



DATA SECURITY BULLETIN

Visa PCI DSS Compliance Validation Framework

November 18, 2008

Visa announces enhancements to its data security programs to further ensure the security of the Visa payment system. The enhancements outlined herein are aimed at driving greater validation of compliance with the Payment Card Industry Data Security Standard (PCI DSS), an important component of Visa's strategy to prevent cardholder data compromises which contribute directly to increased fraud and cardholder confidence concerns. Visa data security compliance programs have provided compelling incentives for large merchants and agents to properly secure cardholder data. The described program enhancements will provide a foundational framework for PCI DSS compliance validation among merchants and service providers across Visa regions.

The Payment Card Industry Data Security Standard (PCI DSS) is a comprehensive set of international security requirements for safeguarding cardholder data. The PCI DSS was developed by Visa, along with the four other founding payment brands of the PCI Security Standards Council, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS requirements are the foundation of Visa's data security compliance programs, including the Account Information Security (AIS) Program and Cardholder Information Security Program (CISP).

Visa is committed to protecting the Visa payment system and Visa cardholder data and appreciates the efforts by Visa issuers, acquirers, merchants and stakeholders to drive data security objectives. Compliance with the PCI DSS results in benefits beyond simply securing cardholder data as sound security practices also help to protect organizations from adverse financial and reputational consequences often associated with cardholder data compromises.

Compliance with the PCI DSS is currently required of any entity that stores, processes or transmits Visa cardholder data. To ensure compliance, Visa has implemented a consistent PCI DSS compliance validation framework within its regions. This new framework establishes baseline compliance requirements for merchants and service providers focused on validation and enforcement of PCI DSS compliance.

This framework establishes the minimal requirements for Visa International regions to follow. Visa International regions include Asia-Pacific (AP); Canada; Central and Eastern Europe, Middle East and Africa (CEMEA); Latin America and Caribbean (LAC); and USA. Visa Europe operates as an independent company and licensee of Visa International for the business operations in the Visa Europe markets. Visa Europe's PCI DSS framework is modeled on the same principles as the framework established by Visa International. Compliance validation and risk mitigation for Level 1 merchants are obligatory for merchants operating in Visa Europe's markets. The Visa Europe policy on the applicable timeframes for Level 1 merchants to achieve compliance entails acquirers entering into agreements with their retailers for specific compliance validation dates. For further information on the Visa Europe framework, please contact datasecuritystandards@visa.com.



Merchant PCI DSS Compliance Framework

Merchant Levels and Validation Requirements

In addition to mandates for complying with the PCI DSS, Visa has defined validation levels based on transaction volume, potential risk and exposure introduced into the Visa system. The following are merchant levels and validation requirements for annual PCI DSS compliance validation:

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

¹Compromised entities may be escalated at regional discretion.

²A 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. Exceptions may apply to global merchants if no common infrastructure exists or if Visa data is not aggregated across borders; in such cases the merchant validates according to regional levels.

Acquirers are responsible for identification of merchant validation level based on the number and type of transactions processed by that acquirer. Acquirers must notify Visa of new Level 1 and 2 merchants annually. Merchant level identification is based on the corporate entity's total volume meeting the transaction thresholds in one country or with one acquirer per year. Volume from independently owned and operated merchant locations (e.g., franchisee, licensee) may be excluded if it is not handled by the corporate entity.

Additionally, acquirers must provide reports to Visa on the compliance status of their Level 1, 2 and 3 merchants at least twice a year. Visa reserves the right to require submission of individual merchant compliance validation documentation from the acquirer.



Note: These global merchant levels are consistent with current merchant levels in the U.S. The framework does not represent any change to the current U.S. merchant compliance program validation requirements or deadlines.

