectives/trends-insights/documents/visa-pfd-biannual-threats-report-fall-2024.pdf>

¹³ Visa Public, Bi-Annual Threats Report: Spring-2025, January 2025, <https://corporate.visa.com/content/dam/VCOM/corporate/solutions/documents/visa-perc-biannual-report-spring-2025.pdf>



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 both present significant challenges.

In 2024, based on reporting from 11 of New Zealand's largest financial institutions, the total card fraud and scam losses in the 12 months to September 2024 was reported at **NZ\$194 million**¹⁴. While the figure has fallen slightly compared to 2023 mentioned earlier, it remains high as threat actors continue to evolve. Based on Visa data, the total card fraud losses in New Zealand in the same reporting period (October 2023 - September 2024) showed a 22%¹⁵ increase compared to the same 12-month period prior (October 2022 - September 2023).

One likely reason for the reduction in the reported figure above is due to underreporting of scams overall. The State of Scams Report in New Zealand 2024¹⁶ indicated a 9% decrease in scam reports made to law enforcement agencies, with 68% of New Zealanders indicating that they did not report scams.



Despite the decrease in overall figures, various categories of **scams** have also increased in the same period. For example, online shopping scams surpassed identity fraud as the most common scam type in 2024¹⁷. And it's little wonder, with reports that **62% of New Zealanders encounter a scam at least once a month**¹⁸, and a 2% increase on scams encountered per month compared to 2023¹⁹.

With the advent of GenAI, it is increasingly attractive for threat actors to make use of GenAI tools to conduct elaborate scams. These technologies are used 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 top incident categories reported in the third quarter of the calendar year in 2024 were phishing and credential harvesting, which saw a 70% increase from the previous quarter²⁰, highlighting the escalating threat of data breaches and the critical importance of maintaining robust cyber security defences.



¹⁴ Ministry of Business, Innovation & Employment, MBIE is helping New Zealanders spot scams through Fraud Awareness Week, 18 November 2024, <https://www.mbie.govt.nz/about/news/mbie-is-helping-new-zealanders-spot-scams-through-fraud-awareness-week#:~:text=New%20data%20released%20today%20from.New%20Zealand's%20largest%20financial%20institutions>

¹⁵ Visa, 24 months comparison ending Sep 2024, VisaNet (October 2022 - September 2024)

¹⁶ GASA, State of Scams Report in New Zealand - 2023, <https://www.gasa.org/research>

¹⁷ Security Brief NZ, Netsafe report urges urgent reform of digital safety law, December 2024, <https://securitybrief.co.nz/story/netsafe-report-urges-urgent-reform-of-digital-safety-law#:~:text=Netsafe%2C%20in%20collaboration%20with%20the>

^{18, 19} GASA, State of Scams Report in New Zealand - 2023, <https://www.gasa.org/research>
²⁰ CERT NZ, Quarter Three Cyber Security Insights 2024, <https://www.cert.govt.nz/insights-and-research/quarterly-report/quarter-three-cyber-security-insights/>

Highlights of key security initiatives in New Zealand

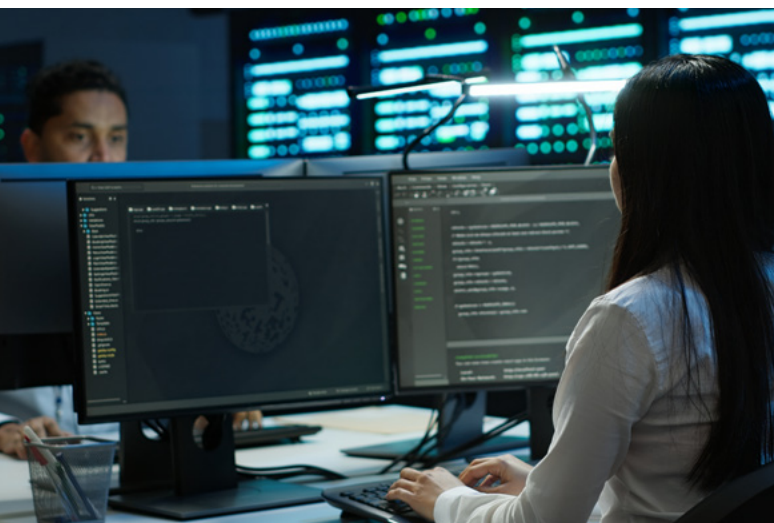
The New Zealand Government's Cyber Security Strategy²¹ envisions a confident and secure New Zealand thriving in the digital world by maximising online opportunities while minimising risks.

