

## Q4 2009 PCI Merchant Newsletter

### Welcome!

Welcome to the first edition of WorldPay's US PCI Quarterly Newsletter. We hope you find the PCI-related articles, updates and industry news useful to your business.

This edition includes:

- Introducing the new and improved WorldPay PCI Web site
- The Prioritized Approach Worksheet - Tracking and Documenting your journey to PCI Compliance
- Merchant Reporting Requirements
- End-to-End Encryption
- Payment Application Data Security Standards
- Payment Applications that store Sensitive Data
- Fraud Warnings for the Hotel, Restaurant and Public House industry
- Skimming Prevention - Best Practices for Merchants
- Account Data Compromise Trends
- Lifecycle Process for Changes to PCI DSS

### The WorldPay PCI Web site

Early December 2009, WorldPay's PCI department launched significant updates to its existing Web site to include current industry information, compliance mandates and changes, valuable resource links and reporting tools for our merchants. Please view our site at [http://worldpay.us/247/supp\\_pci.htm](http://worldpay.us/247/supp_pci.htm)



### Prioritized Approach Worksheet: A Better Way to Track Progress

**MasterCard® has implemented the use of the Prioritized Approach Worksheet for all non-compliant merchants effective immediately. This document, created by the PCI Security Standards Council, gives the acquirer a clearer picture of the merchant's efforts to reach compliance. All non-compliant merchants must complete this document before the end of the fourth quarter 2009.**

WorldPay must report merchant progress updates against the six milestones to the Card Associations. This document enables merchants to demonstrate their progress towards compliance to key stakeholders and allows us to build a case on behalf our merchants in an attempt to avoid any potential financial penalties.

The document also provides guidance that will help merchants identify how to reduce risk to cardholder data as early as possible in their compliance journey. The tool groups together the requirements of PCI DSS 1.2 into six key milestones for merchants to consider in their card data security strategy.

#### 1. Remove sensitive authentication data and limit data retention.

Identifying and purging unnecessary cardholder data can significantly reduce the risk and impact of a data breach as well as potential fines. If you don't need it, don't store it.

#### 2. Protect the perimeter, internal and wireless networks.

Isolate the cardholder network to the components and users that are needed to conduct credit card transactions.

### 3. Secure payment card applications.

This milestone targets controls for applications, application processes, and application servers. Weaknesses in these areas offer easy prey for compromising systems and obtaining access to cardholder data.

### 4. Monitor and control access to your systems.

Controls for this milestone allow you to detect the who, what, when and how concerning who is accessing your network and cardholder data environment.

### 5. Protect stored cardholder data.

For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, milestone five targets key protection mechanisms for that stored data.

### 6. Finalize remaining compliance efforts, and ensure all controls are in place.

The intent of milestone six is to complete PCI DSS requirements and finalize all remaining related policies, procedures and processes needed to protect the cardholder data environment.

The Prioritized Approach tool and instructions can be found through the following link on the PCI Security Standard Council's Web page at <https://www.pcisecuritystandards.org/education/prioritized.shtml>



## Merchant Compliance Reporting Requirements

### Level 1 Merchants

#### Defined

Any merchant that has suffered a hack or an attack that resulted in an account data compromise

Any merchant having greater than six million total combined MasterCard and Maestro or Visa transactions annually

Any merchant that MasterCard or Visa®, in its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the system.

#### Validation Requirement

All Level 1 merchants must complete an annual on-site assessment. All Level 1 merchants that have engaged an internal auditor before June 15, 2009, must validate compliance with the PCI DSS via an annual on-site assessment conducted by a PCI SSC-Certified QSA by December 31, 2010.

To fulfill the network scanning requirement, all merchants must conduct scans on a quarterly basis using a PCI SSC-Approved Scanning Vendor.

### Level 2 Merchants

#### Defined

Any merchant with greater than one million but less than or equal to six million total combined MasterCard and Maestro or Visa transactions annually

#### Validation Requirement

**A Self Assessment Questionnaire is required annually until December 31, 2010.**

All Level 2 merchants must complete an annual on-site assessment conducted by a PCI SSC-Certified Qualified Security Assessor (QSA) and must validate compliance by December 31, 2010. We strongly encourage all Level 2 merchants to engage a QSA as soon as possible.

