ACI UNIVERSAL PAYMENTS℠

ACI WORLDWIDE aciworldwide.com

March 26, 2020

Dear Customer,

During this rapidly changing and unprecedented time, ACI Worldwide hopes that you, your employees, and your loved ones stay safe and well. We have taken significant steps to help ensure the safety of our employees and their families, and we have also moved quickly to protect the payments that are critical to your business and your consumers.

I want to make you aware of an important measure ACI recently implemented to promote safety and business continuity: **We are now requiring most of our employees, including call center employees, to work from home.**

I also want to assure you that ACI has PCI-assessed policies, procedures, and security measures in place to allow employees to securely work from home in a compliant manner. We are utilizing our existing work-from-home policies to train agents, issue secure laptops, and provide secure connections to applications. Our call center work-from-home procedures have been reviewed by ACI's Qualified Security Assessor (QSA).

ACI is committed to maintaining a secure and compliant call center environment. Our call center employees, along with all ACI employees, receive regular security training. The following is a snapshot of requirements in place for our work-from-home call enter employees:

- Establish a designated workspace adequate to perform job responsibilities.
- Take necessary measures to maintain confidentiality of all ACI information and consumer data.
- Permit ACI to inspect the off-site workspace during normal working hours.
- Ensure that no person, other than the ACI employee, is authorized to use ACI equipment; agree to only use ACI equipment for work purposes.
- Comply with all ACI policies, specifically but not limited to, the ACI Global Code of Business Conduct and Ethics, ACI Global Acceptable Use Policy, and ACI Global Information Security Policy.
- Do not copy, move, share, or store any payment card data.
- Use only company-approved hardware devices (mobile phones, telephone handsets, laptops, etc.).

ACI's standard security controls remain unchanged. We continue to secure your data and comply with contractual, compliance, and regulatory requirements. At a high level, these controls include:

- Access and Authorization Controls, including multi-factor authentication, laptop/desktop endpoint security, and remote access via encrypted Virtual Private Network (VPN)
- Data Loss Prevention (DLP)
- Full Disk (Whole Disk) Encryption
- Web-Content Filtering
- Network Admission Control (NAC) / Client Certificate Validation
- Email Security Controls

ACI’s commitment to providing you with a secure and compliant call center solution and secure digital payment options remains consistent during the current global crisis. With ACI working for you, I hope you have more time to concentrate on your rapidly changing priorities and the continued wellbeing of your employees.

Sincerely,

Gene Scriven
Chief Information Security Officer