ONE INC

Data Security and Compliance

One Inc adheres to industry-leading security requirements that reduce your risk of exposure, simplify your network security and compliance practices, and protect your policyholders from payment data theft.

As a fully certified and compliant payment service provider, our security practices consist of the following:

Audit and Assessment Standards

Annual audits include Payment Card Industry Data Security Standard (PCI DSS) Level 1 attestation and System and Organization Controls (SOC) compliance.

Data Monitoring

We deploy industry standard security appliances (F5, Cisco), as well as WAF and IPS Cloud protection services which constantly monitor traffic and block requests considered to be a threat.

All data at rest is encrypted via Transparent Data Encryption(TDE). TDE performs real-time I/O encryption and decryption of the data and log files. Data in transit utilizes HTTPS (HTTP over Transport Layer Security TLS1.2) to encrypt data.

Our release process relies on the execution of automated tests specifically focused on security. Our suite of security-focused tests is executed prior to every release, and test content is reviewed and updated as threats are discovered.

Secure Data Centers

All facilities that host our applications are SOC 2 compliant.

Our colocation data centers utilize the following security measures:

- Multiple physical barriers and locks
- Seven-layer physical surveillance 24 hours a day, 7 days a week, 365 days a year
- Security officers engage in a proprietary security academy that teaches advanced skills in counter-surveillance, surveillance, detection and other tactical protection measures.

Regular Security Training

Pursuant to our PCI DSS Level 1 attestation, our development team is directly involved in annual security training throughout the year. All members of the development team maintain a proficient level of understanding of security trends and threats. Our security team also subscribes to Homeland Security's US-CERT publications, OWASP's publications, and information security publications.

PCI

Payment Card Industry Data Security Standard

Audit of all One Inc systems that store, process, or transmit cardholder data to ensure compliance with the standards set by the PCI DSS Council.

Nacha™

ACH Rules Compliance Audit

Audit of ACH processing controls and operational efficiency ensuring compliance with ACH rules set by Nacha.

HIPAA COMPLIANCE

HIPAA Compliance

Evaluation of One Inc's ability to protect the privacy and security of Protected Health Information (PHI) according to the standards of HIPAA Privacy regulations.

WELLS FARGO

PINless Debit Compliance Assessment Program

Security assessment of policies and procedures around PINless bill payment transactions, ensuring they are in compliance with Payment Network Operating rules.

---

mastercard

Global Risk Management Program

Evaluation of One Inc policies and procedures around compliance, fraud and risk management, data security, business continuity, and customer boarding according to the standards set by MasterCard.

AICPA SOC

System and Organization Controls

Examination of suitability of One Inc payment application security controls according to the standards set by American Institute of Certified Public Accountants (AICPA).

GLBA FISMA SOX

The Gramm-Leach-Bliley Act (GLBA) Compliance

Assessment of One Inc's procedures to protect and appropriately disclose customers' private information.

For a complete list of One Inc's security programs and certifications, visit: https://www.oneinc.com/company/certifications

ONE INC