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

Visa will require confirmation from acquirers that Level 1 and 2 merchants do not retain sensitive authentication data (i.e., full magnetic stripe/track, CVV2 or PIN data) after transaction authorization in violation of Visa rules by **September 30, 2009**. After this date, Visa will impose appropriate risk controls, up to and including fines, on acquirers that fail to provide an Attestation of Compliance Form to Visa confirming that each of its Level 1 and 2 merchants do not retain prohibited magnetic stripe, CVV2 and PIN data. The September 30, 2009, deadline does not supersede any applicable earlier regional deadlines and related enforcement programs previously established.

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

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

Note: In the U.S., the PCI Compliance Acceleration Program (CAP) has established earlier deadlines. The deadlines noted previously do not impact U.S. merchants.

Service Provider PCI DSS Compliance Framework

Service Provider Levels and 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
1¹	VisaNet processors or any service provider that stores, processes and/or transmits over 300,000 transactions per year	<ul style="list-style-type: none">• Annual ROC by QSA• Quarterly network scan by ASV• Attestation of Compliance Form	Included on Visa's List of PCI DSS 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">▪ Annual SAQ▪ Quarterly network scan by ASV▪ Attestation of Compliance Form	Not included on Visa's List of PCI DSS Compliant Service Providers/Confirmati



			on Letter of Receipt ²
--	--	--	-----------------------------------

¹Eliminates gateway definition from several existing regional programs.

²May choose to validate as a Level 1 service provider to be included in Visa's List of PCI DSS Compliant Service Providers.

In addition to aligning service provider validation levels globally, Visa will implement a common PCI DSS compliance validation process for all service providers. **Effective February 1, 2009**, Visa will only require submission of an executed Attestation of Compliance Form and the "Executive Summary" section of the service provider's Report on Compliance (ROC) to demonstrate PCI DSS compliance as a Level 1 service provider. Level 2 service providers will submit version D of the Self-Assessment Questionnaire (SAQ). Visa will not review the contents of the SAQ as issuers and acquirers are responsible for reviewing the accuracy of the SAQ.

All materials should be sent securely via PGP encryption to pciocs@visa.com. If PGP is not available, please contact Visa at pcidss@visa.com to discuss an alternative submission method. Qualified Security Assessors (QSAs) must submit only fully executed Attestation of Compliance forms, properly signed by the QSA and the service provider confirming compliance with the PCI DSS. The ROC Executive Summary must clearly state the scope of the service provider's PCI DSS assessment. Visa reserves the right to require submission of a service provider's complete ROC.

In the U.S., these global service provider levels and new PCI DSS compliance validation submission process will go into effect on February 1, 2009. U.S. service providers that validate PCI DSS compliance and submit their required PCI DSS compliance validation documentation to Visa prior to February 1, 2009, will be accepted under previous service provider levels and submission process.

List of PCI DSS Compliant Service Providers

In February 2009, Visa will publish a new "List of PCI DSS Compliant Service Providers," which will include PCI compliant service providers within its regions, available at www.visa.com/cisp. This list is a tool for Visa issuers, acquirers, merchants and stakeholders in order to identify and use PCI DSS compliant service providers. Visa requires Level 1 service providers to validate PCI DSS compliance every 12 months. Visa's List of PCI DSS Compliant Service Providers denotes service providers that are 1 to 60 days delinquent in re-validation in yellow and those that are 60 to 90 days late in red. A service provider that does not revalidate PCI DSS compliance within 90 days of its annual due date will be removed from the list.

All service providers must be properly registered with Visa as an agent prior to being listed on Visa's List of PCI DSS Compliant Service Providers. Level 2 service providers will not be listed on Visa's List of PCI DSS Compliant Service Providers. Only Level 2 service providers that opt to undergo a Level 1 onsite security assessment will be listed. Service providers who validate



PCI DSS compliance with an annual SAQ and quarterly network scan prior to February 1, 2009, will be grandfathered on Visa's list until their next annual revalidation date.

For More Information

Please go to www.visa.com/cisp for information about this framework and Visa's U.S. data security programs.