

# MasterCard Quarterly Newsletter

## Q2 2009 PCI Update



### **MasterCard Site Data Protection Program**

#### **SDP Program Revisions Effective Immediately**

Due to the number of high profile account data compromise (ADC) events over the past several years and the subsequent noted increase in counterfeit and card-not-present fraud, MasterCard is announcing revisions to the MasterCard Site Data Protection (SDP) Program mandate to help ensure member, merchant, Third Party Processor (TPP), and Data Storage Entity (DSE) compliance with the Payment Card Industry Data Security Standard.

**Site Data Protection Program Revisions include the following:**

<p><b>Revised Noncompliance Assessment Structure</b></p>	<p>New SDP Noncompliance Assessment Structure</p> <p style="text-align: right;">Per Calendar Year</p>			
	<p><b>Entity Classification</b></p>	<p><b>Assessment Amount (USD)</b></p>	<p><b>Assessment Amount (BRL)<sup>1</sup></b></p>	<p><b>Occurrence</b></p>
	<p>Level 1 &amp; 2 Merchants</p>	<p>Up to USD 25,000</p> <p>Up to USD 50,000</p> <p>Up to USD 100,000</p> <p>Up to USD 200,000</p>	<p>Up to BRL 70,000</p> <p>Up to BRL 140,000</p> <p>Up to BRL 280,000</p> <p>Up to BRL 560,000</p>	<p>First Violation</p> <p>Second Violation</p> <p>Third Violation</p> <p>Fourth Violation</p>
	<p>Level 3 Merchants</p>	<p>Up to USD 10,000</p> <p>Up to USD 20,000</p> <p>Up to USD 40,000</p> <p>Up to USD 80,000</p>	<p>Up to BRL 25,000</p> <p>Up to BRL 50,000</p> <p>Up to BRL 100,000</p> <p>Up to BRL 200,000</p>	<p>First Violation</p> <p>Second Violation</p> <p>Third Violation</p> <p>Fourth Violation</p>
	<p>Level 1 &amp; 2 Service Providers</p>	<p>Up to USD 25,000</p> <p>Up to USD 50,000</p> <p>Up to USD 100,000</p> <p>Up to USD 200,000</p>	<p>Up to BRL 70,000</p> <p>Up to BRL 140,000</p> <p>Up to BRL 280,000</p> <p>Up to BRL 560,000</p>	<p>First Violation</p> <p>Second Violation</p> <p>Third Violation</p> <p>Fourth Violation</p>
<p><sup>1</sup>For Brazilian members that have entered into a specific services agreement with the MasterCard local operating subsidiary in Brazil, MasterCard Brasil Soluções de Pagamento Ltda. (*Permanent Establishment—PE*), prices are denominated in Brazilian reais (BRL)</p> <p>The SDP noncompliance assessment structure now contains escalating assessments per violation within a calendar year. Maximum assessments for initial noncompliance for Level 2 and Level 3 merchants have increased to USD 25,000 and USD 10,000, respectively. Furthermore, the USD 500,000 annual aggregate maximum for acquirer noncompliance assessments related to SDP Program noncompliance has been discontinued.</p>				
<p><b>New Requirements for Level 1 Merchants</b></p>	<p>To fulfill this requirement by the 31 December 2010 deadline, MasterCard strongly encourages all Level 1 merchants engage a PCI SSC certified QSA immediately.</p>			
<p><b>New Requirements for Level 2 Merchants</b></p>	<p>Effective 31 December 2010, all Level 2 merchants must complete an annual onsite assessment conducted by a PCI SSC certified QSA. To fulfill this requirement by the 31 December 2010 deadline, MasterCard strongly encourages all Level 2 merchants engage a PCI SSC certified QSA immediately.</p>			
<p><b>Reclassification of Level 1 Service Providers</b></p>	<p>Effective immediately, all TPPs (regardless of volume) and DSEs with greater than 300,000 annual transactions are considered Level 1 Service Providers.</p>			
<p><b>Reclassification of Level 2 Service Providers</b></p>	<p>Effective immediately, all DSEs with 300 000 or less annual transactions are considered level 2 Service Providers</p>			

For further details on the above revisions to the SDP program, please visit [www.mastercardonline.com](http://www.mastercardonline.com) where you can view the [June 15, 2009](#) Global Security Bulletin.



## How Does the New Prioritized Approach Affect SDP Quarterly Reporting?

### PCI SSC Tools for Prioritized Approach

The PCI Council has developed a reference document outlining the Prioritized Approach for merchants and service providers. Additionally, the PCI Council has also created a Prioritized Approach Tool for merchants and service providers to measure and track their progress. This tool also allows them to print an attestation form to demonstrate progress towards PCI Compliance.

### Revised MasterCard Acquirer Submission and Compliance Status Form – Available for Q2 Reporting

As of second quarter 2009, MasterCard has introduced six new reporting fields in the MasterCard Acquirer Submission and Compliance Status Form (V3.1) to represent the six milestones within the PCI DSS Prioritized Approach, with a seventh field for SAQ Type. This updated status form will better enable the merchant, the acquirer, and MasterCard to track PCI DSS compliance progress using the Prioritized Approach.

