Visa Business News

VISA

Compliance 2 December 2021

Australia 2021 Security Roadmap Launch

AP (Australia) | *Acquirers, Issuers, Processors, Agents*

Visa Network

Overview: Visa has published an updated Security Roadmap for Australia and will update associated rules. Visa is also providing cybersecurity recommendations and best practice reminders.

Since Visa launched the prior Security Roadmap in August 2017, the payments landscape has changed significantly. New trends have emerged in the payments threat landscape, and this updated Security Roadmap outlines the steps Visa will take to drive trusted outcomes for Australian consumers and businesses.

Mark Your Calendar:

15 October 2022:

- E-commerce merchants must apply enumeration attack prevention controls
- All merchants required to enroll in EMV 3DS

Related Training From Visa University:

- Intermediate Fraud Prevention

Detection and Prevention of Enumeration Attacks

Enumeration is the criminal practice of submitting fraudulent card-not-present (CNP) transactions into the payments ecosystem in order to obtain valid payment information. The most common attack types are:

- **Enumeration Attack:** This is a fraud attack in which a criminal systematically submits transactions with enumerated values for the primary account number (PAN), Card Verification Value 2 (CVV2), expiration date and postal code to derive legitimate payment account details. This type of attack is commonly referred to as a brute force attack.
- **Account Testing Attack:** This is the process of initiating one or two transactions of low dollar amounts to verify if an account is active in order to take it over for illicit means or to sell. Typically, these attacks focus on a single Bank Identification Number (BIN) range.

When criminals submit invalid authorizations in volume, they maximize the resale value of stolen account data, and clients and merchants pay unnecessary fees.

Today, Visa detects enumeration and account testing activity with an advanced capability known as Visa Account Attack Intelligence (VAAI). VAAI uses cutting-edge machine learning to identify account enumeration activity and analyze the details of an attack, and enables Visa to take appropriate action in near-real-time.

As the threat of enumeration attacks is expected to continue, Visa will introduce a requirement for e-commerce payment providers to invest in capabilities to identify and prevent enumeration attacks. **Effective 15 October 2022**, acquirers must ensure that they or their registered third party agents hosting a seller's payment page have the appropriate controls in place to prevent, identify and disrupt enumeration attacks. Acceptable solutions include near-real-time authorization monitoring for anomaly detection on IP addresses, logins or sessions; throttling, or random pauses on account checking; ability to lock accounts after a certain number of login attempts; and CAPTCHA or ReCAPTCHA. For the full list of solutions, please see Visa's *Anti-Enumeration and Account Testing Best Practices for Merchants*.

Investment in Secure Technologies

In the 22 April 2021 edition of the *Visa Business News*, Visa introduced two frameworks designed to enhance readiness, security and performance in the CNP ecosystem. The Secure Credential Framework will introduce differential pricing for token and PAN transactions, fees for services Visa provides on behalf of its clients, and amendments to the benchmark rates and performance requirements for CNP transactions. The Digital Authentication Framework will extend fraud protection to merchants that implement enhancements to EMV® 3-D Secure (3DS) and token authentication interfaces and standards. These changes become **effective 23 April 2022**.

With the 2017 Security Roadmap, Visa introduced a requirement for merchants in certain merchant category codes (MCCs) to enroll in EMV 3DS due to the propensity for fraud in those industries. Given the frequent changes in fraud schemes and Visa's introduction of incentives for the adoption of secure technology, Visa is removing the MCC-specific enrollment requirement for Australian merchants. **Effective 15 October 2022**, all Australian merchants will be required to enable EMV 3DS alongside their other fraud prevention solutions, regardless of MCC. Merchants identified in the Visa Fraud Monitoring Program (VFMP) who have not enabled EMV 3DS will be subject to the High Risk MCC timeline as outlined in the VFMP Program Guide[1] **effective 15 October 2022**.