To fulfill the network scanning requirement, all merchants must conduct scans on a quarterly basis using a PCI SSC-Approved Scanning Vendor.

### Level 3 Merchants - Defined

Any merchant with greater than 20,000 combined MasterCard and Maestro or Visa transactions annually but less than or equal to one million total combined MasterCard and Maestro or Visa ecommerce transactions annually.

#### Validation Requirement

Self-Assessment Questionnaire is required annually

To fulfill the network scanning requirement, all merchants must conduct scans on a quarterly basis using a PCI SSC-Approved Scanning Vendor.

As of August 2009 the Card Associations have begun aggressively assessing fines against non-compliant level 3 merchants that have not initiated PCI compliance validation efforts.

### **Level 4 Merchants - Defined**

Level 4 Merchants are required to comply with the PCI Data Security Standard; however, validation is not required at this time.

### **Important Reminder**

All PCI Merchant Compliance Validation Documents should be sent to the PCI Compliance Validation Mailbox at [PCIVD@WorldPay.us](mailto:PCIVD@WorldPay.us) to ensure this information is captured and reported to the Card Associations. Please attempt to get your reporting documents to us from your merchants by the 20th of each month, so we have time to process the information appropriately.

### **End-to-End Encryption**

The subject of End-to-End Encryption (E2EE) is now becoming a hot topic of discussion. Also known as "Data Field Encryption," the idea is to protect card information from the swipe to the acquirer processor with no need for the merchant to process or transmit card data in the "clear." Importantly, data field encryption renders cardholder data useless to criminals in the event of a merchant data breach.

In an effort to enhance overall data security in the payment industry and to further the development of data field encryption, Visa has developed best practices to assist merchants in evaluating the new encryption solutions emerging in the marketplace.

For more detail please visit the following pages:  
<http://corporate.visa.com/media/best-practices.pdf>

For more detail regarding the lifecycle and in particular the five stages, please visit the following pages of the PCI SSC Web site:

[https://www.pcisecuritystandards.org/pdfs/OS\\_PCI\\_Lifecycle.pdf](https://www.pcisecuritystandards.org/pdfs/OS_PCI_Lifecycle.pdf)

### **PA-DSS**

As an acquirer, WorldPay must follow requirements laid down by both the PCI Security Standards Council (PCI SSC) and the individual card brands. Formerly, ©Visa Inc. managed payment application compliancy through a program they established known as Payment Application

Best Practices (PABP). This program was managed solely by Visa and was the first generation attempt to build strong application security practices by the payment application software vendors. With the establishment of the PCI SSC in 2006, a slow migration has occurred to transform PABP into what is now known as the Payment Application Data Security Standard (PA DSS). The PA DSS is a standard now managed by the PCI SSC and is a series of rules that need to be complied with if a vendor is to sell off-the-shelf payment applications to third parties (namely merchants). The traditional Payment Card Industry Data Security Standard (PCI DSS) targets entities that store, process, or transmit cardholder data. While not all software vendors store, process or transmit cardholder data, the applications they create perform any one or all of these functions for the entity and hence the creation of the PA DSS. A secure payment application in conjunction with a compliant PCI DSS environment will help minimize potential security risks and exposure of cardholder data.



Payment application vendors need to comply with the PA DSS, which provides a specific set of standards for the development of payment applications. The PCI SSC has produced the following document to assist Payment Application Qualified Security Assessors (PA QSA) in the testing of the payment application code against the PA DSS.

[https://www.pcisecuritystandards.org/pdfs/pci\\_pa\\_dss.pdf](https://www.pcisecuritystandards.org/pdfs/pci_pa_dss.pdf)

Once the PA QSA has completed testing and validation, the testing validation will be submitted to the PCI SSC for acceptance and posting on the PCI SSC-compliant application listing. You can find this listing by clicking on the following link:

[http://www.pcisecuritystandards.org/security\\_standards/vpa/](http://www.pcisecuritystandards.org/security_standards/vpa/)

According to Visa's payment application mandates, effective July 1, 2008, acquirers and processors are only allowed to certify new applications to their platforms that meet this standard.

