Liquid Web™

INDEPENDENT PRACTITIONER'S TRUST SERVICES REPORT

LIQUID WEB, LLC

Co-Location, Web Hosting, and Network Infrastructure Services

Trust Services Report on Management's Assertion

For the Period
July 1, 2016 – June 30, 2017

UHY LLP
Certified Public Accountants

LIQUID WEB, LLC

Trust Services Report on Management's Assertion

TABLE OF CONTENTS

UHY LLP
Certified Public Accountants

I. INDEPENDENT SERVICE AUDITOR'S REPORT

To: Management of Liquid Web, LLC:

We have examined Management's assertion that during the period July 1, 2016 through June 30, 2017, Liquid Web, LLC maintained effective controls over the co-location, web hosting, and network infrastructure services and supporting systems that:

- The systems were protected against unauthorized access (both physical and logical)
- The systems were available for operation and use, as committed or agreed

Based on the AICPA's TSP Section 100, *Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Liquid Web, LLC's management is responsible for this assertion. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and included (1) obtaining an understanding of Liquid Web, LLC's relevant controls over the availability and security of the co-location, web hosting, and network infrastructure services and supporting systems; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Inherent limitations
Because of their nature and inherent limitations of controls, Liquid Web, LLC's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct error or fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. The projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Opinion
In our opinion, management's assertion referred to above is fairly stated, in all material respects, based on the AICPA and CICA trust services security and availability criteria.

UHY LLP

Farmington Hills, Michigan
September 25, 2017

II. MANAGEMENT'S ASSERTION

Liquid Web, LLC Assertion:

The management of Liquid Web, LLC maintained effective controls over the security and availability of their co-location, web hosting, and network infrastructure services system to provide reasonable assurance that the system was:

- Protected against unauthorized access (both physical and logical)
- Available for operation and use, as committed or agreed

throughout the period July 1, 2016 to June 30, 2017 based on the criteria for security and availability in the American Institute of Certified Public Accountants TSP Section 100, *Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Our attached system description identifies the aspects of the system covered by our assertion.

The description contains the following information:

i) The types of services provided.

ii) The components of the system used to provide the services, which are as follows:

(1) *Infrastructure.* The physical structures, IT and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).

(2) *Software.* The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).

(3) *People.* The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).

(4) *Processes.* The automated and manual procedures.

(5) *Data.* Transaction streams, files, databases, tables, and output used or processed by a system.

iii) The boundaries or aspects of the system covered by the description.

iv) Any applicable trust services criteria that are not addressed by a control and the reasons.

v) Relevant details of changes to the service organization's system during the period covered by the description

The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that each individual report user may consider important to its own particular needs.

The controls stated in the description were suitably designed and operated effectively throughout the period July 1, 2016 to June 30, 2017 to meet the applicable trust services criteria.

III. DESCRIPTION OF THE LIQUID WEB SYSTEM USED TO MANAGE AND CONTROL CO-LOCATION, WEB HOSTING, AND NETWORK INFRASTRUCTURE SERVICES

Organization Background

Liquid Web, LLC ("Liquid Web") was founded in 1997 as a privately held managed co-location, web hosting, and network and infrastructure services company and was acquired in 2015 by the private equity firm Madison Dearborn Partners. Liquid Web has five data center facilities, three located in Lansing, Michigan, one located in Phoenix, Arizona, and one in Amsterdam. Liquid Web is a leader in the professional web hosting market with an unwavering dedication to providing the best hosting products available. Liquid Web has over 30,000 clients served in over 150 countries.

Scope of the Report

The scope of the report is limited to Liquid Web's co-location, web hosting, and network infrastructure services at its three data center locations in Lansing, Michigan, its data center in Phoenix, Arizona, and its data center in Amsterdam, Netherlands. This report covers the Liquid Web's services described below and the suitability of the design of controls to meet the criteria for the Security and Availability principles set forth in TSP section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Liquid Web utilizes a third-party data centers for physical security, internet connection, and environmental controls for the Phoenix, Arizona, and Amsterdam, Netherlands data centers. This report does not cover the physical security and environmental controls at those locations. Both the Phoenix and Netherlands data centers provide AICPA SOC Type 2 reports to Liquid Web which cover the physical and environmental controls for their sites.