It emphasises the importance of connectivity for society and the economy, advocating for collective action from individuals, businesses, and the Government to enhance cybersecurity awareness and response. Various government initiatives have been launched across sectors in New Zealand that aim to combat fraud and scams and address data security issues. Annual Fraud Awareness Week is helping New Zealanders spot signs of phishing, impersonation, and online shopping scams. This initiative, along with others, demonstrates commitment to raising public awareness about common scam tactics.

This includes the establishment of the **Serious Fraud Office (SFO)**, in collaboration with the Ministry of Justice and New Zealand Police, to develop the National Counter Fraud and Corruption Strategy²² and advance fraud prevention and awareness activities.

Addressing the issue of scams requires collaboration between government, industry, and consumers. To combat scams effectively, digital platforms operating in New Zealand were urged to adopt the **Australian Online Scams Code (AOSC)** by mid-2025, setting industry-led commitments for fighting scams. Aligning efforts across digital platforms, banking, and telecommunications sectors will foster a collaborative ecosystem approach to effectively combat scams and better protect consumers²³.

Banks are also rolling out a range of responses in 2025 that aim to better protect their customers from scams, as five commitments are being introduced to the NZ Banking Associate Code of Banking Practice by November 2025. These include pre-transaction warnings to customers, identification of and response to high-risk transactions or unusual account transaction activity, and the ability to block or delay transactions in some cases. There is also a requirement for the banks to provide a 24/7 reporting channel for customers who think they've been scammed, and share scammer account information with other banks to help prevent criminal activity²⁴. If a bank failed to adequately warn and protect a customer from a scam, they might have to reimburse them up to NZ\$500,000²⁵.



²¹ Department of the Prime Minister and Cabinet, New Zealand's Cyber Security Strategy 2019, 2 July 2019, <https://www.dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-2019>

²² Serious Fraud Office, National Counter Fraud and Corruption Strategy, <https://www.sfo.govt.nz/fraud-and-corruption/what-we-do>

²³ Ministry of Business, Innovation & Employment, Encouraging action against online financial scams – an open letter to the Digital Platforms sector operating in New Zealand, 9 November 2024, <https://www.mbie.govt.nz/dmsdocument/29911-encouraging-action-against-online-financial-scams-an-open-letter-to-digital-platforms-pdf>

²⁴ New Zealand Banking Association, Banks step up customer scam protections and compensation, 23 April 2025, <https://www.nzba.org.nz/2025/04/23/banks-step-up-customer-scam-protections-and-compensation/>

²⁵ RNZ, Bank scam protections lacking in detail claims consumer advocate Janine Starks, 24 April 2025, <https://www.mz.co.nz/news/business/559022/bank-scam-protections-lacking-in-detail-claims-consumer-advocate-janine-starks>

Additionally, New Zealand has joined the United Kingdom's (UK) Bletchley Declaration on Artificial Intelligence (AI) Safety, which emphasises the responsible, safe, and trustworthy use of AI to boost productivity and innovation²⁶.

Visa continues to put our technology and expertise to work to enhance security, reduce fraud, and deliver seamless digital experiences for New Zealand consumers and businesses. In addition, Visa has invested over **US\$10 billion**²⁷ (NZ\$16.7 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 in account-to-account and CNP payments, both on and off Visa's network. Key solutions within the Visa Protect suite include

Visa Advanced Authorisation (VAA), Visa Consumer Authentication Service (VCAS), Visa Provisioning Intelligence (VPI), and Visa Protect Authentication Intelligence (VPAI).



Visa Advanced Authorisation, for example, has helped New Zealand financial institutions prevent **NZ\$273 million in fraud** from disrupting New Zealand businesses in a single year²⁸.

