



MasterCard Reverses Position on Increasing Merchants' PCI Requirements

January 26, 2010 — MasterCard announced a reversal of its previous decision to increase PCI validation requirements for merchants. In response to a letter from the Institute of Internal Auditors (IIA), MasterCard announced that, as of December 15, 2009, there are additional changes to its Site Data Protection (SDP) Program, the program governing compliance with the Payment Card Industry Data Security Standard (PCI DSS) for merchants and service providers. These changes will decrease the PCI compliance validation requirements for Level 1 and 2 merchants. Validation requirements for Level 3 and 4 merchants remain unchanged as do the validation requirements associated with conducting the required external quarterly vulnerability scans.

Additional information on MasterCard's SDP program is available on its Website <http://www.mastercard.com/us/sdp/index.html>.

BACKGROUND

On June 15, 2009, MasterCard announced changes to its SDP program related to validation requirements for Level 1 and Level 2 merchants. These changes required Level 1 and 2 merchants to complete a full on-site audit, resulting in a Report of Compliance (ROC), performed by a Qualified Security Assessor (QSA). Previously, Level 2 merchants were allowed to file a Self-Assessment Questionnaire (SAQ), and Level 1 Merchants were allowed to use their internal audit departments to complete the on-site assessments.

In response to a letter from the IIA on September 10, 2009, MasterCard decided to once again change its validation requirements for Level 1 and Level 2 merchants. The IIA contends that certified internal auditors, i.e., those with certifications such as CISA, CISM, etc., are sufficiently qualified to conduct the required PCI compliance audits and satisfy the validation requirements.

Regardless of merchant or service provider level, all entities that process, store or transmit cardholder data must comply with the PCI DSS standards. As always, the merchant and service provider levels will continue to determine the requirements for validating compliance, (i.e., ROC vs. self-assessment and quarterly scans).

KEY POINTS

Merchant level definitions and validation requirements

The newly defined validation requirements affect Level 1 and 2 merchants only; Level 3 and 4 merchant requirements remain unchanged, as do the validation requirements associated with the required quarterly external vulnerability scans.

In accordance with the new requirements released by MasterCard, Level 1 and Level 2 merchants will now be allowed to use their internal audit departments to conduct the required assessments for PCI compliance validation. Additionally, Level 2 merchants will not be required to conduct a full on-site assessment resulting in a ROC but can file an SAQ instead. A Level 1 merchant is still required to complete and file a full ROC. However, Level 1 and Level 2 merchants that want to use their internal audit departments for ROC or SAQ must have their auditors attend, pass and maintain PCI Assessor certification and must file an updated ROC or SAQ by June 30, 2011. Level 2 merchants continue to have the option to complete an on-site assessment performed by a certified QSA.

The updated MasterCard validation requirements for merchants are shown below.

MasterCard Merchant Validation Requirements				
Level	Definitions	Requirements as of June 15, 2009	Requirements as of December 15, 2009	Deadline
1	<p>Any merchant that has suffered a hack or an attack that resulted in an account data compromise</p> <p>Any merchant having greater than six million total combined MasterCard and Maestro transactions annually</p> <p>Any merchant meeting the Level 1 criteria of Visa</p> <p>Any merchant that MasterCard, in its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the system</p>	<p>Annual onsite assessment by a QSA</p> <p>Quarterly network scans by an ASV³</p>	<p>Annual onsite assessment by a QSA or internal audit resources¹</p> <p>Quarterly network scans by an ASV³</p>	30 June 2011 ⁵
2	<p>Any merchant with greater than one million but less than or equal to six million total combined MasterCard and Maestro transactions annually</p> <p>Any merchant meeting the Level 2 criteria of Visa</p>	<p>Annual on-site assessment by a QSA</p> <p>Quarterly network scans by an ASV³</p>	<p>Annual on-site at merchant discretion²</p> <p>Annual Self Assessment²</p> <p>Quarterly network scans by an ASV³</p>	30 June 2011
3	<p>Any merchant with greater than 20,000 combined MasterCard and Maestro e-commerce transactions annually but less than or equal to one million total combined MasterCard and Maestro e-commerce transactions annually</p> <p>Any merchant meeting the Level 3 criteria of Visa</p>	<p>Annual SAQ</p> <p>Quarterly network scans by an ASV³</p>	<p>Annual SAQ</p> <p>Quarterly network scans by an ASV³</p>	30 June 2005