Service Offerings Provided

Hosting Services

- Dedicated web hosting - Private servers wholly allocated to the customer and fully managed by Liquid Web.
- Shared web hosting - Dedicated or virtual servers shared between multiple customers.
- Virtual private servers - Dedicated virtual servers
- Colo - Ability to collocate equipment in Liquid web owned data centers.

Network Services

- Load Balancing (Dedicated Load Balancers with Active/Active Redundancy)
- Managed File Replication Services
- Redundant Firewalls I Automatic Failover
- Virtual Private Network (VPN)
- Unmetered Bandwidth Solutions
- Content Delivery Network (CDN)

Backup/Storage Solutions

- Guardian Continuous Data Protection
- Storage Area Network (SAN)
- Terabyte Backup
- Dedicated Server Service Level Agreement (SLA)

Components of the Liquid Web System

Infrastructure

Liquid Web data centers are designed with redundancy installed at every level, ensuring that a failure at any level will not affect customer servers. Liquid Web data center power is conditioned and reliable through the use of centralized Uninterruptible Power Supplies (UPS) solutions backed by generators. Data centers exclusively utilize premium Tier-1 bandwidth providers, ensuring minimal latency and fast connections to all points of the global internet.

The physical machines that provide hosting services for clients may be either dedicated (private servers wholly allocated to the customer) or virtual (share services between several customers). In addition, redundant network firewalls, routers and servers are installed to ensure network equipment failures do not impact customers' availability to their servers.

The Liquid Web network has been designed to accommodate clients demanding the highest quality network performance. There is a central focus on redundancy allowing our network to rapidly self-heal failures without interruptions to connectivity. Our redundancy is multi-tiered with N+1 internal device elements as well as entirely redundant chassis allowing any routing device to fail without interrupting client data connectivity. All core routing and switching equipment is state of the art Cisco.

Software

The following systems comprise of the co-location, web hosting, and network infrastructure services system:

- Identity Management System for Network and VPN access
- Wordpress for content management
- Security monitoring software including a portfolio of network and system security tools and applications
- Availability monitoring software including a robust set of proprietary system level health and service monitoring tools

People

Liquid Web has organized the company into following distinct operating units which are listed below and further defined in the Organizational Structure section below:

- Executive Management
- Heroic Support® Team
- Platform Team
- Security Team
- Advance Services Team
- Sonar Monitoring™ Team
- Systems Restore Team

Processes and Procedures

Liquid Web's policies and controls cover all critical aspects of employment, including hiring, training and development, performance appraisals, and terminations. In addition, all employees have access to an employee handbook, policies, and procedures which define appropriate ethical behavior. Changes to these documents are communicated to existing personnel in writing.

A sanction policy exists within the Acceptable Use Policy, which includes workforce conduct standards regarding acceptable use of Liquid Web's resources. A performance review is performed and documented by each department head on an annual basis.

Data

Liquid Web does not manage, access, transfer, or move client data or content.

Audit Logs and System Log Files - Liquid Web system and network user activity, system activity, and systems diagnostics are captured in audit logs and system logs that are retained within the system and/or forwarded to monitoring and reporting tools for analysis.

The Aspects of the System and Description of its Boundaries

Liquid Web provides a wide array of services to customers including co-location, web hosting, and network and infrastructure services, included below are the primary responsibilities of Liquid Web and customers.

Co-location Services

Co-location services provide space for customer equipment. Liquid Web provides power, cooling, physical security, and a public networking connection to the equipment. The customer is responsible for configuration and troubleshooting any equipment software or hardware issues.

Web Hosting Services

Web Hosting services consist of servers, switches, and firewalls based on managed services purchased. Liquid Web is responsible for all hardware and operating system support and provides physical security to the equipment. The customer is responsible for the software support, configuration and data. Liquid web will configure the systems as requested and make changes as requested by the customer.