²⁶ Beehive (NZ Govt), NZ joins UK initiative for AI safety, 23 October 2024, <https://www.beehive.govt.nz/release/nz-joins-uk-initiative-ai-safety>

²⁷ Visa, Visa's Growing Services Business Infused with New AI-Powered Products, March 2024, <https://investor.visa.com/news/news-details/2024/Visas-Growing-Services-Business-Infused-with-New-AI-Powered-Products/default.aspx>

²⁸ Visa, 12 months ending March 2023, VisaNet (April 2022 – March 2023), <https://www.visa.co.nz/about-visa/newsroom/press-releases/visa-prevents-more-than-270-million-in-fraud-from-disrupting-new-zealand-businesses.html>

Preparing for the future:

Visa Security Roadmap 2025–2028

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

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

Preventing enumeration attacks

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

In these situations, threat actors target merchants with rapid, brute force, card testing attacks. These involve the use of malicious scripts or code, and the sending of 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 New Zealand issuers, acquirers and merchants.

While such attacks make up less than 1%²⁹ of global CNP volume, they continue to be a popular vector for threat actors to validate compromised payment credentials, resulting in significant follow-on fraud.

In the last six months of 2024, Visa saw a 22%³⁰ increase in enumeration attacks compared to the previous period.

These affect all parties in the digital payment ecosystem.

22%³⁰

Issuers suffer substantial financial losses due to fraud and increased processing fees – in the year 1 October 2022 to 30 September 2023, **enumeration attacks led to US\$1.1bn (NZ\$1.8 billion) globally in fraud losses**³¹.

Merchants and acquirers face operational costs, losses from fraudulent transactions, and risk exposures, including compliance, regulatory, and reputation risks. To mitigate these risks, 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 issuers, merchants and acquirers.

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 clients to oversee and address large-scale fraud incidents worldwide, Visa implemented pre-emptive targeted blocks in coordination with affected organisations for 68% of these incidents to prevent fraud without disrupting genuine transactions, resulting in over

51 million declined fraudulent transactions³².

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.

²⁹ Visa Public, Bi-annual Threat Report, December 2023, <https://usa.visa.com/content/dam/VCOM/regional/na/us/run-your-business/documents/pfd-biannual-threats-report-december-2023.pdf>

³⁰ Visa Public, Bi-annual Threat Report, January 2025, <https://corporate.visa.com/content/dam/VCOM/corporate/solutions/documents/visa-perc-biannual-report-spring-2025.pdf>

³¹ 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>

³² Visa Public, Bi-Annual Threats Reports: 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)³³.

VAMP has the potential to address

4x

the amount of fraud globally, accounting for more than **US\$2.5 billion** (NZ\$4.2 billion) **in losses**,



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

The new VAMP, effective since 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 one centralised metric which includes all fraud and disputes for both domestic and cross border CNP 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 Central (VERC)**, a case management tool that allows for independent portfolio performance monitoring and improves operational efficiency.

³³ 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>

Continued investment in secure technologies to balance fraud management and improve customer experience



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 limiting the risk exposure in a breach.

As of April 2024, Visa has issued

1 billion³⁴

**tokens in the Asia Pacific region
boosting digital payments while
enhancing security.**

The region's digital economy experienced an uplift of more than US\$2 billion (NZ\$3.3 billion) in 2023 as a result of **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%)³⁵.

Token provisioning challenges

Tokenisation is beneficial for everyone, but its security relies on managing the risks of token provisioning. Tokens can be wrongly issued to bad actors, leading to fraud after the token is activated. Currently, token provisioning fraud in digital wallets involves threat actors quickly using and discarding tokens, focused on rapid monetisation without keeping the credential for long³⁶. Visa found that token provisioning fraud losses reached an estimated US\$450 million (NZ\$751 million) globally in 2022 alone³⁷. 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 (VPI) 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 New Zealand since October 2023, VPIit is designed to help reduce overall ecosystem fraud and increase the number of valid token provisioning requests.

34 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%20B9.>

35 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%20the%201%20billion%20%20milestone%20in%20Asia%20Pacific>.

36 Visa PublicConfidential, Bi-Annual Threat 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>

37 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 cases, 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 engineering³⁸.

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 2027.

