Dear Client,

Official Payments is required to be compliant with a number of industry standards that overlap with many of the SSAE 16 (formerly known as SAS 70) standards to ensure that operational controls related to financial reporting, security, processing integrity and confidentiality are in place.

We are regularly audited by independent third party assessors to ensure our strict adherence and compliance with those standards and regulations and thus have chosen not to pursue the additional testing associated with SSAE 16.

As a result of independent third party assessments, Official Payments is compliant with the following:

- Payment Card Industry Data Security Standard (PCI DSS) – Level 1 Service Provider. The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. You may read more about these standards at https://www.pcisecuritystandards.org/. You can confirm that Official Payments has met the requirements by reviewing the list of PCI DSS Compliant Service Providers at http://www.visa.com/cisp.

- Internal Revenue Service (IRS) – Independent Verification and Validation. The Internal Revenue Service (IRS) performs an annual Independent Verification and Validation (IV&V) Security Risk Assessment of the Official Payments infrastructure. This assessment includes, but is not limited to Vulnerability Assessments (Internet penetration and intrusion detection testing) and Application Functionality Assessments of the Official Payments credit/debit card payment system and network. The IV&V Security Risk Assessment scope is limited to the existing system configuration and review of the system relative to its conformance with National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53 Recommended Security Controls for Federal Information Systems. NIST SP 800-53 addresses security controls for the following computer areas:
  - Computer Security
  - Communications Security
  - Personnel Security
  - Physical Security
  - Security Education, Training and Awareness
  - Procedural Security

  Included within the scope are hardware components, software components, operating procedures and data.

3550 Engineering Dr, Suite 400, Norcross GA 30092
[p] 770.325.3100 [f] 770.325.3099
[url] www.OfficialPayments.com

A technical analysis of the network infrastructure is also conducted to determine the degree to which components may be susceptible to attacks or incidents that could have an impact on data confidentiality or integrity or lead to resource misuse. The network vulnerability assessment includes an External Network and Firewall Vulnerability Assessment, Internal Network Vulnerability Assessment and a Dial-up Access Vulnerability Assessment.

- National Automated Clearing House Association. NACHA oversees the Automated Clearing House (ACH) Network, one of the largest electronic payment networks in the world. NACHA is responsible for the administration, development and enforcement of the NACHA Operating Rules and sound risk management practices for the ACH Network. More information may be obtained at www.nacha.org and www.electronicpayments.org.

- TRUSTe – Web Privacy Seal Holder. TRUSTe helps consumers and businesses identify trustworthy online organizations through its Web Privacy Seal, Email Privacy Seal and Trusted Download Programs. More information is available at www.truste.org.

- Sarbanes-Oxley (SOX). The Sarbanes-Oxley Act requires audits that review controls, policies and procedures that show a company's financial data is accurate and that adequate controls are in place to safeguard the data. The Sarbanes IT audit is a system level audit that focuses on the reliability and integrity of hardware, software and information in the systems.

For additional information, please contact:

Raj Gautam
Information Security Officer
Phone: 925-855-5087
Email: Raj.Gautam@OfficialPayments.com

Sincerely,

Official Payments

July 2012