Network and Infrastructure Services

Liquid Web provides initial configuration of software, hardware and network at customer request. Liquid Web additionally provides ongoing changes and support at customer request. Customer is responsible for ensuring the configurations and changes requested are fit for purpose and meet customer's specific compliance and performance requirements.

Description of Liquid Web Control Activities and Processes Control Environment

Oversight Responsibility

Roles and responsibilities among the various departments within Liquid Web are documented and provided to employees, which are maintained by each respective department. Additionally, reporting lines are documented within each job description. Department heads are responsible for documenting policies and procedures including job descriptions. The Chief Architect oversees the Security Team, which are responsible for the Liquid Web security and availability policies and procedures.

The oversight of the day-to-day operations of the Company is under the direction of the CEO and the Executive Management Team consisting of the various heads of functional departments. The Management Team meets on a weekly basis to review the results of operations, discuss unusual activity or events, review key metrics and financial results, and discuss other matters important to the operation of the Company.

In addition, the Executive Management Team is responsible for:

- Reviewing the professional services to be provided by Liquid Web's independent auditors and the independence of such auditors;
- Reviewing the scope and results of all audits - internal and external; and
- Reviewing the system of internal controls and other matters relating to Liquid Web's co-location, web hosting, and network and infrastructure services.

Organizational Structure

Executive Management: The Executive Management team is responsible for monitoring trends in the hosting services industry and identifying risks internally and externally. Executive management constantly considers new technology trends, risks, and opportunities as well as the impact of any applicable regulation or legislation on the security or availability of services provided by Liquid Web. Executive Management is responsible for implementing appropriate measures to monitor and manage these risks. Appropriate measures may include the addition or revision of control procedures, conducting specific investigations, or any other means necessary to provide adequate control.

Heroic Support® Team: Liquid Web has established a 24/7/365 Heroic Support® team that is professionally educated and available on-site at each data center 24 hours per day. Liquid Web currently employs 320+ Heroic Support® engineers with specialties in Technical Support, Service Delivery, Networking, Security and more.

Platform Team: The Platform Team consist of the network team - engineers, security team - engineers, and compliance and purchasing teams is following the NIST Feed, US Cert Feed, and facilities would track the weather with an on call rotation if there is severe weather. An email notification would be sent out if there is something that needs to be documented as far as regulatory or environmental trends.

Security Team: The Security Team continuously monitors the entire Liquid Web network for possible intrusions and attacks. The team investigates any issues and takes appropriate action. Real-time monitoring activity is presented in dashboards. The network monitoring dashboard graphic displays potential attack signature messages detected by perimeter firewalls and reports the activity back to the Security team.

Advance Services Team: The Advanced Services team is responsible for the service delivery, system restores, training and monitoring.

Sonar Monitoring™ Team: The Sonar Monitoring™ team utilizes a robust set of proprietary system level health and service monitoring tools to constantly ensure server's optimal performance through early detection of problems. In the event that an issue is identified, our Sonar Monitoring™ Team responds immediately, reducing downtime and repairing any issues proactively, in many cases before the client is even aware of the problem. Server failure monitoring, disk space monitoring, load monitoring, and memory available monitoring is performed by the Monitoring Team. Alerts are tracked to resolution within the ticketing system.

Systems Restore Team: The system restore team is responsible for the restoring failed systems for customer with the defined SLA's and relies on alerts from the monitoring team. The System Setup team configures the hardware and deploys customer devices into the datacenter as requested. The training team handles all aspects of training for Liquid web, including technical, security, and compliance related training.

Commitment to Competence and Accountability

Executive Management is ultimately responsible for the development and maintenance of policies and procedures. Individual department heads are responsible for maintaining and updating policies for their departments. These policies and procedures have been implemented to ensure consistent and effective security and availability over Liquid Web's hosting services.

Hiring procedures include a comprehensive screening of candidate's qualifications and experience to ensure they have the qualifications to fulfill their job responsibilities. Hiring procedures also include background and reference checks for employees prior to hire.