### **To Whom Does the PA DSS Apply?**

The following guide can be used to determine whether PA DSS applies to a given payment application:

1. PA DSS does apply to payment applications that are typically sold and installed "off the shelf" without much customization by software vendors.
2. PA DSS does apply to payment applications provided in modules, which typically includes a "baseline" module and other modules specific to customer types or functions, or customized per customer request. PA DSS may only apply to the baseline module if that module is the only one performing payment functions (once confirmed by a PA QSA). If other modules also perform payment functions, PA DSS applies to those modules as well. Note that it is considered a "best practice" for software vendors to isolate payment functions into a single or small number of baseline modules, reserving other modules for non-payment functions. This best practice (though not a requirement) can limit the number of modules subject to PA DSS.
3. PA DSS does NOT apply to a payment application developed for and sold to only one customer given that this application will be covered as part of the customer's normal PCI DSS-compliance review. Note that such an application (which may be referred to as a "bespoke" application) is sold to only one customer (usually a large merchant or service provider), and it is designed and developed according to customer-provided specifications.

4. PADSS does NOT apply to payment applications developed by merchants and service providers if used only in-house (not sold to a third party), because this in-house developed payment application would be covered as part of the merchant's or service provider's normal PCI DSS compliance.

For further information on PA DSS v1.2 for supporting documents, please visit:

[https://www.pcisecuritystandards.org/security\\_standards/pa\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml)



### **CLASSIFICATIONS**

WorldPay has developed three classifications for all payment applications within its merchant population. These three classifications are PA DSS Compliant, Known Vulnerable and Unknown. Let's discuss each one in a little further detail.

**PA DSS Compliant** – This is an application that has been validated by a PA QSA and has been listed on the PCI SSC's approved payment application listing. This is the preferred application type.

**Known Vulnerable** – These are applications that have been identified by VISA as either storing prohibited cardholder data and/or having been previously compromised. Effective January 1, 2008, Visa mandated that all acquirers and processors discontinue the boarding of merchants using Known Vulnerable applications. This list is maintained by Visa; however, it is not available to the general public due to security reasons.

**Unknown** – These are applications that have NOT received a PA DSS validation certification; however, they have NOT been identified as Known Vulnerable.



## VISA MANDATES

In 2008, Visa laid out a series of mandates, forcing merchants to migrate towards compliant applications. Below are the specific mandates from Visa. Each one and its meaning will be discussed in detail.

Phase	Compliance Mandate	Effective Date
1	Newly boarded merchants must not use known vulnerable payment applications, and VisaNet Processors (VNPs) and agents must not certify new payment applications to their platforms that are known vulnerable payment applications.	1/1/08
2	VNPs and agents must only certify new payment applications to their platforms that are PA-DSS compliant.	7/1/08
3	Newly boarded Level 3 and Level 4 merchants must be PCI DSS compliant or use PA DSS-compliant applications*	10/1/08/
4	VNPs and agents must decertify all vulnerable payment applications.**	10/1/09
5	Acquirers must ensure their merchants, VNPs and agents use only PA-DSS compliant applications.	7/1/10

**Phase 1** – This mandate was the first attempt to begin eliminating Known Vulnerable applications from the merchant base and eliminate the certification of Known Vulnerable applications by acquirers and processors. Effective January 1, 2008, WorldPay stopped boarding merchants utilizing a Known Vulnerable application. WorldPay’s Terminal Products team discontinued certifications of applications that appeared on the Known Vulnerable list.

**Phase 2** – In the second phase, not only did WorldPay NOT certify Known Vulnerable applications, but also now only certify payment applications to our platform that received a PA DSS-validation certificate.

**Phase 3** – With this mandate, merchants began to see the effects of PA DSS compliance and how the Visa mandates affect their processing. Essentially, any new merchant utilizing a payment application that boarded with WorldPay could only board under one of the following conditions:

A) The merchant was using a PA DSS-certified application or

B) That merchant was PCI DSS compliant.

