

USA800 Data Security Standards

USA800 is PCI Level-1 compliant. The key purpose of achieving this certification is to process payment cards securely in a manner that protects USA800, its clients and their customers from the risks of data compromise and fraud. Compliance with the Payment Card Industry Data Security Standard (PCI DSS) focuses on protection measures surrounding full primary account numbers (PANs) and the associated three-digit or four-digit card verification code (CVV2, CVC2, CID, or CAV2) in face-to-face, e-commerce, and Mail Order/Telephone Order (MOTO) environments. PCI certification is important because it means that USA800 has taken formal steps to prevent any security breach, and in particular any related to use of payment cards. Organized crime is constantly developing new techniques to acquire and make unauthorized use of payment card information. While PCI compliance does not guarantee invulnerability, it demonstrates that USA800 has taken the necessary steps to prevent a breach, and has also implemented measures to detect and remediate any new techniques that come about. This brings peace of mind to consumers that all reasonable steps have been taken to protect them from financial fraud, which in-turn enables USA800 and its clients reduce vulnerability and business risk.

In order to become PCI compliant, USA800 engaged IOActive, an authorized third-party assessor (QSC) certificated by the PCI SSC. IOActive conducted a third-party security assessment in line with the Payment Card Industry Data Security Standard (PCI DSS) to determine that USA800 has satisfactorily achieved compliance with that standard. The scope of the assessment covered the requirements that comprise VISA's Cardholder Information Security Program (CISP) and MasterCard's Site Data Protection (SDP) program, as well as Discover's (DISC) and American Express's Data Security Operating Policies. During the process, USA800:

- Engaged AT&T Managed Security Services to conduct penetration testing and provide intrusion detection and intrusion prevention
- Remediated any security risks identified by IOActive and AT&T
- Updated policies surrounding handling of payment card data
- Implemented revised physical and technical security procedures
- Modified software coding, management, review, testing and deployment practices
- Upgraded all technical systems and infrastructure associated with payment card data
- Deployed mechanisms to pause and resume voice recordings during payment card information exchange
- Trained all personnel developing systems or handling PCI-related information
- Ensured no storage of PAN or CVV beyond persistence and transmission of the current transaction
- Tokenized all mechanisms that process or transmit cardholder data
- Eliminated any historical recording or storage of PAN or CVV

Intrusion detection and prevention technologies are permanently built into USA800's network, and we will continue with regular penetration testing (security scans) as part of the process of maintaining PCI compliance. We are committed to protecting our clients, their customers and ourselves from the risks of data compromise and fraud.