New hires sign an acknowledgement upon hire to acknowledge they will abide by the information security policies. Information Security training covers the communication of roles and responsibilities in terms of support and boundaries of the system for internal users. Employees are required to attend security awareness training on an annual basis. New hire training reviews the terms of services agreements. Training documentation as well as new employee orientation training materials are available on the company Internal Wiki for those employees whose roles affect system operation.

A performance review is performed and documented by each department head on an annual basis.

Risk Assessment Process

Liquid Web recognizes that risk management is a critical component of its operation that helps ensure that assets are properly managed and clients are properly served. Through regular and open communication among staff, management, and its client base, Liquid Web identifies risks that could negatively impact the security of the business. For any significant risks that are identified and communicated, Executive Management is responsible for implementing appropriate measures to monitor and manage these risks. Appropriate measures may include the addition or revision of control procedures, conducting specific investigations, or any other means necessary to provide adequate control. The risk assessment policy outlines the requirements for the risk assessment including the requirement to evaluate the mitigating controls for each threat and vulnerability.

A written policy is available on the company intranet that defines the requirements and provides the authority for the Network and Security Teams to identify, assess, and remediate risks to Liquid web's information infrastructure associated with conducting business.

Information and Communication Systems

Internal User Communication

Liquid Web's system security and availability and related security commitments are communicated via a posting on the Liquid Web's Internal Wiki. All company policies, including security and availability policies are available to all associates via the Liquid Web Internal Wiki.

Internal Planned upgrades and changes that are part of normal project management are communicated via weekly department head meetings as well as intercompany email.

External User Communication

Each Liquid Web service offering has established appropriate terms of service which outline the services and associated boundaries for external users.

Security and availability commitments made to external users are communicated within the Terms of Service, which is provided to external users upon onboarding

Monitoring

Management and supervisory personnel are responsible for monitoring the quality of internal control performance as a routine part of their daily duties. To assist them, Liquid Web utilizes a series of management reports and other methods to monitor the business. Key reports are reviewed by management to help ensure appropriate action is taken as needed. If issues arise that cannot be readily resolved, issues are escalated to Executive Management.

The Liquid Web's Management Team monitors the company's services providers and their ability to meet the company's requirements related to security and availability. Liquid Web obtains and reviews applicable Service Organization Reports for subservice providers that provide services significant to the co-location, web hosting, and network and infrastructure services annually to ensure subservice providers are maintaining appropriate controls.

Liquid Web Sonar Monitoring™

Sonar Monitoring™ is a dedicated division of Liquid Web solely focused on providing service reliability and immediate incident resolution. The Sonar Monitoring TM team utilizes a robust set of proprietary system level health and service monitoring tools to constantly ensure your server's optimal performance through early detection of problems. In the event that an issue is identified, our Sonar Monitoring TM Team responds immediately, reducing downtime and repairing any issues proactively, in many cases before the client is even aware of the problem.

The Sonar Monitoring TM team focuses on prevention of, as well as immediate response to, service interruptions, whether they be software, hardware or network-related. With the bulk of service failures being prevented before occurrence, and nearly all remaining service failures being corrected within minutes, the team operates as a persistent proactive manager of client service consistency. The Liquid Web Sonar Monitoring TM Team has enabled us to provide the industry's leading 30-minute hardware replacement SLA.

The entire network is constantly monitored using a custom developed real time network monitoring and alerting system by the Sonar Monitoring™ Team. The Network and Security Teams utilize proprietary and commercially available tools on a regular basis to evaluate compliance with policy, SLAs, and industry best practices. Real time monitoring, which includes monitors on the walls, and each tech has a side bar that shows approaching SLAs. Liquid Web uses an issue tracking system to record and monitor security and availability issues through resolution. Any unusual or suspicious network activity is highlighted and forwarded to network administrators for investigation and resolution.

Michigan Data Center Features

Liquid Web's data center locations are staffed by highly skilled engineers around the clock. Liquid Web data centers are designed with redundancy installed at every level, ensuring that a failure at any level will not affect customer servers. Liquid Web data center power is conditioned and reliable through the use of centralized Uninterruptible Power Supplies (UPS) solutions backed by state-of-the-art generator technology. Liquid Web's network is robust and reliable. Data centers exclusively utilize premium Tier-1 bandwidth providers, ensuring minimal latency and fast connections to all points of the global internet. Additionally, data centers are equipped with equipment racks, smoke and fire detection, fire suppression, dedicated air conditioning, alarm map with hot spots, and humidity monitoring. The UPS and generators are tested annually.

