



May 4, 2010



## Payment Card Industry (PCI) Compliance

## Press Release

### What is PCI?

The Payment Card Industry (PCI) has implemented a stringent set of requirements called the PCI Data Security Standard (DSS) which defines specific requirements for companies seeking to store, process, or provide services related to credit card data. Compliance with the PCI DSS is validated through annual audits. Depending on the annual volume of credit card transactions an audit may be self-assessed or assessed by a Qualified Security Assessor (QSA) who performs an on-site audit. Companies who fail to obtain PCI compliance may have their payment processor terminate their services and/or face significant financial penalties for continued non-compliance.

The PCI DSS contains 6 categories of compliance requirements that apply to all merchants. Merchants are companies that process their own transactions where as service providers, such as PBD, process transactions on behalf of other companies. Service providers are required to meet all PCI DSS requirements as well as a separate specific set of requirements designed for service providers, payment gateways, and other multi-merchant service companies. The high-level categories of the PCI DSS are:

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

### What does PCI mean at PBD?

Reaching and maintaining PCI compliance means we are delivering on the superior service every time approach which is PBD's mission statement. We are proud to have external validation that we are doing the right things for our business and for our client's businesses. PBD is able to do this by having Trustwave send an auditor on-site annually to validate our status as a Level 1 service provider and Level 3 merchant. We aggressively pursue opportunities to improve internal processes and electronic systems based on the best practice guidance provided by the PCI DSS.

### This means:

PBD built a whole new network, secure in every sense from the ground up, for our key enterprise systems including Enterprise Resource Planning (ERP) solution and PCI related servers. A series of redundant firewalls, switches, and servers are maintained in a Tier 1 data center. Our infrastructure contains a number of advanced security innovations, such as:

- Data Leak Prevention – DLP blocks credit card numbers from being transmitted in web and email communications
- Intrusion Prevention Services – IPS inspects all electronic traffic for thousands of known attacks and prevents the malicious traffic from reaching our systems
- Application Layer Firewalls – Application layer firewalls, or web firewalls, add additional security that compliments the network and host based security controls

### PCI Compliance Benefits

- Validates Security & Documentation
- Repetitive Processes
- Clear Data Ownership

### Goals of Payment Card Compliance:

1. Build & Maintains a secure network
2. Protects Cardholder Data
3. Maintain a vulnerability management program
4. Implements strong access control measures
5. Regularly monitors and tests network
6. Maintains an information Security Policy

## PCI Continued...



PBD has implemented an enterprise encryption management solution in combination with Advanced Encryption Standard (AES) based data warehousing encryption to protect credit card data. The enterprise encryption Management allows PBD to extend the encryption process to clients, meaning that security can be enforced from very early in the data processing flow prior to the data even reaching PBD's systems. From the time the data arrives until secure destruction, based on our asset retention and disposal schedule, it is maintained in an encrypted state within all PBD systems and backups.

Access to sensitive data is limited using Role Based Access Control. This allows PBD to provide each entity requiring access with the minimum level of access required for functionality. Data masking techniques ensure that credit card numbers are hidden unless specifically defined business functions require un-obstructed view. Every time anyone accesses sensitive information it's recorded in our audit logs which are reviewed regularly.

PBD performs internal vulnerability assessments as part of an overall risk management strategy. In addition, 3<sup>rd</sup> party vulnerability scans are conducted on a monthly basis by the largest PCI auditing firm, Trustwave. More aggressive penetration testing against our infrastructure and applications is performed regularly by a 3<sup>rd</sup> party as well. Changes to systems or processes based on risk analysis or assessment are performed according to a defined change management process.

PBD uses a comprehensive Information Security Policy (ISP) in combination with other administrative and technical controls to keep our systems running in a compliant manner. Regular administrative log reviews, audits, configuration guidelines, as well as physical and logical security controls are defined within the ISP. The ISP is reviewed regularly and consulted for any pending process changes to keep us improving in a secure and compliant manner.

### Why choose a PCI Compliant Partner?

There are countless examples of the specific ways that we care for the physical and logical information assets of our clients and how PCI has helped us improve those processes. Choosing a partner whose knowledge, systems, and processes have been certified as being aligned with the PCI DSS adds peace of mind from dangers like identity theft and cyber-crime. PBD invests in innovative technologies, like those discussed here, to provide superior security every time. We recognize and understand the strength that PCI compliance adds to an organization. Compliance is the only responsible choice for us as a leading fulfillment solutions provider and partner. We value the trust of our clients and are always respectful in the manner that we handle data.

*"After successful compliance and living compliantly, organizations realize that 80%+ of the requirements are very good business practices and should have been implemented anyway. PCI DSS will be the catalyst for getting up to par on the best business practices. "*

*Bjarke Ormstrup*

*Vice President of Information Technology*



For more information please contact us

1.866.998.4PBD  
Sales.marketing@PBD.com  
Visit us at [www.pbd.com](http://www.pbd.com)