CORE

# A Partner That Values Security & Compliance

Security and compliance are critical for every technology purchase, but for your agency's payment platform, they are paramount to deliver a seamless, secure, and satisfactory experience for both citizens and agency staff. Data breaches run rampant in today's online payment world. Without a PCI-DSS Level 1 compliant platform and a partner committed to delivering a secure, flexible system, agencies leave themselves open to incredible risk.

**NEARLY 70% OF CONSUMERS**
worry about the security of the digital platforms they use to make payments.

**7 OUT OF 10 CONSUMERS**
say they feel more comfortable using a payment method that doesn't require sharing financial details with merchants.

Ransomware and phishing attacks targeting local government agencies
**INCREASED BY 65%**
in the last two years.

**MORE THAN 50%**
of local governments experienced data breaches in the last year.

Organizations found to be non-PCI compliant can expect fines between
**$5,000 - $100,000 PER MONTH.**

**54% OF CONSTITUENTS**
say that government agencies are not keeping up with innovations in bill pay (and they wish that local government agencies would emulate the practices implemented by the banking industry).

**83% OF CONSUMERS**
prefer to make payments digitally on their phones or other online platforms.

With a payment platform built with top-level security and compliance, government agencies can confidently deliver a safe payment experience for constituents, keep data and citizen information safe, and plan for future risks with a security and compliance-focused partner.

CORE

## CORE's security and compliance offers:

### Encryption, Tokenization, and Hosted Solutions

CORE offers increased security and compliance with encryption, tokenization, and hosted solutions. Secure EMV/ chip credit card solutions reduce fraud while also providing a great experience to citizens during payment. CORE also incorporates industry best practices, including safeguards for password protection, inactive users, application timeouts, and more.

### Detailed Audit Trails

A digital audit trail is available in CORE, making it easy to search for specific charges or citizens. Any addition, void, or reversal is tracked within the audit trail. Detailed logs of user activity are also maintained, including user identification, type of event, date and time of event, result of the event, originating location of the event, and the name of the affected data, system component, or resource. These logs are protected from unauthorized access, secured by a file integrity monitoring (FIM) system. This system alerts the Compliance Committee upon unauthorized access.

### Secure Access Controls

Within CORE, user role-based access is assigned by user group, department, and application-specific controls. These user-based access types allow some users more access to the backend, while protecting other users from seeing confidential information.

### Robust PMO Processes

Designed to help every new customer rollout their customized CORE solution on time and aligned with specific safety standards, CORE's PMO follows a proven process. This process includes a design phase to identify specific requirements, a development and configuration phase to tailor the platform to those requirements, a test phase to ensure everything is secure and running smoothly, a training phase to educate users, a go live phase, and a support phase.

CORE

# PCI-DSS Level Compliance

CORE maintains compliance with PCI (Payment Card Industry) standards through a comprehensive approach that encompasses several key practices:

## Regular Audits and Assessments

CORE undergoes regular audits and assessments conducted by qualified third-party assessors to ensure adherence to PCI standards. These assessments evaluate various aspects of the organization's systems, processes, and controls to identify any non-compliance issues.

## Secure Network Architecture

CORE employs robust network architecture designed to safeguard sensitive cardholder data. This includes implementing firewalls, encryption, intrusion detection systems, and other security measures to protect data both in transit and at rest.

## Data Encryption

All cardholder data processed, stored, or transmitted by CORE is encrypted using industry-standard encryption algorithms. This encryption ensures that sensitive information remains secure and inaccessible to unauthorized parties

## Access Control Measures

CORE implements strict access controls to restrict access to cardholder data only to authorized personnel who require it for their job responsibilities. This includes role-based access control, strong authentication mechanisms, and regular review and updates of access permissions.

## Security Policies and Procedures

CORE develops and maintains comprehensive security policies and procedures that outline specific requirements for handling cardholder data. These policies cover areas such as data storage, transmission, access control, incident response, and employee training.

## Employee Training and Awarenes

CORE provides regular training and awareness programs to all employees to ensure they understand their responsibilities regarding PCI compliance. This includes training on security best practices, handling of cardholder data, recognizing and reporting security incidents, and compliance requirements.

### Vulnerability Management

CORE employs robust vulnerability management processes to identify, assess, and mitigate security vulnerabilities in its systems and applications. This includes regular vulnerability scans, penetration testing, and timely patch management to address any identified weaknesses.

### Incident Response Plan

CORE maintains a detailed incident response plan to effectively respond to and manage security incidents or breaches. This plan outlines the steps to be taken in the event of a security incident, including containment, investigation, remediation, notification, and recovery.

### Continuous Monitoring and Improvement

CORE continuously monitors its systems and processes to identify areas for improvement and enhance its overall security posture. This includes staying informed about emerging threats and evolving security technologies to adapt and strengthen its defenses accordingly.

**By implementing these practices and maintaining a strong commitment to security and compliance, CORE ensures that it meets and exceeds the stringent requirements set forth by the PCI Security Standards Council.**

CORE

## Staying Secure and Compliant with CORE:

With more than 30 years of experience, CORE has delivered integrated solutions to government agencies—at the city, county, and state level—and other organizations across the nation. Designed to meet the latest standards for accessibility and safety, CORE's platform is certified to meet the highest security standards. Choosing a partner who understands the risks of taking payments online, in-person, and out in the field is critical. A proven partner can provide guidance and assist government agencies as they transition from outdated systems, cash payments, and more.

To ensure your agency offers a safe, secure, and compliant payment process, we recommend:

### Prioritizing Citizen Data Privacy

Keeping citizen data safe and secure is important, but maintaining citizen privacy is even more critical. At CORE, we protect citizen's data as if it were our own. By prioritizing citizen data privacy, CORE and government agencies can maintain citizen trust, helping agencies continue to operate effectively and efficiently.

### A Culture of Security and Privacy

Security and privacy are at the forefront of every CORE platform design and update. Training, code reviews, and policy and procedure adherence is baked into the culture at CORE. Processes and technology are architected to maintain the highest level of security, while also prioritizing frictionless, seamless experiences for both citizens and agencies.

### Risk Mitigation to Prevent Data Breaches

To prevent a data breach that could cost your agency millions and damage your reputation irreparably, CORE employs best-in-class industry standards of security and compliance. User training and ongoing support add to CORE's risk mitigation efforts.

## TRANSFORM YOUR PAYMENT EXPERIENCE

PCI-DSS Level-1 Compliant Platform

Anywhere, anytime, any device access

Actionable reporting and insights

CORE

corebt.com

866.567.CORE (2673)

950 Warren Avenue, Suite 400,
East Providence, RI 02914

EMV REGISTERED
Single Dip • Service Fee Processing • EMV Certified

PCI COMPLIANT
Level 1 Proivider

REGISTERED ISO/MSP

ACH

VISA
GLOBAL REGISTRY OF SERVICE PROVIDERS
On the list! 2022

HIPAA COMPLIANT

eta

TPSP
AMERICAN EXPRESS

TPS PROVIDER
NACHA