Physical Security

Physical access to the building and data center is monitored by live, real-time via recorded video surveillance via premise security guard and Infrastructure team personnel. Electronic security systems control data center access and are accompanied by a full complement of motion detecting security cameras, which monitor the entire facility.

Physical access to the building and data center area is controlled via card key systems. Liquid Web restricts data center access to technical staff only. Daily, a log of employees who have accessed the data center is sent to select managers via email for review to ensure only appropriate persons are access the data center.

Access to telecom and central switching equipment is restricted via key locked closets. Data center facility external walls are reinforced poured concrete. Level 3 technicians are on site 24 hours per day, keeping incident response times to a minimum.

All data center visitors are required to register and wear a visitor badge at all times. All visitors are escorted by a Liquid Web associate at all times while on site. Additionally, visitor profiles are visible via the building monitor so employees are aware of the visitors currently in the building.

The Infrastructure Team performs a monthly review of unused badges, failed badge access attempts, deleted and added badges, and changes to badge access.

Power Systems

Our power systems feature extensive fault tolerance and resilience at every layer. Incoming service is routed underground to a dedicated on-site transformer. This system routes to our automatic transfer switch which monitors power quality, and automatically transfers to our emergency generators in the event they are needed. Each facility is also protected by one or more Uninterruptible Power Supplies (UPS), featuring redundant battery cabinets, and full maintenance bypass cabinets allowing for service and upgrades without interruption of power to our servers.

Power distribution units handle final power transformation and distribution to racks, ensuring clean consistent power to data center equipment.

Each facility has multiple emergency generators waiting on standby, featuring over 24 hours of autonomous runtime before requiring refueling. Generator power is activated automatically in the event of a utility failure by the transfer switch. The data center load is maintained by the UPS units with at least 15 minutes of capacity, however this is not necessary as the generator is active and up to speed within 1O seconds of a power failure.

Cooling

Environmental processing systems include one 45 ton Liebert down-flow air conditioners and a mixture of Liebert up flow air conditioning units ranging in sizes of 20, 22, 24, and 30 tons. Temperature and humidity are precisely monitored and regulated year round to ensure optimal equipment reliability. Alerts are sent to Operations personnel any time temperature or humidity is outside an established range. Each unit contains independent compressors and cooling loops to further enhance fault tolerance and reliability. Air filtration systems actively remove foreign particulates from circulation and cycle the entire data center air supply in a matter of minutes.

Environmental

The following environmental controls are present in the data center:

- Equipment kept on elevated racks in data center
- Smoke and fire detection system
- Fire suppression system
- Dedicated NC
- Alarm map with hot spots
- Humidity monitoring
- UPS
- Generator

Weather monitors are mounted on the walls throughout the facility to monitor for severe weather. Additionally, the Facilities Team monitors the weather for natural disaster preparedness.

Phoenix Data Center Features

Liquid Web utilizes, PhoenixNap to host the Liquid Web environment in the Southwest region of America. The data center includes physical and environmental controls such as HVAC, Electrical and physical security including access to areas. Any changes to the environment or physical controls are done via a ticketing system with PhoenixNap. Liquid Web has access to their environment via on-site employees of LiquidWeb, physical access via on-site Liquidweb employees. The data center provides Liquid Web a SOC 1 SOC 2, PCI, etc. that Liquid Web reviews to ensure the physical security and environmental controls outlined above are in place and operating effectively.

The physical security and environmental controls of PhoenixNAP are managed by the service provider and not included in the scope of this report.

Amsterdam Data Center Features

Liquid Web utilizes, EvoSwitch to host the Liquid Web environment in the Country of Netherlands. The data center includes physical and environmental controls such as HVAC, Electrical and physical security including access to areas. Any changes to the environment or physical controls are done via a ticketing system with EvoSwitch. Liquid Web has access to their environment via IPMI and physical access via the EvoSwitch staff. The data center provides Liquid Web a SOC 1 SOC 2, PCI, etc. that Liquid Web reviews to ensure the physical security and environmental controls outlined above are in place and operating effectively.