Note: Visa will sunset EMV 3DS version 1.0.2 by **15 October 2022**. After this date, merchants will not be able to use 3DS v1.0.2 for authentication. Providers will need to work with their merchants who are using the legacy protocol to migrate them to an updated EMV 3DS solution **before 15 October 2022**.

Additionally, it is imperative for issuers to maintain a robust system capable of adjusting to dynamic fraud trends in real-time to limit fraud losses. In the 7 October 2021 edition of the *Visa Business News*, Visa announced a requirement for AP issuers and their processors to implement appropriate real-time risk scoring capabilties for authorization decisioning for all Visa products (except Prepaid products) by **15 October 2022**.

[1] Available for clients and agents only.

Providing Secure Digital Payment Experiences

With cash in Australia expected to account for only 2.1% of sales at the point of sale by 2024,[2] digital payment experiences will drive how Australians pay and get paid for goods and services well into the future. As tokenized Visa credentials can be used to bind a device and a token, issuers can offer their customers instant access to a new or replacement digital Visa card for immediate use. With digital payment credentials, there is no risk of a physical card being lost or stolen, which accounts for most fraud in the face-to-face to environment.

In the 19 August 2021 edition of the *Visa Business News*, Visa announced that **commencing 15 October 2022**, all **newly issued or replacement** contactless cards and contactless payment devices must be configured to support contactless ATM transactions and all cards and devices must have this functionality by **1 October 2030**. By removing the need for a physical card to be inserted at an ATM, Visa aims to address the risk of skimming and reduce subsequent fraudulent spend at other locations.

[2] Global Payments Report, FIS Global, March 2021

Guarding Against Cyber Attacks

Visa routinely identifies cyber threats to the ecosystem and updates its clients and the public through security alerts, intelligence alerts and the biannual Threats Report. These publications include indicators of compromise along with best practices and recommendations to prevent, identify and remediate cyber threats.

Basic data security hygiene is underpinned by global standards. The Payment Card Industry Data Security Standard (PCI DSS) (which is a Visa Supplemental Requirement) sets the technical and operational requirements to help organizations—merchants, financial institutions, payment processors, service providers and technology providers—keep their cyber defenses primed against attacks aimed at stealing accountholder data. As cyber attack trends evolve, so too does the PCI DSS, with the latest version 4.0 expected to be published in early 2022. As with prior versions of the standard, Visa will announce a transition plan for compliance with PCI DSS v4. Visa encourages clients to transition to the updated standards as soon as possible to ensure that data is protected in accordance with the most up-to-date security controls.

Scams

While card fraud in Australia only increased by 0.6% in 2020 from the prior year,[3] scams impacting Australian consumers and businesses have been on the rise. From January 2021 to August 2021, Australians reported losing AUD 211 million in scams, representing an increase of 89% compared to the prior year.[4]

Fraud occurs when a third party obtains unauthorized access to a consumer or business's payment credentials, typically through a data compromise. A scam, on the other hand, occurs when a victim is misled to provide their payment credentials to someone they believe to be a trusted entity. These credentials are then used to perpetrate account takeovers or for unauthorized payments or transfers. In the 11 February 2021 edition of the *Visa Business News*, Visa provided descriptions of common account takeover fraud techniques along with best practices to mitigate the risk of such fraud occurring.

Visa's existing processes and rules aim to prevent the Visa system from being used by scammers to monetize scammed credentials. In the *Visa Global Acquirer Risk Standards (GARS)* (a Visa Supplemental Requirement), Visa outlines requirements for acquirers to manage the risks to their business and the greater ecosystem across onboarding, monitoring and working with third parties. This includes capabilities to identify merchants that may be driving scam activity or that may have become victims of scams. Visa's global fraud and dispute monitoring programs also help to identify and remediate fraud or scam activity.

Despite these controls, Visa recognizes that an industry approach through education and awareness is best to help prevent Australian consumers and businesses from becoming victims of scams. Visa actively works with law enforcement and across industry groups to drive messaging on what to look out for and common scam sources through its Payment Intelligence alerts.