**Phase 4** – The Phase 4 mandate stated that all acquirers and processors must examine their existing merchant base and remove all merchants using a Known Vulnerable application. Combining Phase 1, which captured new merchants, with Phase 4, which captured existing merchants boarded prior to January 1, 2008, all merchants would be evaluated for elimination of Known Vulnerable applications in the payment system.

**Phase 5** – This is the final deadline for all Phases 1 - 4 compliancy. For all merchants utilizing payment applications in the payment system would either be PA DSS compliant or PCI DSS compliant as of July 1, 2010.

*\* In-house use only developed applications and stand-alone POS hardware terminals are not applicable.*

*\*\* VisaNet Processors (VNP's) and agents must decertify vulnerable payment applications within 12 months of identification.*

### Payment Application and Level 3/ Level 4 Program

Specifically targeted at meeting Visa’s Payment Application Mandate 5, WorldPay will roll out its Payment Application and Level 3/Level 4 Program beginning January 2010. In addition to meeting the Visa payment application mandates, this program is designed to assess Level 3 and Level 4 merchants based upon their risk. For starters, it is important to recognize our security partner who will assist us in meeting this challenge.

Arsenal Security Group is a Virginia-headquartered Qualified Security Assessor (QSA) with offices located throughout the United States and London. WorldPay (both US and UK entities) have entered into agreements with Arsenal Security Group to provide global security programs to the

WorldPay merchant base. These security programs vary from payment application validation, to merchant PCI compliance, to data encryption and other security consulting efforts. It is a global PCI consulting provider and has expertise in dealing with large global Fortune 500 companies, along with smaller franchise locations and brick and mortar merchant businesses. It is a PCI-approved QSA and has over 25 years of PCI and IT consulting services.

In addition to the Visa mandates, announced in 2007, Visa also instituted a program called the Compliance Acceleration Program (CAP). As part of the CAP, acquirers were to create a plan to address PCI in the Level 3 and Level 4 populations. Visa recommended a risk-based approach for enforcement to this large population. Currently, WorldPay US monitors 100% of its Level 3 (e-Commerce) customers by mandating compliance validation quarterly. Therefore, the Arsenal risk-ranking program concentrates on the Level 4 population.

To put this in perspective, the WorldPay US Level 4 merchant base is a significant portion of our considerable portfolio. It is evident then that management of compliance to the standards for this population would be difficult to obtain without implementing a risk-based approach.



The roll out of the Level 3/Level 4 Payment Application Program will be delivered to customers boarded from 10-1-08 to 12-31-09. Effective January 1, 2010, this program will become part of the boarding process for all merchants on an on-

going basis; any merchant in the boarding process will be susceptible to the program outlined below.

The program will involve WorldPay identifying merchants who are deemed higher risk based on their initial boarding criteria. These merchants will be provided access to a complimentary PCI scan tool. This tool will scan a merchant's internal systems against three PCI factors:

- 1) Is the merchant storing cardholder data on the resident systems?
- 2) Do system passwords meet PCI requirement 8.5 criteria?
- 3) What is the exact payment application and version number utilized by the payment terminal?

This information will be gathered and reviewed by WorldPay PCI management. Based on the results of the scan, next steps will be determined and discussed with the merchant. Examples of next steps could be deletion of cardholder data found, upgrading of a payment application, modifications to system password rules, no further action needed at all, or a combination of any of the above elements.

### ***WorldPay Merchants Boarded 10-1-08 through 12-31-09***

In October 2009, WorldPay began a test run of the new program with a population of approximately 500 merchants. The steps to this process are as follows:

1. First notification letters were sent to the test population. These letters notified them of the WorldPay program, along with referencing the specific Visa mandates and the need for compliance. The letter instructed the merchants to perform the following actions:
  - a. Go to [www.worldpayus-vsreg.arsenalsecuritygroup.com](http://www.worldpayus-vsreg.arsenalsecuritygroup.com) and register for Arsenal Security Group's SST (SmartSearch Technology). This is a free risk analysis tool provided to the merchants by WorldPay.
  - b. Upon completion of the SST download, both WorldPay and the merchant will receive notification of the results of the scan. The SST scan searches three elements:

- i. Does the merchant have any unprotected cardholder data on his or her systems?
  - ii. What is the merchant's payment application?
  - iii. Does the merchant passwords meet PCI standards?
- a. The results of the scan are reviewed by an WorldPay PCI Manager, and a decision is made concerning future action:
- i. If the scan comes back as passing, there is no further action.
  - ii. If the scan comes back as failing, the merchant must then enter Arsenal Security Group's CMP (Compliance Management Portal).
- b. Failure to perform the download of SST or enrollment in the CMP will result in a \$25.00 per month penalty fee until action is performed.
- i. The merchant has 60 days to download the SST.
  - ii. The merchant has 90 days to complete the CMP,
- c. The \$25.00 fee may be reimbursed should the merchant notify WorldPay of its intent to perform the appropriate action.
- d. This test program will be reviewed at the end of 2009 for improvements to the process.

### ***Newly Boarded WorldPay Merchants as of January 2010***

1. Effective January 2010, every two weeks there will be a mailing sent to all merchants boarded within that time frame who were identified as Unknown
2. The process for existing merchants outlined in step 1a will then commence
3. This process will become routine for all newly boarded merchants on the WorldPay platform.

### ***Visa Alerts Acquirers to Payment Applications that store Sensitive Data***

Both Visa mandates and the Payment Card Industry Data Security Standard (PCI DSS) prohibit the storage of the full contents of any magnetic stripe, Card Verification Value 2 (CVV2) or PIN data. This is also more commonly known as **Sensitive Authentication Data**.

Merchants and agents are at high risk of being compromised if they use Payment Applications that store sensitive cardholder data or have inherent security weaknesses. It is critical that merchants and agents do not use Payment Applications known to retain sensitive cardholder data elements and that acquirer's take corrective action to address any identified deficiencies.

Merchants and agents should only use Payment Applications that have been validated against Visa's Payment Application Best Practices (PABP), now known as the Payment Application Data Security Standard (PA DSS). A list of PA-DSS validated applications is available at the following site: [www.pcisecuritystandards.org/security\\_standards/vpa/](http://www.pcisecuritystandards.org/security_standards/vpa/)

Payment applications often store sensitive cardholder data post-authorization without the merchant's or the agent's knowledge. Merchants and agents should ask their Payment Application vendors (or resellers and integrators) to confirm that their software does not store magnetic-stripe data, CVV2, PINs or encrypted PIN blocks.

Please refer to the "Key dates for your diary" section below to see some key PA-DSS deadlines that you should be aware of.



### ***Fraud Warning: Hotel, Restaurant and Public House***

WorldPay is aware that merchants in the Hotel, Restaurant and Public House sector are under an increased level of focus from fraudsters in respect to their billing and/or booking hardware and software. There have been several reported incidents that can be found online.

Please ensure **ALL** physical and logical security procedures are being observed, especially those

that are set out in the PCI DSS standards (please follow the link below) and ensure you have the latest updates installed from your vendor's software.

If in doubt, please speak to your vendor to ensure you have taken all steps that they recommend for your systems.

If you have any suspicions, make contact with your WorldPay Relationship Manager or the PCI team.

### ***Skimming Prevention - Best Practices for Merchants***

The Security Standards Council has just released a useful information supplement covering Skimming Prevention that we would recommend for your review.

The document was created to assist and educate merchants on implanting and sustaining security best practices associated with skimming attacks. Though currently not mandated by PCI SSC, guidelines and best practices documents are produced to help educate and create awareness of challenges faced by the payment industry.

Even if your business is not impacted by this, it may still provide useful information around what the payment industry is up against. This document contains a non-exhaustive list of security guidelines that is there to help merchants to:

- Be aware of the risks relating to skimming.
- Be aware of the vulnerabilities inherent in the use of point-of-sale terminals and terminal infrastructure.
- Be aware of the vulnerabilities associated with staff that has access to consumer payment devices.
- Prevent or deter criminal attacks against point-of-sale terminals and terminal infrastructure.