4 ⁴	All other merchants	Compliance validation is at the discretion of the acquirer To validate: Annual SAQ and quarterly network scans by an ASV	Compliance validation is at discretion of acquirer To validate: Annual SAQ and quarterly network scans by an ASV	Consult Acquirer
----------------	---------------------	---	---	------------------

Levels, Definitions and Deadlines from the MasterCard Web site.

Notes:

1 – Effective 30 June 2011, Level 1 merchants that choose to conduct an annual on-site assessment using an internal auditor must ensure that primary internal audit staff engaged in validating PCI DSS compliance attend PCI-SSC offered merchant training programs and pass any PCI SSC associated accreditation program annually in order to continue to use internal auditors.

2 – Effective 30 June 2011, Level 2 merchants that choose to complete an annual self-assessment questionnaire must ensure that staff engaged in the self-assessment attend PCI SSC offered merchant training programs and pass any associated PCI SSC accreditation program annually in order to continue the option of self-assessment for compliance. Alternatively, Level 2 merchants may, at their own discretion, complete an annual on-site assessment conducted by a PCI SSC approved QSA rather than complete an annual self-assessment questionnaire.

3 – Quarterly network scans must be conducted by a PCI SSC Approved Scanning Vendor (ASV).

4 – Level 4 Merchants are required to comply with the PCI DSS. Level 4 merchants should consult their acquirer to determine if compliance validation is also required.

5 – Initial compliance validation date for Level 1 merchants has passed. 30 June 2011 deadline affects merchants that choose to conduct an annual on-site assessment using an internal auditor.

IMPACT TO ORGANIZATIONS

While these new changes from MasterCard ease the compliance requirements at one end, they impose new requirements on those organizations who want to continue to use their internal audit resources. These organizations will now have to provide and maintain annual training and certification for those internal auditors who will be conducting the assessments. This means an increase in training budgets to cover this additional expense.

For Level 1 merchants that have always used internal audit resources to validate compliance, this alternative might be less costly than contracting with a QSA.

Level 2 merchants, however, face a more complicated decision. They will have to determine whether the cost of maintaining this training and certification is more or less expensive than contracting with a QSA, especially when other factors such as staffing and opportunity costs are taken into account. Those Level 2 merchants who currently do not have internal audit resources would be faced with the cost of hiring to meet these requirements.

These new requirements affect MasterCard only. Other card brands may specify stricter validation requirements that force merchants to contract with a QSA firm. American Express does not allow the use of internal audit resources, and VISA reserves the right to decide if a Level 1 merchant can or cannot use internal audit resources. In these cases, maintaining trained and certified internal audit resources may provide a minimal return on investment. Level 1 merchants that don't currently use internal audit resources should check with their acquirers to determine if this option is acceptable to other card brands before deciding.

HOW JEFFERSON WELLS CAN HELP

More than 20 Jefferson Wells Information Security professionals are Qualified Security Assessors, and we've performed PCI assessments and provided related PCI services since 2003. Our commitment to value and service excellence enables clients to complete their PCI validation requirements quickly and efficiently.

As a QSA and ASV, Jefferson Wells maintains a direct relationship with the PCI Security Council and the card brand companies. These relationships help us quickly escalate PCI DSS-related issues or questions for speedy resolution.

PCI-related services fall within the Jefferson Wells Information Security Center of Expertise (COE). The Information Security COE is comprised of professionals with deep technical and security expertise who have significant "hands-on" experience in information security, network technology and vulnerability assessments. Additional services include penetration testing, wireless assessments and more.

For additional information, contact your Jefferson Wells Business Development Manager

Jefferson Wells delivers professional services in the areas of risk advisory, tax, and finance and accounting. We serve clients, including Fortune 500 and Global 1000 companies, from offices worldwide.

Jefferson Wells is not a certified public accounting firm.
© 2010 Jefferson Wells International, Inc. All rights reserved.