



World Class Security

- PCI Level 4 Compliance
PCI DSS Certificate #
D282-6F6B-2114-36AD
- All data is backed up daily to additional storage devices.
- Staffed 24/7/365 by advanced technical and security personnel.
- To ensure continuous operation, LeadMaster manages fully redundant data lines.
- Security patches are monitored and kept up to date on all servers.
- All servers are backed up on a daily basis.

LeadMaster Security and Infrastructure Advanced Security Systems

Infrastructure

The LeadMaster application resides on state-of-the-art industry standard server platforms in a VM environment. To maximize uptime, each server is configured with RAID Level 5 and hot-swap drives. Our primary production servers are backed up with real-time standby servers waiting to assume the identity of a production system in the event of failure.

PCI Compliance

The gold standard in security, LeadMaster is certified as Level 4 PCI compliant. The certificate is attached at the end of this document.

Physical security

LeadMaster's production equipment is housed at a **world-class network operations facility**. Staffed 24/7/365 by advanced technical and security personnel, the restricted access data center enforces strict security measures to ensure security of equipment and data, including identification checks. This facility possesses a Class-A government disaster rating against hurricanes, power failures, nuclear fallout and war related threats. Our data center location is also equipped with multiple backup systems in the event of power failure or natural disasters, including full redundant battery backup power, a diesel backup generator and hurricane disaster rating.

Reliability

To ensure continuous operation, LeadMaster manages fully redundant data lines from multiple carriers. In the event that one carrier experiences an outage, all system traffic is automatically transferred to an alternate carrier.

Perimeter defense and internal systems security

LeadMaster has taken rigorous measures to ensure the security of its network and servers as well as all data residing on the system. All data travels over a secure network with personnel strictly adhering to all security precautions. Multiple firewalls and operating system lock-down methods are in place to prevent unauthorized access. To further our intrusion detection procedures, our staff continually reviews security and network logs to identify vulnerabilities. Security patches are monitored and kept up to date on all servers.



LeadMaster custom user security permissions are defined in a security matrix developed in consultation with each client.

Data backup

Data backups are performed daily to a Storage Area Network. Backups are stored for up to 30 days.

Data encryption

LeadMaster offers the strongest browser encryption available through 128-bit SSL data encryption in order to protect all client data transmitted to and from the system via the Internet. A signed security certificate ensures that confidential information cannot be viewed, intercepted or altered. Users are alerted to the secure status by a lock displayed in the browser window.

User authentication

Logon to the online LeadMaster system requires verification of a unique username and password, which the user may send encrypted via SSL.

Access control

LeadMaster controls access to each client database as well as to specific functions within the system. Custom user security permissions are defined in a security matrix developed in consultation with each client. This matrix identifies the client's unique user types and defines the access privileges imparted to users in each group. This system allows both flexibility and tight security, as it can allow or prohibit access to any or all functions within the system, as well as limiting access by geography or campaigns.

Logging

User activity within the system is logged to provide clients with an audit trail if the need arises.

The image shows a PCI DSS Certificate of Compliance issued by Trustwave. The certificate is for LeadMaster Operating Company, classified as a Merchant, with an expiration date of 2012-08-01. The certificate number is 63CA-8885-39CA-B0DD. The awarded to section lists LeadMaster Operating Company. The Trustwave Engagement Information section includes details such as Self-Assessment Questionnaire: Pass, Date Completed: 2012-02-29, Version Completed: PCI SAQ C 2.0, Client SAQ Attestation: Russell King, Title: Founding Partner, Vulnerability Scan: Pass, and Date Completed: 2012-05-01 20:38:18. The client authorization section is signed by Andy Brownell, Founding Partner. The certificate includes a disclaimer and participating organizations: Visa® Europe, Visa® Inc., MasterCard® Worldwide, American Express®, Discover® Financial Services, JCB Co., Ltd. The Trustwave logo and tagline "Security begins with Trust" are also present.

PCI DSS Certificate of Compliance

Certificate Number: 63CA-8885-39CA-B0DD

Awarded To:
LeadMaster Operating Company
Classification: Merchant
Expiration Date: 2012-08-01

Trustwave Engagement Information
Self-Assessment Questionnaire: Pass
Date Completed: 2012-02-29
Version Completed: PCI SAQ C 2.0
Client SAQ Attestation: Russell King
Title: Founding Partner
Vulnerability Scan: Pass
Date Completed: 2012-05-01 20:38:18

Client Authorization: Andy Brownell
Print Name Sign Name

This signed contact at LeadMaster Operating Company agrees to the accuracy of all information provided within TrustKeeper.

To maintain compliance, the above named client (referred to below as "CLIENT") must be aware of and validate against their individual requirements as set by the Payment Card Industry Security Standards Council and the payment card brands. For information on requirements, please visit www.pcisecuritystandards.org. In addition, CLIENT must continually identify and provide to Trustwave information regarding any new system that stores, processes, or transmits cardholder data, so that this system can be included in the scope of the validation process. This certificate is valid through the expiration date stated above. It is the client's sole responsibility to maintain compliance with the card association security requirements and obtain validation on at least a quarterly basis. Trustwave makes no representation or warranty as to whether CLIENT systems are secure from either an internal or external attack or whether cardholder data is at risk of being compromised. This certificate is for the sole purpose of identifying compliance and the attestation for said compliance by CLIENT and cannot be used for any other purpose without the express written consent of Trustwave's legal counsel.

Participating organizations: Visa® Europe, Visa® Inc., MasterCard® Worldwide, American Express®, Discover® Financial Services, JCB Co., Ltd.

Trustwave
Security begins with Trust™

Trustwave ©2012