Issuers are encouraged to migrate towards more secure authentication methods, such as biometric or in-app authentication, or newer methods like passkeys, app-to-app and app-to-web, 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 request³⁹. A consistently high quantity and quality of data fields help enhance business outcomes for merchants, cardholders and issuers.

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. Another instance is using passkeys. Passkeys are a secure and convenient authentication method that uses biometrics or device-based cryptographic keys to replace traditional passwords which are often vulnerable to phishing.

³⁸ 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>

³⁹ 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>

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 digital payments ecosystem. It not only mitigates fraud but also 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 its effective use can greatly enhance fraud mitigation strategies. This is reflected in various initiatives aimed at bolstering fraud mitigation strategies across the ecosystem:

APR '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 providing 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 supporting investment in low-friction, robust authentication methods⁴⁰.

APR '24



The streamlined **merchant** Payment Card Industry Data Security Standard (**PCI DSS**) **compliance reporting** announced in April 2024 focuses on a risk-based assessment in identification and enforcement⁴¹.

AUG '24



Updated **Visa Secure minimum data requirements** to support issuers' authentication decision-making to determine whether a transaction should be frictionlessly approved or challenged⁴².

OCT '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 2024⁴³.

Updated requirements on Fraud Reporting Systems to include **confirmed fraud on declines** for better model development and to support issuers in making smarter risk-based decisions that drive down fraud⁴⁴.

⁴⁰ 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/>

⁴¹ Visa, Account Information Security Program and PCI, accessed November 2024, <https://corporate.visa.com/en/resources/security-compliance.html#1>

⁴² 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>

⁴³ Visa, Visa Global Acquirer Risk Standards, 1 October 2024, <https://usa.visa.com/dam/VCOM/download/merchants/visa-global-acquirer-risk-standards.pdf>

⁴⁴ Visa, Visa Core Rules and Visa Product and Service Rules, 19 October 2024, <https://usa.visa.com/dam/VCOM/download/about-visa/visa-rules-public.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, Visa can enhance the 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 during 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.

Based on Visa’s authentication data from 2021 to 2023, all New Zealand issuers⁴⁵ have used risk-based authentication since the introduction of EMV 3DS.

The use of risk-based authentication refers to the use of additional data elements in EMV 3DS to ensure seamless, enhanced user experiences for cardholders where transactions are authenticated frictionlessly (with no step-up). Cardholders can complete a secure purchase without experiencing the additional steps typically associated with increased security measures, effectively protecting them from fraud. Issuers in New Zealand have implemented this with varying levels of success, with some stepping up more than others.



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.

⁴⁵ Visa, 3Y Authentication Data ending December 2023, VisaNet (January 2021 – December 2023). Dataset is based on issuer authentication data on NZ issued cards.

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.

AI 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. 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 analytics⁴⁶. 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 help 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.



⁴⁶ 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 New Zealand 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 CNP transactions present 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 CNP conversion rates and poor online experience.



of all accepted eCommerce orders in Asia Pacific today are fraudulent⁴⁷.

While New Zealand saw a decrease in unauthorised fraud of around 10% in 2023, **there was a significant 32% growth in 2024⁴⁸.**