**Please Note: Enforcement of these six new reporting fields only applies to merchants eligible for SAQ D and onsite assessments.**

These fields are optional fields for second quarter and third quarter 2009 reporting. However, these fields become mandatory in fourth quarter 2009 for merchants, acquirers, and service providers that are working toward PCI compliance. This is mandatory for all ADC cases for 2nd quarter 2009 reporting.

MasterCard will continue to provide additional information on this new approach in the coming months. More information regarding the updates to reporting is available in the MasterCard Security Bulletin released May 15, 2009. All Global Security Bulletins can be found at [www.mastercardonline.com](http://www.mastercardonline.com).

The Prioritized Approach was announced on March 3, 2009 by the PCI Council and is available on the PCI SSC website at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org). The new MasterCard Acquirer Submission and Compliance Status Form (V3.1) is available for Q2 SDP reporting and can be found at [www.mastercard.com/sdp](http://www.mastercard.com/sdp). Please be sure to communicate this to your merchant population. You can also visit the PCI SSC website where you can view the Prioritized Approach webinar at your convenience at <https://www.pcisecuritystandards.org/education/webinars.shtml>.

## Completeness of Reporting

As you continue to work with your merchant base in driving compliance, it is important to ensure that each merchant is engaged and making progress. All acquirers are reminded that MasterCard continues to focus on consistency, completeness and accuracy of the quarterly reporting process. Your continued commitment to data security and preserving the integrity of the payment system is much appreciated.

### **Please Note: There are two steps to be completed when reporting merchants to MasterCard**

1. Quarterly reporting to MasterCard using the MasterCard Acquirer Submission and Compliance Status Form
2. Registering PCI compliant merchants in the MasterCard Registration Program (MRP) signifying compliance with the SDP Program mandate

### **As a reminder...**

All fields must be filled out on the Acquirer Submission and Compliance Status Form. These fields include the Sensitive Authentication Data field. Please note that MasterCard will be strictly enforcing completion of this field in 2009.

The Sensitive Authentication Data field directly addresses the issue of prohibited cardholder data storage. To the best of your knowledge, please indicate in this field whether the merchant is, or is not storing sensitive authentication data post authorization. Acceptable forms of evidence to answer "No" in this field would be a compliant Onsite Assessment or Report on Compliance for Level 1 and Level 2 merchants and a compliant Self Assessment for Level 3 merchants.

This field allows MasterCard and our customers to determine if merchants are storing data that is prohibited in a post authorization environment. An answer of "Yes" in this field implies that a merchant is engaging in risky behavior and therefore is also in violation of MasterCard rules, so be sure you are working with your merchants to prevent this violation from occurring.

## Reporting of ADCs

Please ensure that any merchants that are the subject of an account data compromise are properly reported via the quarterly submission process. It is important that we are able to appropriately track these merchants through to PCI compliance after a compromise.

In terms of identifying them on the SDP submission form, these merchants should have "ADC" designated as the Merchant Status. This status can be designated via the dropdown box.

## Update on the Posting of Service Providers

As of January 1, 2009, MasterCard will no longer list those Service Providers who have only submitted an SAQ. The posting will contain only those entities who have successfully completed an annual onsite review using a PCI Security Standards Council approved Qualified Security Assessor.

## Service Provider PCI Action Plan

Beginning second quarter 2009, service providers must use an updated version of the PCI Action Plan (V2.0), which will include the six new reporting fields noted above. Previously, the PCI Action Plan allowed only for the tracking of progress toward PCI compliance based on the historical 1–12 requirements of the PCI DSS. To access the PCI Action Plan, please send an e-mail message requesting the latest version to: [sdp@mastercard.com](mailto:sdp@mastercard.com)



## **MasterCard PCI Merchant Education Program - PCI 360**

### **New Webinars Available July 2009**

Webinars are complimentary and we encourage you to share the link with your merchants –

[www.webcasts.com/mastercardpci](http://www.webcasts.com/mastercardpci)

#### **The Cost of An Account Data Compromise**

This webinar focuses on account data compromise (ADC) and examines some of the key trends as well as the costs associated with a data breach. Account data compromise is a concern for all parties involved in the payments system: from financial institutions to retailers to the consumers who may have been subject to a breach. This presentation provides an overview of some of the issues surrounding data breaches, and sheds light on the obvious and hidden costs a breached institution often faces, both monetary and reputation-related. Finally, the presentation will also review specific measures that can help prevent account data compromise – from maintaining PCI compliance to advancing awareness and education.

#### **Merchant Mayhem - Wireless Encryption and Wireless Threat Identification**

This webinar discusses the March 31, 2009 WEP removal requirement and the future of wireless encryption after June 30, 2010 as it relates to Merchant PCI compliance. Also discussed are some common wireless threats and what merchants can do to help identify and reduce their attack surface to wireless threats.

#### **2009 Update to the Security and the Payments System**

The module covers Payment Applications and PIN Entry Devices – the transition of PA DSS to the council, the requirements surrounding both Payment Applications and PIN Entry Devices and how to choose an application or device that suits your business.