### ***Lifecycle Process for Changes to PCI DSS***

Any changes to the Data Security Standard follow a defined 24-month lifecycle with five stages. The lifecycle ensures a gradual, phased use of new versions of the standard without invalidating current implementations of PCI DSS or putting any

organization out of compliance the moment changes are published. With the release of PCI DSS version 1.2 on October 1, 2008, the Council was committed to following this process to ensure transparency and continuity of compliance. The Council will publish similar lifecycles for the Payment Application Data Security Standard (PADSS) and the PIN Transaction Security (PTS) Requirement - formerly known as PCI PED.

The current stage is two, where feedback gathering has begun in earnest. As WorldPay sits on the Board of Advisors, we are actively involved at this stage. During the month of November, they entered stage three, which is the lengthy feedback, review and decision phase.

- Identify any compromised terminals as soon as possible, and notify the appropriate agencies to respond and minimize the impact of a successful attack

To see the full document, please click in the following link:

[https://www.pcisecuritystandards.org/education/info\\_sup.shtml](https://www.pcisecuritystandards.org/education/info_sup.shtml)



### ***Account Data Compromises***

As a result of the Card Associations' efforts to eliminate the storage of prohibited data, fewer compromised organizations are found to store card data. While storage of cardholder data continues to be an issue, theft of data that are in transit is on the rise. Hackers are now shifting to new attack vectors to illegally obtain cardholder data. There has been an increase in the use of unauthorized applications (referred to as malware) in recent years. Malware such as RAM-parsing, packet analyzer, and/or key-logger are some of examples of unauthorized applications currently in use. RAM-parsing is malware used to gather information passed from

the payment application to its host computer through RAM. Packet analyzing or sniffing program is a program that intercepts traffic entering or leaving a particular system and records that traffic. Key-logger records the information entered on the keyboard or card reader device as it travels from the magnetic-stripe reader to the computer or payment application. As a result, merchants and service providers not only need to utilize PA DSS-compliant software but also ensure that their network environment is secure and complies with the PCI DSS.

The following statistics illustrates the comparison of compromises according to payment channel:

- 68% Brick and Mortar
- 31% e-Commerce
- 1% MO/TO

76% of compromises involved either the food service establishment (49%) or a retail location (27%).

- Food service experiences the majority of compromises due to their reliance on third-party software that are normally supported remotely. Hackers have been exploiting remote control software that is not securely configured. Exploitation of remote access is the number one technical cause of breaches.

Hackers use automated scanners to troll the internet for vulnerable systems. The majority of compromised systems were found to be connected to the Internet for authorization. It stands to reason that any connection to the Internet should be considered a connection to an un-trusted network and secured accordingly.

61% of all compromised merchants were supported by a third party vendor or integrators. The causes of the compromises were either due to outdated systems or to the unsecured configuration of the system. Many merchants depend heavily on third-party vendors or integrators to install, configure and support their payment applications. Negligence on the part of the third party in appropriately configuring payment applications, more often than not, has contributed to the payment card compromises.

Common PCI DSS failures discovered during a data breach investigation are:

- Requirement 3 - Protect stored cardholder data
- Requirement 6 - Develop and maintain secure applications

- Requirement 10 - Track and monitor all access to network resources and cardholder data
- Requirement 12 - Maintain an information security policy

The five technical causes for the majority of data compromises globally are:

- SQL Injection (17%)
- Remote Access (16%)
- Backdoor/Trojan (15%)
- Perimeter Security Issues (13%)
- Weak Passwords (12%)

In summary, payment card security extends beyond simply using PA DSS validated payment applications and eliminating the storage of prohibited cardholder data. Merchants and service providers must comply with the PCI DSS in its entirety in order to effectively protect cardholder data.



### ***Non-Compliant PIN-Entry Device (PED) and Known-Compromised Devices***

Current Card Association mandates require that all acquirers and acquiring processors begin retirement of PIN Pads and terminal devices that are not PED compliant (non lab evaluated), are not Triple Data Encryption Standard (TDES) encrypted or that are on Visa's known-compromised devices list.