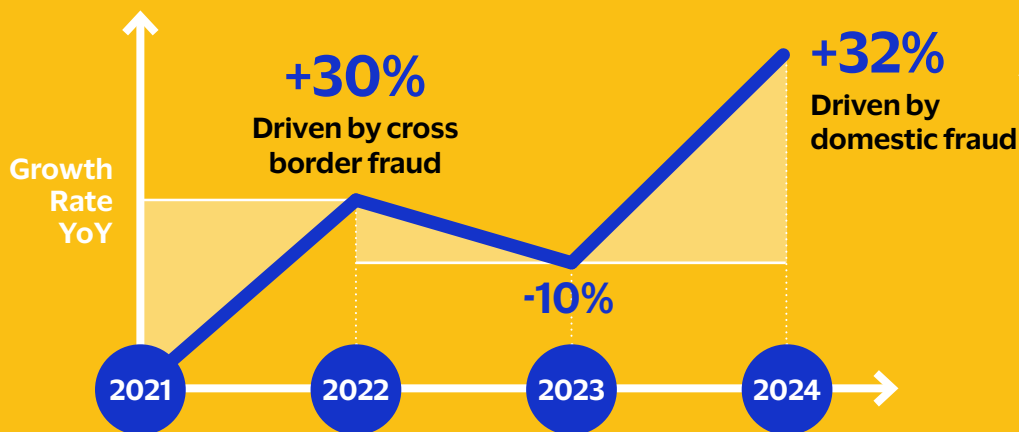


This growth was attributed to an increase in CNP channels across domestic and cross-border transactions, with domestic fraud growing two times faster than cross-border. This was partly due to an increase in issuer fraud reporting related to wire transfers and cryptocurrency merchants, **where a higher number of scam incidents were observed.** Additionally, the rise in fraud can be attributed to an increased number of scam reports to Visa, which further contributed to the overall rise.

⁴⁷ Visa, 2024 Global eCommerce Payments & Fraud Report, 25th Edition, <https://www.cybersource.com/content/dam/documents/campaign/fraud-report/global-fraud-report-2024.pdf>

⁴⁸ Visa, 4 year comparison ending December 2024, VisaNet (January 2021 – December 2024)

FRAUD RATE GROWTH YEAR-ON-YEAR IN NEW ZEALAND



Fraud growth in 2024 is the

highest in the last five years



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 CVV or dynamic CVV2. There is a requirement for merchants to capture the CVV2 in authorisation for all unsecure remote ecommerce transactions (non-authenticated and non-tokenised).

Expanding Account Name Inquiry (ANI), 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

DRIVERS FOR FRAUD GROWTH DIFFERED ACROSS MERCHANT CATEGORY CODE (MCCS) CHANNELS



Domestic CNP fraud

-  Advertising Services
-  Wire Transfers

Cross border CNP fraud

-  Cryptocurrency/ Digital Wallets
-  Travel Agencies
-  Digital Goods
-  Advertising Services

Pacific region will provide ecosystem participants with more data. This additional data will enhance their ability to verify cardholder identities, reduce exposure to fraud and scams in CNP transactions, and make more informed decisions, enhancing their ability to verify cardholder identities and make informed decisions.

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 businesses receive actionable insights to optimise their payments business and deliver a secure customer experience.

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 merchants⁴⁹. 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 cybercrime underground marketplaces.

The Visa Integrity Risk Program (VIRP)⁵⁰ 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, or adversely impact the Visa payment system. The VIRP ensures that acquirers, and their agents, that support High Integrity Risk Merchants (such as gambling, adult content, dating and escort services Merchant Category Codes (MCCs) among others) maintain proper controls and oversight of processes to identify and deter illegal transactions from entering the Visa payment system.

⁴⁹ Visa Public, Biannual Threats Report, June 2023, <https://usa.visa.com/content/dam/VCOM/regional/na/us/support-legal/documents/visa-pfd-biannual-threats-report.pdf>

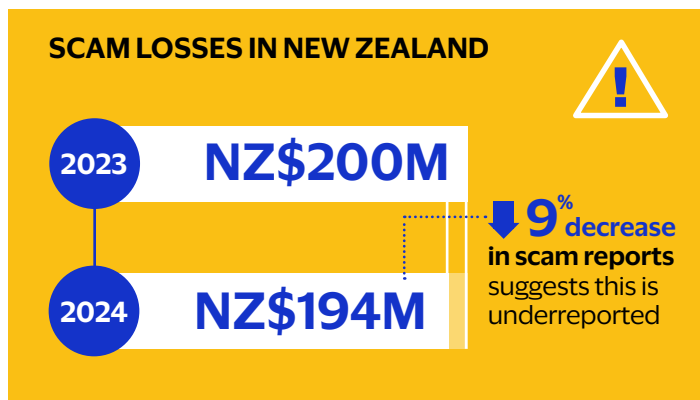
⁵⁰ Visa, Protecting the integrity of the Visa network, 6 April 2023, <https://corporate.visa.com/content/dam/VCOM/corporate/visa-perspectives/documents/protecting-the-integrity-of-the-visa-network.pdf>



Authorised Fraud (scams)

There is increased attention on scams as a growing concern for all participants in New Zealand's digital payment ecosystem. As referenced above, the latest data released in 2024 from PaymentsNZ shows that **NZ\$194 million** was lost to card fraud and scams from 1 October 2023 to 30 September 2024 from 11 of New Zealand's largest financial institutions.

