

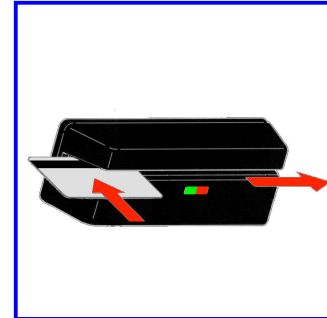


Card-Trak System™ Security Bulletin

Issued: 01.03.13

Description

The Bellatrix Card-Trak System gathers stores and transmits credit card sales information. To ensure the security of the transactions, the Card-Trak System complies with or exceeds the security requirements of Payment Card Industry (PCI) Data Security Standard (DSS) version 2.0 Bellatrix is committed to providing a secure and effective credit card purchase experience for our newspaper customers.



Payment Card Industry Data Security Standard

PCI DSS version 2.0 is a set of comprehensive requirements for enhancing payment account data security that was developed by the founding payment brands of the PCI Security Standards Council to help facilitate the broad adoption of consistent data security measures on a global basis. Members include American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. A complete description of the standards used is available at: <https://www.pcisecuritystandards.org>

Background

The Card-Trak System for newspapers has been accepted for use by the major newspapers groups including Belo, McClatchy, Gannet, Newscorp, Dow Jones, and the Tribune Companies. Card-Trak is accepted for use by major credit card processors including PayPal, Chase Card Services, and Paystation.

These companies have validated the strong security features of the Card-Trak System. In addition, Coinstar Entertainment retained an independent QSA (Qualified Security Assessor) to validate that the Card-Trak System is compliant with existing rules and regulations for the Payment Card Industry.

Security Specifics

The security specifics of the Card-Trak System remain confidential so as to protect the security of our clients; however, we can share the following information to address specific PCI DSS security questions.



Card-Trak System™ Security Bulletin

Issued: 01.03.13

Data Storage Security

Card-Trak Data is always stored with full encryption in all phases of the credit card transactions as per PCI standards. When the customer uses a credit card, only a portion of the data track is stored and is fully encrypted as per PCI standards. Data is stored in the individual credit card swipe units until retrieved and is fully protected by encryption to AES 128 standards. Even if the reader unit is removed, the data and software may not be removed as the hardware is locked and the data is fully encrypted to PCI standards.

Data Transmission Security

Data is retrieved via infrared (IR) link from a ruggedized PDA that operates with proprietary Card-Trak software. The PDA encrypts the data one more time and access is password protected. To provide additional security the PDA is “paired” with each Card Trak reader unit. A PDA handheld that is not paired will not communicate with the Card-Trak reader. These redundant security functions protect the data to PCI standards.

The upload PC runs additional proprietary Card-Trak software. The Data that is retrieved from the handheld at the upload PC is stored in an encrypted format and then decrypted before being re-encrypted for transmission over the Internet to the credit card processor. The standards for the transmission encryption and delivery of data are determined by the credit card processor. This PC is also protected by multiple levels of security, including passwords (multiple) and an electronic key that is removed from the machine when not in use by an authorized operator. These functions ensure that data passing through the PC is password protected as per PCI standards.

Employee Security Training

In addition to the security features of the hardware and software Bellatrix provides the users with best practice methods for security including password changes, hardware control and security policies. This instruction also assures compliance with PCI standards.