# PCI 360 [www.webcasts.com/mastercardpci](http://www.webcasts.com/mastercardpci)

- 2009 Overview of the PCI Security Standards Council
- A Detailed Look at PCI DSS Requirements Version 1.1
- A Merchant's Journey Toward Compliance
- Understanding Account Data Compromise
- Preparing for a Successful PCI Assessment, Lessons from the Field
- Reducing Your Risk: A Look into PCI Vulnerability Scanning
- A look at the new Self Assessment Questionnaire
- Network Segmentation
- Maximize Internal Preparations for PCI DSS
- Data Encryption: Understanding Encryption and PCI DSS
- PCI Requirements Update Version 1.2
- Data Storage
- PCI Perspectives: Service Provider
- PCI Perspectives: PA DSS Vendor

## PCI Security Standards Council

### PCI DSS Prioritized Approach

As discussed in our Q1 2009 Newsletter, the PCI DSS Prioritized Approach is Intended as a "roadmap" to compliance based on risk associated with storing, processing, and/or transmitting cardholder data and as an educational resource that offers guidance to organizations seeking to become PCI DSS compliant. The Prioritized Approach, released by the PCI SSC March 3, 2009, provides a framework for PCI DSS compliance efforts using six security milestones to help identify the highest risk targets. This framework also can help organizations demonstrate progress on their compliance efforts.

The approach was developed in an effort to give organizations a way to reduce risk as well as lower costs associated with account data compromise events by:

- Ensuring magnetic stripe data and other sensitive authentication data is not retained
- Minimizing and securing primary account number (PAN) storage
- Focusing initial efforts on specific requirements within the PCI DSS

### Benefits of the Prioritized Approach

- A roadmap for organizations to prioritize risk
- A practical approach allowing "quick wins"
- Objective and measurable progress indicators
- Organizational planning effort support (financial and operational)
- A clear process to drive consistency among Qualified Security Assessors (QSAs)

**Note:** To achieve PCI DSS compliance, merchants and service providers must successfully implement all PCI DSS requirements, regardless of the order in which they are satisfied or whether the organization seeking compliance follows the PCI DSS Prioritized Approach



### A comprehensive PCI Standards Training program offered by the PCI SSC

The Payment Card Industry Security Standards Council (PCI SSC) is pleased to announce the following locations for 2009 PCI SSC Standards Training Program.

Session	Date	Time	Location
1	1, 2, 3 July	08:30-17:30 Day 1&2 08:30-12:30 Day 3	Hilton Heathrow London Airport Hotel
2	22, 23, 24 July	08:30-17:30 Day 1&2 08:30-12:30 Day 3	Intercontinental Toronto Yorkville

The two-day intensive course entitled Standards Training, is designed to help merchants improve preparation for onsite assessment, understand what is involved in creating their own internal assessment capability and establish an internal compliance program to help them sustain PCI DSS security practices and compliance when the assessment process is completed.

The Standards Training is targeted at security and IT personnel that are responsible for their company's PCI DSS activities. The course was created by PCI SSC based on training offered to Council certified QSAs. This gives attendees the chance to learn directly from the authority responsible for managing the standard and the QSA certification process on what to expect during a PCI DSS assessment along with real world case studies.

Standards Training is the only official PCI SSC sponsored standards training available in the market.

For more information and to register please go to: <https://www.pcisecuritystandards.org/education/training.shtml>

## Frequently Asked Questions

### **Q. Does the Prioritized Approach replace the PCI DSS 1.2?**

A. No. All Businesses that touch payment card data are required to achieve and maintain compliance with the PCI DSS 1.2. This tool does not replace the standard.

### **Q. Why is MasterCard requesting acquirers to report on merchants compliance using the Prioritized Approach?**

A. The prioritized approach helps acquirers and MasterCard determine the level of PCI DSS compliance activity completed by the merchant and helps measure the level of risk associated with noncompliance.

### **Q. As an Acquirer, how will I communicate progress against the Prioritized Approach to MasterCard?**

A. Acquirers can use the information provided in the Prioritized Approach tool in which merchants and service providers measure and track their progress to populate the revised Acquirer Submission and Compliance Status Form (V3.1).

### **Q. Is this a fast track to PCI Compliance?**

A. No. The Prioritized Approach will help organizations understand where they can act first on their compliance journey to have the most immediate impact on card data security. All requirements of the PCI DSS 1.2 must be met and maintained in order to achieve compliance.

### **Q. Who do the six new Prioritized Approach reporting fields in the MasterCard Acquirer Submission and Compliance Status Form pertain to?**

A. These six new fields only apply to those merchants using SAQ Type D and those receiving onsite assessments.

### **Q. Where can I find the latest version of the Service Provider PCI Action Plan for Service Providers?**

A. Please email [sdp@mastercard.com](mailto:sdp@mastercard.com) and request the latest version.

### **Q. Where can I find the Attestation of Compliance form?**

A. Please visit [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org) to find the new AOC.

Contact MasterCard at [pci\\_education@mastercard.com](mailto:pci_education@mastercard.com) for more information.