In compliance with these mandates, WorldPay no longer supports boarding or exchanges of units that are non lab evaluated, on Visa's known-compromised list or that are Single Data Encryption Standard (SDES) encrypted.

These units must be completely removed from the field no later than July 1, 2010. Card Association fines may be levied on merchants who do not comply with this mandate.

For a complete list of non lab evaluated and known-compromised devices, as well as replacement suggestions, please visit the PIN-Entry device section on the PCI Support Center page of WorldPay.us. Go to [http://www.WorldPay.us/247/supp\\_pci.htm](http://www.WorldPay.us/247/supp_pci.htm).

*This Statement message was sent to all merchants the week of August 3<sup>rd</sup> 2010*



### **Key Dates**

#### **December 20, 2009**

Please provide your PCI compliance validation documents to the PCI Compliance Validation Mailbox at [PCIVD@WorldPay.us](mailto:PCIVD@WorldPay.us).

#### **July 2010**

Acquirers must ensure their merchants, VNP's and agents use only PA-DSS compliant payment applications.

#### **December 31, 2010**

All Level 1 and Level 2 merchants must complete an annual on-site assessment conducted by a PCI SCC-Certified Qualified Security Assessor (QSA). MasterCard strongly encourages that all impacted merchants engage a QSA as soon as possible.

### **WorldPay Monthly Webinar Series**

The WorldPay PCI Monthly Education Webinar occurs on the 3<sup>rd</sup> Wednesday of each month at 3:00 p.m. EST.

#### **Wednesday, December 16, 2009 at 3:00 p.m. EST**

#### ***"The PCI Security Standards and How They Are Formed"***

*Presented by Troy Leach, Chief Technology Officer of the PCI Security Standards Council*

Reserve your Webinar seat:

<https://www2.gotomeeting.com/register/939137290>

#### **January 20, 2010 at 3:00 p.m. EST**

#### ***"MC Site Data Protection Plan and Account Data Compromise Update"***

*Presented by MasterCard*

Reserve your Webinar seat by pasting web address [www.attgic.com/pci](http://www.attgic.com/pci)

**\*\*participants will be asked to enter their name\*\***

#### **Telephone Link**

Local: 1-480-629-9560

Toll Free: 1-877-941-1884

**\*\*participants please mention the WorldPay and MasterCard SDP Webinar to the operator\*\***

### **MasterCard's PCI 360 Merchant Education Program**

In our efforts to increase awareness and understanding of the Payment Card Industry Data Security Standard (PCI DSS), MasterCard has introduced a complimentary merchant education initiative offered to our acquiring bank customers and their merchants.

- Gain the knowledge needed to become PCI compliant.
- Learn directly from industry security experts.
- View recorded webcasts on your own time.
- Take advantage of materials to educate your team and new employees.

<http://www.mastercard.com/us/sdp/education/pci%20merchant%20education%20program.html>

### **The PCI Merchant Compliance Team**

*LeAnn Brown, Head of PCI*

*Leslie V. Potter, PCI Management  
Merchant Compliance Levels 1, 2 & 3*

*Michael Lyons, PCI Management  
Merchant Compliance Level 4 and PA-DSS*

*Wayne Ignacio, PCI Management and  
Account Data Compromise*

*Humberto Chacon, National Client Relations  
National Customers Levels 1, 2 & 3*

**Security Partner**



Mark Lippman  
Senior Partner  
[mlippman@arsenalsecuritygroup.com](mailto:mlippman@arsenalsecuritygroup.com)  
703-980-8715 (c)  
703-563-7446 (f)  
[www.arsenalsecuritygroup.com](http://www.arsenalsecuritygroup.com)

Thank you for taking the time to read and review our newsletter. We would welcome your feedback and encourage you to send your comments about the content of this edition or suggestions for the next to [PCISecurity@rbsworldpay.us](mailto:PCISecurity@rbsworldpay.us).

WorldPay  
[http://www.worldpay.us/247/supp\\_pci.htm](http://www.worldpay.us/247/supp_pci.htm)  
600 Morgan Falls | Atlanta GA 30350 | US