CISP BULLETIN

Level 4 Merchant Compliance Program Requirements

May 14, 2007

The Visa Cardholder Information Security Program (CISP) requires acquirers to ensure that their merchants maintain compliance with the Payment Card Industry Data Security Standard (PCI DSS). As part of CISP, Visa has established risk-prioritized merchant validation requirements based on the volume of transactions and the potential risk introduced into the payment system. Acquirers are required to ensure that their Level 1, 2 and 3 merchants validate PCI DSS compliance annually. While acquirers are required to ensure their Level 4 merchants comply with the PCI DSS, validation is currently at the discretion of acquirers. Though Level 4 merchants handle fewer transactions than Level 1, 2, or 3 merchants—cumulatively less than one third of all Visa transactions—they account for more than 99 percent of the merchants that accept Visa. Consequently, cardholder data compromises affect Level 4 merchants with greater frequency than Level 1, 2 and 3 merchants combined.

Level 4 Merchant Compliance Program

In an effort to stem the number of cardholder data compromises, Visa is requiring acquirers to develop a formal written compliance program that identifies, prioritizes and manages overall risk within their Level 4 merchant populations. Many acquirers have already provided Visa with a summary of their plans to address Level 4 merchant compliance as part of the PCI Compliance Acceleration Program (CAP). Acquirers that have yet to provide their plans must e-mail a summary of their Level 4 merchant compliance plan to cisp@visa.com by July 31, 2007. Acquirers that do not provide their plans by this deadline may be subject to the imposition of risk controls. The Level 4 merchant compliance plan must include: 1) a timeline of critical events; 2) a risk-profiling strategy; 3) a merchant education strategy; 4) a compliance strategy; and 5) compliance reporting.

1) Timeline of Critical Events

- Outline target completion dates for the overall strategy.
- Summarize plans to monitor progress of program execution and provide updates to Acquirer Audit and Risk or other appropriate executive management committee.

2) Risk-Profiling Strategy

- Define a process that prioritizes Level 4 merchants into appropriate risk categories or subgroups in order to efficiently focus security efforts on those merchants that pose the greatest potential risk to the payment system. Factors such as likelihood of sensitive data retention, transaction volume, market segment, acceptance channel, number of locations and other factors can help qualify or quantify the risk a merchant poses and may be used to categorize merchants into specific risk subgroups within an acquirer portfolio. Refer to the attached Risk Prioritization document for examples.

- Outline a process to prioritize Level 4 merchant subgroups and target compliance efforts for each subgroup.

3) Merchant Education Strategy

- Describe plans to educate Level 4 merchants about cardholder data security, storage of prohibited cardholder data and PCI DSS compliance. Include the planned communication channels and approximate frequency.
- Describe the methodology for distributing pertinent Visa communications, such as data security alerts, bulletins and webinars, to merchants in order to increase awareness of critical security risks. Acquirers should encourage their merchants to visit www.visa.com/cisp.

4) Compliance Strategy

- Apply targeted compliance measures to merchant subgroups based upon the following risk-prioritized steps:

  1) Eliminate prohibited data

  2) Protect stored data

  3) Secure the environment in accordance with the PCI DSS
- Develop an approach to verify that prohibited cardholder data (e.g., full magnetic stripe, CVV2 and PIN data) is not retained after transaction authorization.
- Establish a strategy to identify the payment applications (including application vendor and version) used by Level 4 merchants and ensure that the applications are included on Visa's List of Payment Application Best Practices-Validated Payment Applications, available at www.visa.com/cisp. Also ensure that merchants do not use a payment application that has been previously identified as storing prohibited data. Refer to "Visa Alerts Members about Payment Applications that Store Prohibited Data" (*Visa Business Review*, Issue No. 070227) for a list of vulnerable payment applications, and monitor for updates.
- Establish a strategy to ensure that third-party agents used by Level 4 merchants have validated PCI DSS compliance and are included on Visa's List of CISP-Compliant Service Providers, available at www.visa.com/cisp.
- Outline a plan to ensure merchants that have a business need to retain cardholder account numbers are adequately protecting the data in accordance with PCI DSS.

5) Compliance Reporting

- Monitor progress of program execution on a monthly basis. This should include regular reporting to executive management and the board as appropriate. Visa reserves the right to request that acquirers periodically provide these compliance progress reports to Visa.

Data security is a shared responsibility among all payment system participants. Visa is committed to increasing cardholder data security awareness by providing communications, webinars, training and support to acquirers, merchants, agents, software vendors and ISOs. Visa will continue to work with acquirers in support of Level 4 merchant compliance efforts and provide assistance to facilitate the completion of acquirers' Level 4 merchant compliance plans. Level 4 plans must be e-mailed to cisp@visa.com by July 31, 2007.

Risk Prioritization

Visa recommends that acquirers define a process that prioritizes Level 4 merchants into appropriate risk categories or subgroups in order to efficiently focus security efforts on those merchants that pose the greatest potential risk to the payments system. In devising a risk-prioritized approach, acquirers should evaluate the impact exposure of noncompliance, such as fines for noncompliance and the potential liability and costs in the event of a data compromise. Evaluating the likelihood of a data compromise is equally important. Following are examples of risk-prioritization considerations that can be used to determine the impact exposure and likelihood of a data compromise.

Risk Consideration	Lower Risk	Higher Risk
Acceptance Channel	Card not present	Card present
Payment Technology	Stand-alone POS terminal	Integrated POS terminal
Transaction Volume	Low	High
Number of Locations	<5	>5
Merchant Category		Restaurants, universities

Acceptance Channel – Based on a merchant's acceptance channel, acquirers can determine the potential exposure in the event of a compromise. Magnetic stripe data handled by card-present merchants, if compromised, may increase the potential for fraud exposure as well the acquirer's exposure to fines. Compromises of Interlink-accepting merchants, which involve PIN data in addition to magnetic stripe data, have been found to exacerbate the exposure even further.

Payment Technology – Merchants using integrated point-of-sale (POS) systems inherently present greater risk than those using stand-alone dial-up POS systems.

Transaction Volume – Merchants with the potential to lose larger amounts of cardholder data pose a greater risk to acquirers than those who handle less data.

Number of Locations – Increasing the number of merchant locations operating under a common name has been found to increase the likelihood of compromise of a given merchant. This can be attributed to brand recognition and expectations that multiple locations may share common vulnerabilities.

Merchant Category – A merchant's industry segment, defined by Merchant Category Code (MCC), may affect the likelihood of a data compromise. Criminals may target specific industry segments, assuming that common vulnerabilities may exist across that industry. For example, over the past year Visa has found restaurants to be targeted more than any other merchant industry segment.

For more information on Visa's Cardholder Information Security Program, please visit http://www.visa.com/cisp. Questions about this bulletin may be directed to CISP@Visa.com. For the complete VBR, Visa members may refer to the *Visa Business Review* article, "Level 4 Merchant Compliance Program Requirements", May 2007; Issue 070508.