A Pronto MSP
Case study

# PCI DSS Compliance for User Data Security

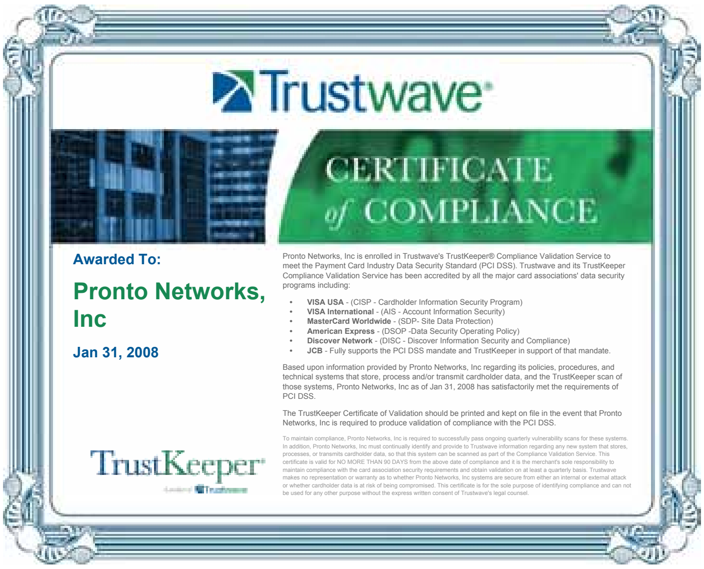
## Empowering WISPs with secure credit card processing solutions, compliant to mandatory Payment Card Industry Data Security Standards

In recent years, companies have come to realize that astronomical losses aren't always incurred in the form of money. Theft of information such as customers' credit card details can cost companies much more than just hefty fines. It can erode hard-earned brand reputation, too. In June 2005, details of 40 million credit cards were stolen from the database of an Atlanta-based credit card transaction solution provider. Visa and American Express subsequently stopped business with the company. In May 2007, the wireless LAN security breach at a Massachusetts-based company resulted in the largest credit card theft in history. Such cases comprise just a fraction of data theft attacks on networks across the globe.

The coin has a brighter side, though. Companies can easily avert data theft by ensuring adherence to PCI DSS (Payment Card Industry Data Security Standard), which has now been made mandatory. Companies found not adhering to the Standards may end up paying enormous fines to PCI and the government. Punitive measures, apart, the sheer peace PCI Compliance brings with it is motivating companies to go for it. WISPs are also joining the league.

### Pronto MSP's Security Assurance

Pronto Networks' Managed Service Platform (MSP), which has proven itself as a reliable credit card processing partner for WISPs, now comes with the assurance of PCI DSS Compliance. Ambiron has independently checked and passed Pronto MSP's Verisign transactions for PCI DSS Compliance. Pronto MSP's wireless security policy manages user credentials and tailors policies based on their levels of authorization. In addition, the wireless infrastructure itself is protected from attacks. Pronto OSS' Oracle Database (DB) structure and Centralized Authentication ensure that all user data such as passwords, ids and credit card details are stored in a central repository. In simple terms, all the sensitive information is stored in one 'digital safe', in a format that can be read only by security policy manages user credentials and tailors policies based on their levels of authorization. In addition, the wireless infrastructure itself is protected from attacks. Pronto OSS' Oracle Database (DB) structure and Centralized Authentication ensure that all user data such as passwords, ids and credit card details are stored in a central repository. In simple terms, all the sensitive information is stored in one 'digital safe', in a format that can be read only by Pronto OSS. The hardened system opens ports and protocols for authorized users only. Centralized authentication system authorizes users by authenticating their unique credentials, through information accessed from the central repository.



Trustwave®

CERTIFICATE *of* COMPLIANCE

Awarded To:

**Pronto Networks, Inc**

Jan 31, 2008

Pronto Networks, Inc is enrolled in Trustwave's TrustKeeper® Compliance Validation Service to meet the Payment Card Industry Data Security Standard (PCI DSS). Trustwave and its TrustKeeper Compliance Validation Service has been accredited by all the major card associations' data security programs including:

- **VISA USA** - (CISP - Cardholder Information Security Program)
- **VISA International** - (AIS - Account Information Security)
- **MasterCard Worldwide** - (SDP- Site Data Protection)
- **American Express** - (DSOP -Data Security Operating Policy)
- **Discover Network** - (DISC - Discover Information Security and Compliance)
- **JCB** - Fully supports the PCI DSS mandate and TrustKeeper in support of that mandate.

Based upon information provided by Pronto Networks, Inc regarding its policies, procedures, and technical systems that store, process and/or transmit cardholder data, and the TrustKeeper scan of those systems, Pronto Networks, Inc as of Jan 31, 2008 has satisfactorily met the requirements of PCI DSS.

The TrustKeeper Certificate of Validation should be printed and kept on file in the event that Pronto Networks, Inc is required to produce validation of compliance with the PCI DSS.

To maintain compliance, Pronto Networks, Inc is required to successfully pass ongoing quarterly vulnerability scans for these systems. In addition, Pronto Networks, Inc 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 scanned as part of the Compliance Validation Service. This certificate is valid for NO MORE THAN 90 DAYS from the above date of compliance and it is the merchant'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 Pronto Networks, Inc 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 can not be used for any other purpose without the express written consent of Trustwave's legal counsel.

TrustKeeper®

Complimenting the centralized security features is Pronto MSP's registration portal - customized for your customers – that ensures secure collection of sensitive credit card information. Thus, Pronto MSP ensures that while your customers experience completely secure credit card transactions, you are safe against loss of reputation or money.

### Why Pronto MSP?

1. Pronto MSP has passed PCI compliance check independently conducted by Ambiron
2. Pronto's PCI compliant system ensures safe processing of your customers' credit card details, during Verisign transactions
3. Centralized authentication and centralized policy determination through integrated Oracle DB ensure complete security for your customers' credit card information, even in the involvement of 3rd party ISPs

### Pronto MSP's PCI Compliant Security Measures

1. Building and maintenance of a secure network
2. Protection of cardholder data
3. Maintenance of a vulnerability management program
4. Implementation of strong access control measures
5. Regular monitoring and testing of networks
6. Maintenance of an information security policy

Corporate Headquarters: 4637 Chabot Drive, Suite 206 Pleasanton, CA 94588. Tel: 925 227 5500
For more information: www.prontonetworks.com, email: info@prontonetworks.com