WHITEPAPER

The critical nature of PCI compliance in hosted billing solutions

In business, reputation, trust, and reliability are everything. Even one incident that exposes sensitive customer data can create concern and, ultimately, defection. Customers need to know that the businesses they trust with their most sensitive, private information are taking every possible step to ensure the security of that data.

For transaction-based businesses, that means full compliance with the PCI Data Security Standard (DSS)—a standard that ensures that the entire online billing process, from point-of-sale devices, PCs and servers to wireless hotspots, Web shopping applications, storage systems and data transmissions by service providers, are complying with the standard at all times. If PCI compliance isn't ironclad, you're risking your customer's satisfaction, your reputation, and the security of untold numbers of innocent consumers.

And that can affect your bottom line. According to a June, 2008 study by Javelin Strategy & Research, more than half of consumers experiencing a security breach remain less confident in the breached organization's ability to protect and manage their personal data. Thirty percent said they would never purchase goods or services again from the organization, and 20% said they would never maintain any kind of relationship with the company again.

And loss of customer satisfaction and trust is merely the beginning of potential problems by handling customer financial and credit card information in a non-PCI compliant manner. You're risking your company by exposing it to potential lawsuits and untold direct financial damage. And, if non-compliant, credit card companies can even stop conducting business with you.

Although comprehensive PCI compliance is a tall order, it's the only way to ensure the safety of customers' data. Some companies prefer to delegate PCI compliance to their vendors and service providers. By doing so, companies can avoid the need to dedicate personnel to the process, and can get back to what makes them unique—focusing on their products, services and customers.

But trusting a vendor enough to delegate transaction protection to them should be more than a leap of faith. To make the process work smoothly, seamlessly and professionally, companies must know, without a shadow of a doubt, that their trust is well-placed.

WHAT IS PCI AND HOW HARD IS IT TO COMPLY?

The Payment Card Industry Data Security Standard (PCI-DSS), under the auspices of the PCI Security Standards Council, regulates the security procedures for organizations that process, transmit or store cardholder data. It is endorsed by all major card institutions, including American Express, Visa Inc., MasterCard Worldwide, Discover Financial Services and JCB International.

There are four levels of PCI DSS validation: from Level 4 at the low end to Level 1 at the highest level. To achieve Level 1 PCI DSS validation, service providers must demonstrate full compliance with all 12 requirements listed below. Level 1 providers must undergo an annual on-site PCI security audit and quarterly network security and vulnerability scans, validated by a qualified security assessor and approved scanning vendor, respectively. Once validated, the vendor will appear on an approved list for Level 1 companies, maintained by the PCI Security Standards Council.

Levels 2, 3, and 4, for merchants lower transaction levels than Level 1 merchants, are required only to complete annual self-assessment questionnaires and perform quarterly network vulnerability scans. There is no official validation of results.

The requirements for PCI DSS validation are comprehensive, and include these 12 major requirements for validation and certification:

- Install and maintain a firewall configuration to protect cardholder data
- Don't use vendor-supplied defaults for system passwords and other security parameters
- Protect stored cardholder data
- Encrypt transmission of cardholder data sent across open, public networks
- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security

But it's not enough to simply try to comply with these 12 principles. If even one of them falls through the cracks, your customers' personal information could be compromised. And it happens more than one might think. Many companies—even those trying hard to comply with the PCI standard—just don't have the background, skill or time to meet all requirements. For example, although PCI DSS prohibits merchants from storing cards' security codes or track data, Trustwave found that most compromised merchants did just that.

Credit card data compromises also can result from problems with a merchant's network, either because they have not followed information security best practices or because they maintain connection to outside parties that don't follow proper policies and procedures. And finally, compromise also can occur when attackers exploit improperly configured remote access applications that allow a third party to connect to a merchant's network

TAKE NO CHANCES – ASK HARD QUESTIONS OF YOUR BILLING PROVIDER ABOUT THEIR CERTIFIED PCI COMPLIANCE

When it comes to customer data, nothing but the most ironclad protection will suffice. That's why it's critically important that your vendors, such as on-demand billing and CRM providers, stand up to scrutiny by reaching Level 1 PCI compliance—the highest level possible.

By dealing only with service providers that have achieved Level 1 PCI DSS compliance validation, companies can be assured of fully secure support of online applications, regardless of the volume of credit card information stored, processed or transmitted.

Studies bear this out. A recent report from on-demand data security and compliance management vendor Trustwave found that smaller merchants that typically rely on a lower level of PCI compliance are more often targeted by malicious hackers.

But finding the right service provider, with the right dedication and competence, requires diligence.

No matter how many transactions a company processes per year, insisting on a Level 1 compliant service provider will ensure the highest level of security. To make sure you're dealing with a Level 1-qualified company, insist on seeing the service provider's certificate of Level 1 status.

Trustwave has yet to investigate a single case of payment card compromise in which the victim has been in compliance with the PCI DSS at the time of the breach.

—**Trustwave Global Compromise Statistics**, Quarterly Report, March, 2008

Trustwave®
Information Security & Compliance

To assess the service provider's commitment to keeping abreast of the latest in PCI compliance, make sure the company devotes a team to the process on an ongoing basis. Make sure the company's engineers stand ready to make any changes necessary, and to act proactively.