Whilst this figure has fallen slightly compared to the previous year (NZ\$200 million), the Banking Ombudsman Scheme has reported a massive increase in bank impersonation scams as scams become increasingly hard to detect⁵¹.



Conversely, The State of Scams in NZ 2024 report found that there was a 9% decrease in reports made to law enforcement agencies in the same period where 68% of New Zealanders indicated that they did not report scams because they were uncertain of the reporting channels to use and did not believe that reporting would make a difference. This was despite one in two New Zealanders seeing an increase in scam encounters in the last 12 months. This suggests that a significant number of scams could be underreported.



Online shopping scams overtook identity theft as the biggest cause of losses, with advances in artificial intelligence making scams more convincing and harder to detect⁵². But it is increasingly challenging to detect whether AI was used, with 47% of New Zealanders were uncertain on whether AI was used in their scam encounters⁵³. The 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.

⁵¹ Ministry of Business, Innovation & Employment, MBIE is helping New Zealanders spot scams through Fraud Awareness Week, 18 November 2024, <https://www.mbie.govt.nz/about/news/mbie-is-helping-new-zealanders-spot-scams-through-fraud-awareness-week#:~:text=New%20data%20released%20today%20from,New%20Zealand's%20largest%20financial%20institutions>

⁵² NZ Herald, Kiwis lose \$2.3b to digital scams, Government readies three big moves, 18 November 2024, <https://www.nzherald.co.nz/business/kiwis-lose-23b-to-digital-scams-government-readies-three-big-moves/HUX4P5N3ONHLRKLZAJD7DQR2OU/>

⁵³ The State of Scams in NZ 2024 Report, Netsafe, GASA, <https://www.gasa.org/research>



In the same 12 month period, there is a push for initiatives in the New Zealand banking industry for issuers to better protect customers from scams and online fraud. Actions taken by issuers include scams awareness campaigns to educate consumers about common fraud schemes, and establishing interbank sharing of scam information to help identify and reduce fraudulent payments to mule accounts⁵⁴.

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)

uses our extensive experience from **Visa Advanced Authorisation (VAA)** and incorporates deep learning AI detection models to score account-to-account transactions in real-time. This solution has been launched in collaboration with payment operators in the UK and Latin America. Results from the UK pilot revealed Visa identified 54% of fraudulent transactions which had already passed through the banks' sophisticated fraud detection systems without detection, suggesting Visa's proven predictive AI technology is an important contribution to this growing space and could potentially help save £330 million for UK consumers, businesses and the economy⁵⁵.

Additionally, in late December 2024, Visa announced it had completed the acquisition of Featurespace, a developer of real-time 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 clients around the world to grow and protect their businesses⁵⁶.

To further defend the ecosystem and protect consumers against scams, Visa unveiled its scam disruption practice, **Visa Scam Disruption (VSD)**, in March 2025. VSD focuses on identifying and stopping complex scams as they emerge. It combines Visa's proprietary technology with the deep expertise of our cross-disciplinary taskforce to dismantle scam operations. The newly formalised group prevented more than US\$350 million⁵⁷ (NZ\$588 million) in attempted fraud in 2024 using new technology and human-driven processes.

⁵⁴ Ministry of Business, Innovation & Employment, Strengthening bank processes and consumer protections against scams, 29 February 2024, <https://www.mbie.govt.nz/dmsdocument/28096-strengthening-bank-processes-and-consumer-protections-against-scams-open-letter-to-the-new-zealand-banking-industry-pdf>

⁵⁵ 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>

⁵⁶ Visa, Visa to acquire Featurespace, 26 September 2024, <https://investor.visa.com/news/news-details/2024/Visa-to-Acquire-Featurespace/default.aspx>

⁵⁷ Visa, Visa Unveils its Scam Disruption Practice, Helping Protect Consumers and the Financial Ecosystem Globally, 11 March 2025, <https://investor.visa.com/news/news-details/2025/Visa-Unveils-its-Scam-Disruption-Practice-Helping-Protect-Consumers-and-the-Financial-Ecosystem-Globally/default.aspx>

Enhancing the cyber security posture of ecosystem participants

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

In 2023, there was a total of 316⁵⁸ cyber security incidents reported, a 10% decrease compared to the previous year.

