



## NEWS RELEASE

---

# Visa Sets Global PCI DSS Deadlines

## *Data Security Compliance Requirements Aligned Across Visa Regions*

---

**Auckland – 11 November 2008** – Visa Inc. (NYSE: V) today announced global mandates for compliance with the Payment Card Industry Data Security Standard (PCI DSS), creating a consistent framework for compliance among merchants, service providers and their agents.

The framework includes a global set of requirements for merchants to validate their compliance with PCI DSS; and for the largest merchants, dates by which they must reach full PCI DSS compliance. Deadlines are also set for large and mid-level merchants to demonstrate that they are not storing certain types of sensitive card data.

Service provider levels and PCI DSS validation requirements have likewise been aligned under a global standard and compliance timeline. In Asia Pacific, Visa has launched a registry of service providers that have been reported to be fully compliant with the PCI DSS. Upon being listed on the registry, service providers are able to promote their services to Visa's global network of 16,600 financial institution clients and millions of merchants. The registry benefits the industry's overall push to protect the electronic payment system and help protect businesses from financial and reputational harm that often results from cardholder data compromises by serving as a valuable resource for issuers, acquirers and merchants that are required to identify and work with PCI DSS compliant service providers.

The new framework establishes the minimum requirements for Visa Inc. regions. As an independent company and licensee of Visa International for the business operations in European markets, Visa Europe's PCI DSS framework requires compliance validation and risk mitigation for Level 1 merchants; however the region will be adhering to a different timeline and process for executing compliance validation.

"Compliance with PCI DSS is vital to ensuring the integrity of the global payments system," said Mike Smith, regional head of Risk Management, Asia Pacific for Visa. "Aligning compliance programs across the Visa regions is the latest step in our commitment to safeguarding cardholder data. In Asia Pacific, apart from implementing these new global mandates and launching the registry of service providers, Visa has run several merchant and client training sessions – most recently in Australia and Japan – to bring local partners up to speed with the new compliance requirements."

### **MERCHANT VALIDATION REQUIREMENTS**

#### **Alignment of Merchant Levels and PCI DSS Validation Requirements**

A comprehensive set of international security requirements for safeguarding cardholder data, PCI DSS was developed by Visa along with the four other founding payment brands of the PCI Security Standards Council. Compliance is required of all merchants and any entity that stores, processes or transmits cardholder data.

Validation of compliance is part of that process, with validation requirements varying for merchants based on factors such as transaction volume. Visa has globally aligned merchant levels and annual PCI DSS validation requirements as follows:

Level / Tier <sup>1</sup>	Merchant Criteria	Validation Requirements
1	Merchants processing over 6 million Visa transactions annually (all channels) <b>or</b> Global merchants identified as Level 1 by any Visa region <sup>2</sup>	<ul style="list-style-type: none"> <li>▪ Annual Report on Compliance (“ROC”) by Qualified Security Assessor (“QSA”)</li> <li>▪ Quarterly network scan by Approved Scan Vendor (“ASV”)</li> <li>▪ Attestation of Compliance Form</li> </ul>
2	Merchants processing 1 million to 6 million Visa transactions annually (all channels)	<ul style="list-style-type: none"> <li>▪ Annual Self-Assessment Questionnaire (“SAQ”)</li> <li>▪ Quarterly network scan by ASV</li> <li>▪ Attestation of Compliance Form</li> </ul>
3	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually	<ul style="list-style-type: none"> <li>▪ Annual SAQ</li> <li>▪ Quarterly network scan by ASV</li> <li>▪ Attestation of Compliance Form</li> </ul>
4	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually	<ul style="list-style-type: none"> <li>▪ Annual SAQ recommended</li> <li>▪ Quarterly network scan by ASV if applicable</li> <li>▪ Compliance validation requirements set by acquirer</li> </ul>

<sup>1</sup> – Compromised entities may be escalated at regional discretion

<sup>2</sup> – Merchant meeting Level 1 criteria in any Visa country/region that operates in more than one country/region is considered a global Level 1 merchant. Exception may apply to global merchants if no common infrastructure and if Visa data is not aggregated across borders; in such cases merchant validates according to regional levels.