Ask about the company's track record. Have they ever been involved with a data breach, either internally or involving a customer? And ask for—and check—references. If other companies are satisfied with the service provider, chances are you will be as well.

Here are some questions to ask before hiring a service provider:

- What was the process you went through to become Level 1 PCS-DSS compliant?
- What is your process for maintaining compliance?
- How many engineers are devoted to PCI compliance?
- What lengths do you go to ensure that your PCI compliance processes and procedures are top-quality and up to date?
- What testing processes do you use?
- How do you ensure that your system does not store cardholder data such as track data or card security codes.
- Do your applications undergo a third-party code review and application penetration test annually?
- Have you ever been involved in a data breach, either internally or through a client?
- Is the environment properly segmented from public networks?
- Is two-factor authentication enabled as required by PCI DSS?
- How long have you been in business?
- Can I talk to some satisfied customers?

BEYOND ASKING HARD QUESTIONS, PROTECT YOURSELF AND CHECK ON YOUR BILLING PROVIDER

The PCI Security Standards Council cannot prevent companies from claiming PCI Compliance (in fact many do), but only those that are named in the PCI Data Security Standard (PCI DSS) annual report are truly compliant. Companies that are unsure of whether or not their billing provider is PCI Level 1 compliant are urged to check the list of those companies that are certified as such, at http://usa.visa.com/merchants/risk_management/cisp_service_providers.html.

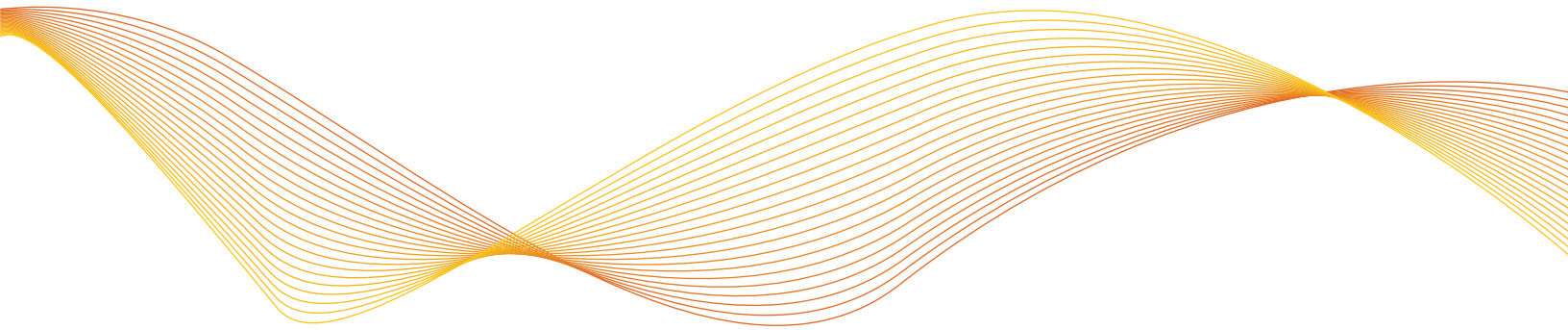
ARIA SYSTEMS: AN EXPERIENCED, LEVEL 1 PCI COMPLIANT BILLING VENDOR

Aria Systems puts its customers—and their customers—first. As a Level 1 PCI-DSS compliant on-demand billing and customer lifecycle management vendor, Aria Systems ensures the security of all transactions.

Level 1 PCI-DSS compliance means submitting to an annual on-site PCI security audit and quarterly network security and vulnerability scans, each by an independent auditor. Those independent assessments ensure that Aria Systems complies at the highest level with all security standards related to maintaining a secure network, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks, and maintaining an information security policy.

That means implementing multiple security levels to restrict the data individual CSRs can view and the actions they can perform, encrypting payment card data at both the network and database layers, tightly controlling network access and monitoring by firewalls and intrusion detection systems. In addition, Aria Systems offers an optional, additional layer of security featuring third-party authentication with programs such as MasterCard SecureCode and Verified by Visa.

All of this takes dedication: a team of engineers is dedicate to maintaining and updating PCI compliance-related issues on a daily basis, and making sure that the company's policies, processes and procedures are followed without fail.



Aria Systems is the leading provider of subscription billing solutions and offers the only "monetization platform" encompassing the full spectrum of Billing and Customer Lifecycle Management services. The **A+ Billing Platform** offers clients the on-demand billing industry's most flexible tool for accelerating revenue capture, optimizing cash flow, and enabling actionable market intelligence while significantly reducing operating costs throughout each phase of the customer lifecycle. Acknowledged as the SaaS billing leader in terms of experience and execution, Aria manages and maintains more than 1 million accounts and has processed more than 1 billion transactions since it began operations in 2003. With Hummer Winblad, Venrock, and software billing icon Dave Labuda as investors, the company is based in Media, Pa. (metropolitan Philadelphia), with offices in the San Francisco bay area as well.

Learn more at www.ariasystems.com