



CISP BULLETIN

Changes to Merchant Validation Levels for the Payment Card Industry Data Security Standard

July 18, 2006

This bulletin details the changes to merchant validation levels for the Payment Card Industry Data Security Standard ("PCI DSS"). The revision broadens the definition of level 2 to include all acceptance channels so it is no longer limited strictly to e-commerce transactions. Merchants new to level 2 are required to validate PCI DSS compliance with members by September 30, 2007. Changes to merchant validation levels are effective immediately.

Since June 2001, the *Visa U.S.A. Inc. Operating Regulations* have required that a member comply, and ensure its merchants and agents comply, with the Cardholder Information Security Program ("CISP"). To maintain the effectiveness of the PCI DSS and related CISP validation processes, Visa USA (in conjunction with MasterCard) revised the merchant validation levels to better reflect the risks present in the marketplace. For convenience, a table is provided below that maps the new merchant levels to previous levels. The validation requirements for each level remain unchanged. Acquirers may choose to implement more stringent validation requirements as needed. Service provider levels are not being revised at this time but will be reviewed shortly to determine if modifications are warranted.

New Merchant Levels Defined (Effective Immediately)

Merchant Level	New Criteria	Prior Criteria	Required Validation Action
Merchant Level 1	No change.	Any merchant processing over 6,000,000 Visa transactions per year or compromised in the past year, regardless of acceptance channel.	No change to validation action for this level. Annual onsite audit and quarterly scans required.
Merchant Level 2	Any merchant processing 1 million to 6 million Visa transactions per year, regardless of acceptance channel.	Any merchant processing between 150,000 and 6 million Visa e-commerce transactions per year.	No change to validation action, but new definition expands the number of level 2 merchants to include former level 4 merchants. Annual self-assessment questionnaire and quarterly scans required.



New Merchant Levels Defined (Effective Immediately) (Continued)

Merchant Level	New Criteria	Prior Criteria	Required Validation Action
Merchant Level 3	Any merchant processing 20,000 to 1 million Visa e-commerce transactions per year.	Any merchant processing 20,000 to 150,000 Visa e-commerce transactions per year.	No change to validation action, but new definition expands level 3 to include merchants formerly in level 2 processing fewer than 1 million e-commerce transactions per year. Annual self-assessment questionnaire and quarterly scans required.
Merchant Level 4	Any merchant processing less than 20,000 Visa e-commerce transactions per year, and all other merchants processing up to 1 million Visa transactions per year.	Any merchant processing less than 20,000 Visa e-commerce transactions per year, and all other merchants processing up to 6 million Visa transactions per year.	No change to validation action, but new definition reduces the number of level 4 merchants. Annual self-assessment questionnaire and quarterly scans may be required as specified by the member.

Acquirer Validation Requirements

Acquirers have until September 30, 2007 to ensure their newly-identified level 2 merchants validate compliance. Members are responsible for identifying merchant validation levels and notifying their merchants of the appropriate compliance requirements. Generally, merchants identified by members as reaching any new/increased merchant level will have 12 months from time of identification to provide members with fully compliant validation documentation, unless the member requires validation sooner.

Acquirers will be required to provide Visa with a list of their level 2 merchants no later than September 30, 2006. Acquirers remain responsible for maintaining all compliance validation documentation, including the *Self-Assessment Questionnaire* and quarterly *System Perimeter Scan Report*. Compliance documentation must be made available to Visa upon request. If the results of the questionnaire or scan indicate areas within a merchant's operation that require remediation to become compliant, the member has the responsibility to ensure compliance is achieved.

How to Determine Merchant Validation Levels

Acquirers are responsible for determining the compliance validation levels of their merchants. To maintain effective compliance programs, Visa recommends that acquirers review merchant volumes on a quarterly basis. Additionally, Visa will validate merchant lists with acquirers on an annual basis. All merchants will fall into one of the four merchant levels based on Visa transaction volume over a 12-month period. Transaction volume is based on the aggregate number of Visa transactions (inclusive of credit, debit and prepaid) from a merchant Doing Business As ("DBA"). The table below is intended to help members determine validation levels for merchants with multiple DBAs and for those that operate franchise organizations.



Validation Levels for Merchants with Multiple DBAs or Franchise Organizations

Scenario	Merchant Validation Levels Determined Based On	Scope of Audit
1) Corporate entity stores, processes or transmits cardholder data on behalf of all of their DBAs.	For the corporate entity, cumulative volume of all transactions stored, processed or transmitted by the corporate entity (inclusive of all DBA volume).	Corporate entity and all DBAs, including point-of-sale locations for each DBA.
2) Corporate entity stores, processes or transmits cardholder data on behalf of a portion of their DBAs.	For the corporate entity, cumulative volume of all transactions stored, processed or transmitted by the corporate entity (inclusive of covered DBA volume). For each individual DBA not covered under the corporate entity, the cumulative volume of all transactions stored, processed or transmitted by the DBA.	Corporate entity and DBAs, including point-of-sale locations for each DBA. Individual DBA, including point-of-sale locations for the DBA.
3) Corporate entity does not store, process or transmit cardholder data on behalf of any of their DBAs.	For each individual DBA , cumulative volume of all transactions stored, processed or transmitted by the individual DBA.	Individual DBA, including point-of-sale locations for the DBA.
4) Corporate entity stores, processes or transmits cardholder data on behalf of franchise locations.	For the corporate entity , cumulative volume of all transactions stored, processed or transmitted by the corporate entity (inclusive of all company-owned locations and data handled on behalf of franchises). For the franchise , individual transaction volume.	Corporate entity to include corporate operations, company-owned locations and data handled on behalf of franchises. Individual franchise operations.
5) Corporate entity does not store, process or transmit cardholder data on behalf of franchise locations.	For the corporate entity , cumulative volume of all transactions stored, processed or transmitted by the corporate entity (inclusive of all company-owned locations). For the franchise , individual transaction volume.	Corporate entity to include corporate operations and company-owned locations. Individual franchise operations.

An acquirer must ensure that all of its merchants adhere to the PCI DSS, regardless of validation requirements. To comply with the spirit of the program, acquirers should always strive to ensure that all payment card transactions handled by their merchants are secured in compliance with the PCI DSS. In this regard, Visa strongly encourages acquirers to establish compliance validation requirements for their level 4 merchants. Acquirers may implement a risk-based approach in requiring validation of level 4 merchants, considering factors such as



volume, market segment, acceptance channel or other risk factors. In sum, Visa encourages acquirers to educate all of their merchants on the importance of data security and of minimizing the data retained by the merchant.

For additional information on merchant validation requirements and/or the PCI Data Security Standard, visit the CISP Web site at www.Visa.com/cisp.