The physical security and environmental controls of EvoSwitch are managed by the service provider and not included in the scope of this report.

Network Security

Network authentication is controlled via redundant RADIUS servers controlled exclusively by the network administration group. Each encryption key for RADIUS servers is unique to that device. No shared encryption keys are utilized.

Corporate policy dictates that all changes to internal network equipment must be peer reviewed prior to implementation, except emergency changes which are peer reviewed after implementation.

The entire network is monitored in real-time using a custom developed real time network monitoring and alerting system. Any unusual or suspicious network activity is highlighted and forwarded to network administrators for investigation and resolution. Firewalls are in place to protect the internal Liquid Web network. Firewall and network device configuration log files are monitored and reviewed on a daily basis. Administrator access to the firewall is restricted to members of the Network Engineering Team. An IPS (Tenable) is in place and sends alerts to Security personnel for high and critical severity vulnerabilities. Administrator access to the IDS was restricted to authorized Security personnel

Quarterly internal vulnerability assessments and external network assessments are conducted. Remediation efforts of issues found are documented by IT management

Eset Antivirus software is installed on all windows workstations and servers in the company. Antivirus is configured to update every 60 minutes and to run a weekly scan. Antivirus software is not installed on Macintosh and Linux devices.

Logical Security

New users and employees added to the Liquid Web network are requested by Human Resources/employee's manager to the Office IT department, where the account is created. The Office IT department will assign them to an LDAP group profile based on their department. Modifications to user access are requested by the new Department Head and granted by the Office IT department. Current roles would be reviewed at this time and modifications in the group access are updated as necessary. Modifications in access found during the review are sent to Office IT by the Department Heads. Terminated employees are communicated from Human Resources to the Office IT department where access is disabled. Access is disabled within one business day of termination. A user access reviews is performed annually by the Department Heads.

All authorized users of Liquid Web Network are identified and authenticated via a unique user-id and password, and two factor authentication using IDM. Network and application User IDs are unique and passwords are not stored in plain text. Password parameters for IDM are as follows:

- Maximum Age: 90 days
- Password History: 4 Passwords
- Complexity: Number, Letter, and Special Character required
- Minimum Length: 8 Characters
- Lockout Threshold: 6 attempts
- Lockout Duration: 10 minutes

In order to authenticate to the Permissions application, users must first authenticate through IDM. Passwords for permissions are as follows

- Minimum Length: 7 Characters
- Complexity: Password must contain at least three out four classes (Upper case, Lower case, Number, or special characters.)

Remote access to the Liquid Web network is highly controlled via Virtual Private Network (VPN) requiring two factor authentication supplied by an RSA token.

Change Management

Corporate policy dictates that all changes to internal network equipment must be peer reviewed prior to implementation, except emergency changes which are peer reviewed after implementation. Changes to customer servers must be requested by the customer with their approval obtained prior to initiating the change request. All changes that would impact customer service must go through a defined change procedure, which includes testing and code review of changes prior to implementation. Maintenance windows exist for customers and Liquid Web will provide a notification on the change, including required patch updates. Changes to the code base trigger a notification to the development department. Any code changes pushed without prior notification by the Development T earn would be followed up on by the Team Leads for investigation. Liquid Web utilizes a comprehensive issue tracking and help desk system which provides for the review and approval of emergency changes, which is included within the normal changes. When possible emergency changes are tested prior to implementation, otherwise testing is performed after implementation.

Backup and Recovery

A weekly review of Liquid Web internal system and infrastructure configuration backup jobs is performed by management to ensure that all scheduled internal systems and infrastructure backups were successfully performed.

Backup data for Liquid Web internal systems and infrastructure are maintained at an alternate Liquid Web datacenter. Access to backup data is restricted to authorized employees.

Annually, Liquid Web performs a tabletop test of system redundancy to ensure the system remains available to customers.