7.9 SYSTEMS AND OTHER QUESTIONS

Please explain your Disaster Recovery/Systems Redundancy

Our business continuity, disaster recovery and resiliency plans are customized for each client. They are distributed to all key management personnel and updated semi-annually. Copies of the plan are kept locally, as well as on a corporate server located in Dallas, Texas. All plans are backed up in the Azure Cloud.

Please review the *attached document* for details, including:

- Prevention
- Distributed agent workforce locations
- Process flow
- Recovery
- Emergency management team

Describe your back-up and redundancy. Do you have a backup generator at each site and the proposed location to handle this business?

All platform services are provided via the cloud and all (multiple) data centers are fully redundant to include UPSs, generators, A/C components and dual-path electrical and telecom paths.

Agent redundancy is ensured by having an on-demand, onshore workforce dispersed throughout the United States and Canada. Our virtual business model enables us to shift work and resources as business demands fluctuate and weather changes.

Do you have a redundant internet and telecom providers?

Multiple carriers are used for internet access and telephony routing for inbound and outbound calls

How much downtime has your contact centers experienced in the past 12 months due to systems, electrical and weather-related incidents?

There has been zero downtime during this period—none occurring due to system-, electrical- or weather-related events.

What days of the week and hours is your IT center staffed?

Our IT operations are manned 24 hours, 7 days a week.

How many people do you have in your systems department?

We have 14 IT professionals.

Describe your technology and systems as it relates to this project for the following:

- **CRM – N/A**
- **Dialer- Bright Pattern. Dialer, if applicable supports preview, predictive and progressive dialing.**
- **ACD – N/A**
- **Email – Use Zillow's system.**
- **Live Web Chat – Use Zillow's system.**
- **Social Media – N/A**
- **Digital Recording – Bright Pattern: 100% of calls are recorded and stored securely.**
- **Workforce Management – Vyne, proprietary Working Solutions agent website where leaders and agents see program status and alerts, receive business updates, review performance metrics, and share other real-time information. (Section 7.10 of this RFP offers a more in-depth look at Vyne.)**
- **Chatbots – N/A**
- **Artificial Intelligence – N/A**

Long-distance (LD) providers?

Working Solutions uses multiple LD carriers.

Compliance and Certifications (PCI, HIPAA, SOC2, etc.) PCI is a requirement.

Working Solutions is PCI Level 1 certified. An *AOC is provided here*.

Ensuring compliance: For the Payment Card Industry Data Security Standard (PCI DSS), Working Solutions completed its last audit in October 2018. The 2019 audit is being finalized now. All parts of platforms and operations are Level 1 certified for credit card transactions. Covers security management, network architecture, software design and development, storage and transmission, and remote-access policies. Vulnerability scans of systems are done quarterly.

Going beyond certification: Industry standards certainly have their place. They are, however, are just the price of admission to safeguard data and privacy. That's why at Working Solutions we invest in common-sense measures, such as data masking and securing agent desktops, if required, to further ensure consumer protection and privacy.

Integrated approach

To protect information, Working Solutions focuses on agents, infrastructure and data for an integrated security strategy.

Agents: Agents adhere to strict administrative processes and physical security standards. Included are ethics and security training, clean-desk policy, business associate agreements and confidentiality compliance for HIPAA (Health Insurance Portability and Accountability Act). Rigorous background checks and drug screening are conducted.

Infrastructure: Working Solutions offers multichannel contact center application services. Residing in a hardened environment, these services provide peace of mind for clients and their customers. This work encompasses disaster recovery, redundancy and failover. Network security includes firewalls, redundant technology and intrusion detection.

Data: Technical standards are met for data protection, ranging from Payment Card Industry Data Security Standard (PCI DSS) Level 1 security for payment card transactions to HIPAA compliance for healthcare. Our work adheres to documented and auditable policies, procedures and processes to protect physical data—as well as encryption and monitoring for data in transit.