[3] "Australian Payment Fraud 2021," Australian Payments Network

[4] "Losses Reported to Scamwatch Exceed $211 Million, Phone Scams Exploding," Australian Competition & Consumer Commission, 27 September 2021

Ecosystem Resilience

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

Visa also has requirements in place for any entity directly connected to the Visa network regarding the qualifications of personnel managing these connections, along with maintenance of the appropriate access controls, records, documentation and logs.

Additionally, in the event a Visa issuer is unavailable to respond to authorization requests, Visa can stand in to respond on their behalf. Last year Visa announced Smarter Stand-in Processing (STIP), which uses real-time artificial intelligence to help financial institutions manage transaction authorizations when service disruption occurs. Using deep learning to analyze past transactions, Smarter STIP generates informed decisions to approve or decline transactions on behalf of issuers if their systems are unable to respond to authorization requests.

As the payments landscape continues to evolve with new technologies, Visa expects the threat landscape to continue to change. Fraudsters have the ability to leverage new technologies and adapt their attack vectors quickly. Clients should be on the lookout for upcoming changes to Visa's Risk programs and best practices as Visa continues to ensure the safety and security of the evolving ecosystem.

EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo, LLC.

Additional Resources

Advance Copy of the Visa Rules

The advance copy of the upcoming Visa Rules illustrates the associated rule changes that will be reflected in the next edition of the publication. If there are any differences between the published version of the rules and this advance copy, the published version of the rules will prevail.

- *Visa Secure Updates and Introduction of Enumeration Attack Reduction Requirements (Australia and New Zealand) (Advance Copy)*

Documents & Publications

"Updates to Fraud Prevention Requirements," *Visa Business News*, 7 October 2021 (clients and processors only)

"Contactless Issuance Rules Will Be Updated to Require Support for ATM Transactions," *Visa Business News*, 19 August 2021 (clients and processors only)

"Visa Guidance to Guard Against Enumeration Attacks and Account Testing Schemes," *Visa Business News*, 12 August 2021

"Introduction of Secure Credential Framework and Digital Authentication Framework," *Visa Business News*, 22 April 2021

"Best Practices to Mitigate Risk of Account Takeover Fraud," *Visa Business News*, 11 February 2021

"Visa Will Discontinue Support of 3-D Secure 1.0.2," *Visa Business News*, 4 February 2021

"Visa Smarter Stand-In Processing Will Be Introduced," *Visa Business News*, 6 August 2020 (clients and processors only)

Visa Global Acquirer Risk Standards

Online Resources

Payment Systems Intelligence

Visa Fraud Monitoring Program (clients and agents only)

Note: For Visa Online resources, you will be prompted to log in.

For More Information

Contact your local Visa Risk representative. Merchants and third party agents should contact their issuer or acquirer.

Notice: This Visa communication is furnished to you solely in your capacity as a customer of Visa Inc. (through its operating companies of Visa U.S.A Inc., Visa International Service Association, Visa Worldwide Pte. Ltd, Visa Europe Ltd., Visa International Servicios de Pago España, S.R.L.U. and Visa Canada Corporation) or its authorized agent, or as a participant in the Visa payments system. By accepting this Visa communication, you acknowledge that the information contained herein (the "Information") is confidential and subject to the confidentiality restrictions contained in the Visa Rules, 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 Inc. or as a participant in the Visa payments system. You may disseminate this Information to a merchant participating in the Visa payments system if: (i) you serve the role of "acquirer" within the Visa payments system; (ii) you have a direct relationship with such merchant which includes an obligation to keep Information confidential; and (iii) the Information is designated as "affects merchants" demonstrated by display of the storefront icon on the communication. A merchant receiving such Information must maintain the confidentiality of such Information and disseminate and use it on a "need to know" basis and only in their capacity as a participant in the Visa payments system. Except as otherwise provided, the Information may only be disseminated within your organization on a need-to-know basis to enable your participation in the Visa payments system. Visa is not responsible for errors in or omissions from this publication.