Acquirers are responsible for their merchant customers’ compliance and must provide regular compliance status reports to Visa on their Level 1, 2 and 3 merchants at least twice a year. Compliance validation guidelines for Level 4 merchants will be determined by their respective acquirers

**Prohibited Data Storage Deadline for Level 1 and 2 Merchants – 30 September 2009**

Visa will require confirmation from acquirers by 30 September 2009 that their Level 1 and 2 merchants do not retain sensitive payment card data such as full magnetic stripe (also known as track data), security codes or PIN data after transaction authorization.

"Hackers are looking for this type of data because of its use in counterfeiting payment cards, and that is why Visa prohibits its storage," said Smith.

After the deadline, Visa will impose appropriate risk controls, up to and including acquirer fines for failure to provide an attestation form to Visa confirming that each of the acquirer’s Level 1 and 2 merchants do not retain prohibited data.

**PCI DSS Compliance Validation Deadline for Level 1 Merchants – 30 September 2010**

Visa will require acquirers to provide an Attestation of Compliance for each of their Level 1 merchants demonstrating that each has validated full PCI DSS compliance by 30 September 2010. After that date, Visa will impose appropriate risk controls, up to and including acquirer fines for failure to provide an attestation form to Visa confirming that each of its Level 1 merchants has validated full PCI DSS compliance. The 30 September 2010 deadline does not supersede any applicable earlier regional deadlines and related enforcement programs previously established.

**SERVICE PROVIDER VALIDATION REQUIREMENTS**

**Alignment of Service Provider Levels and PCI DSS Validation Requirements**

Effective 1 February 2009, service providers that store, process or transmit Visa cardholder data on behalf of Visa acquirers, issuers, merchants or other service providers will fall into one of two service provider levels:

Level	All Regions	Validation Requirements	Result
1 <sup>1</sup>	VisaNet processors or any service provider that stores, processes and / or transmits over 300,000 transactions per year	<ul style="list-style-type: none"> <li>• Annual ROC by QSA</li> <li>• Quarterly network scan by ASV</li> <li>• Attestation of Compliance Form</li> </ul>	Included on Visa's list of compliant Service Providers
2	Any service provider that stores, processes and / or transmits less than 300,000 transactions per year	<ul style="list-style-type: none"> <li>▪ Annual SAQ</li> <li>▪ Quarterly network scan by ASV</li> <li>▪ Attestation of Compliance Form</li> </ul>	Not included on Visa's list / Confirmation Letter of Receipt <sup>2</sup>

<sup>1</sup> – Eliminates gateway definition from several existing regional programs

<sup>2</sup> – May choose to validate as a Level 1 service provider to be included in Visa's List of Compliant Service Providers

### Registry of Service Providers Program

Visa launched the Registry of Service Providers in November 2008 for payment service providers in Asia Pacific to report their PCI DSS compliance directly to Visa. Visa will charge an annual registration fee of US\$5,000 to registered service providers who will then have a competitive edge in promoting their services to Visa's global network of financial institutions and merchants.

The Registry of Service Providers lists payment service providers that have been reported to be fully compliant with the PCI DSS through onsite reviews conducted by Qualified Security Assessors (QSA). The registry is available at [www.visa-asia/spregistry](http://www.visa-asia/spregistry).

"Standardizing compliance requirements better addresses the security risks in our truly global marketplace and is critical to ensuring the future growth of electronic payments worldwide," Smith concluded.

### Summary of Aligned Framework by Date

Effective Date	Globally Aligned Mandate
February 1, 2009	Effective date for globally aligned Service Provider level definitions
September 30, 2009	Acquirers must attest that Level 1 and 2 merchants do not retain prohibited payment card data subsequent to authorization of a transaction
September 30, 2010	PCI DSS compliance validation deadline for Level 1 merchants

### About Visa

Visa operates the world's largest retail electronic payments network providing processing services and payment product platforms. This includes consumer credit, debit, prepaid and commercial payments, which are offered under the Visa, Visa Electron, Interlink and PLUS brands. Visa enjoys unsurpassed acceptance around the world and Visa/PLUS is one of the world's largest global ATM networks, offering cash access in local currency in more than 170 countries. For more information, visit [www.corporate.visa.com](http://www.corporate.visa.com).

###

### Contact:

Sarah Ward, Porter Novelli, Telephone: (09) 632 0524, [sarahw@porternovelli.co.nz](mailto:sarahw@porternovelli.co.nz)