However, the proportion of financially-motivated cyber crime activity has exceeded state sponsored activity for the first time, which poses a large risk to the ecosystem. Ransomware 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 – with phishing being the highest observed technique.

In response to these cyber threats, the New Zealand Government is proactively taking measures to bolster its cyber security. In 2023, the Government announced the creation of a lead operational cyber security agency, CERT NZ, to enhance New Zealand's ability to tackle emerging cyber security challenges and provide joined-up, customer-centric services for New Zealanders⁵⁹.



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.

⁵⁸ NCSC, Cyber Threat Report 2022/2023, <https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-2022-2023-Cyber-Threat-Report.pdf>

⁵⁹ NCSC, Government moves to create lead cyber security agency, 26 July 2023, <https://www.ncsc.govt.nz/news/lead-cyber-agency>

Across the digital 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.

IN 2023,

**over a million
New Zealanders**
had their private
information compromised
through significant
data breaches,

one of the country's largest
data breach to date⁶⁰.



**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 Visa⁶¹.

Visa's **Account Information Security Program (AIS)** is a global compliance program dedicated to maintaining the safety and integrity of Visa's payment ecosystem⁶². This is achieved through monitoring compliance and addressing security deficiencies to prevent compromise of Visa account data. Visa has transitioned 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 has shifted 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.

⁶⁰ Office of the Privacy Commissioner (OPC), New Zealand's biggest data breach shows retention is the sleeping giant of data security, 3 April 2023, <https://www.privacy.org.nz/publications/statements-media-releases/new-zealands-biggest-data-breach-shows-retention-is-the-sleeping-giant-of-data-security/>.

⁶¹ To maintain transparency Visa established the public listing of service providers and their current PCI DSS validation status for all ecosystem participants at <https://www.visa.com/splisting/searchGrsp.do>

⁶² 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](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 New Zealanders 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.



As a result **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**⁶³, 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 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 popularity⁶⁴. 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. 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 among New Zealand's 570,000 small businesses⁶⁵.

Finally, Visa continues to pave the way for a new era of commerce with the launch of **Visa Intelligent Commerce**⁶⁶. Visa Intelligent Commerce builds off more than 30 years of expertise working with AI and machine learning to manage risk and fraud to enable safe and secure payment experiences. Together with AI industry leaders including Anthropic, IBM, Microsoft, Mistral AI, OpenAI, Perplexity, Samsung, Stripe and more, Visa will enable personalised, secure AI commerce on a global scale.

⁶³ Visa Payment Passkey Delivers a Modern Authentication Solution, August 2024, <https://corporate.visa.com/en/products/visa-payment-passkey.html#:~:text=Established%20by%20a%20consortium%20of,lock%20to%20authenticate%20the%20consumer.>

⁶⁴ Visa Reinvents the Card, Unveils New Products for Digital Age, May 2024, <https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.20686.html>

⁶⁵ Ministry of Business, Innovation & Employment, Small Businesses in 2022, <https://www.mbie.govt.nz/dmsdocument/27313-small-business-factsheet-2022-pdf>

⁶⁶ Find and Buy with AI: Visa Unveils New Era of Commerce, April 2025, <https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.21361.html>




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 New Zealand 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 Ecommerce landscape and threat environment evolves, driving security alongside payment innovation as we enable new and exciting ways to pay.

Considering our expectations of the New Zealand threat landscape in the coming years, Visa has mapped the steps we are already taking with clients during the three years ahead 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

2026-28 and beyond

 Shift from SMS OTP to more secure authentication methods (biometrics, in-app)

 Preparation for the migration to Advanced Encryption Standard (AES)

 Visa's 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 digital payments 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 <https://www.visa.com/splisting/searchGrsp.do>
- 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 CNP and CP 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
- Use 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, and use secure technologies, such as Click to Pay with EMV® 3DS
- 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 payments 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

Visa Confidential