CU Solutions Group, Incorporated

For the Period
January 1, 2016
through
December 31, 2016

SOC 3 Report

Report on Controls at a Service Organization Relevant to Security, Availability, Confidentiality and Processing Integrity

Rehmann
Business wisdom delivered.

CU SOLUTIONS GROUP, INCORPORATED
CREDIT UNION WEB SOLUTIONS SERVICES SYSTEM

TABLE OF CONTENTS **PAGE**

Rehmann

Rehmann Robson

7124 Central Ave.
Toledo, OH 43617
P: 419.865.8118
F: 419.865.3764
rehmann.com

I. INDEPENDENT SERVICE AUDITORS' REPORT

Board of Directors
CU Solutions Group, Incorporated
Livonia, Michigan

Scope

We have examined CU Solutions Group, Incorporated ("CUSG") management assertion that, during the period January 1, 2016 to December 31, 2016, it maintained effective controls to provide reasonable assurance that the criteria for the security, availability, processing integrity, and confidentiality principles set forth in the American Institute of Certified Public Accountants' ("AICPA") TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*) ("applicable trust services criteria") were met throughout the period January 1, 2016 to December 31, 2016.

Service Organization's Responsibilities

In Section II, CUSG has provided its assertion titled "CU Solutions Group, Incorporated's Management Assertion" regarding its Credit Union Web Solutions Services System for the period January 1, 2016 to December 31, 2016, (the "assertion") about the fairness of the presentation of the description based on the description criteria and suitability of design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. CUSG is responsible for preparing the description and the assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; identifying the risks that would prevent the applicable trust services criteria from being met; designing, implementing, and documenting the controls to meet the applicable trust services criteria; and specifying the controls that meet the applicable trust services criteria and stating them in the description.

Independent Service Auditors' Responsibilities

Our responsibility is to express an opinion on the assertion based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA and, accordingly, included (1) obtaining an understanding of CUSG's relevant security, availability, processing integrity, and confidentiality controls, (2) testing and evaluating the operating effectiveness of the controls and (3) performing such procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Inherent Limitations

Because of the nature and inherent limitations of controls, CUSG's ability to meet the aforementioned criteria may be affected. For example, fraud, unauthorized access to systems and information, and failure to comply with internal and external policies or requirements may not be prevented or detected. Also, the projection of any conclusions, based on our findings, to future periods is subject to the risk that any changes or future events may alter the validity of such conclusions.

Opinion

In our opinion, CUSG's management assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability, processing integrity, and confidentiality.

March 29, 2017

Rehmann Robson LLC

II. CU SOLUTIONS GROUP, INCORPORATED'S MANAGEMENT ASSERTION

We have prepared the description in Section III, titled "Description of CU Solutions Group, Incorporated's Credit Union Web Solutions Services System for the Period January 1, 2016 through December 31, 2016" (the "description"), based on the criteria for a description of a service organization's system identified in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (the "description criteria"). The description is intended to provide users with information about the Credit Union Web Solutions Services System, particularly system controls intended to meet the criteria for the security, availability, processing integrity, and confidentiality principles set forth in TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (*AICPA*, Trust Services Principles and Criteria)* ("applicable trust services criteria").

We confirm, to the best of our knowledge and belief, that CU Solutions Group, Incorporated maintained effective controls over the security, availability, processing integrity, and confidentiality of its Credit Union Web Solutions Services System ("System") to provide reasonable assurance that:

- the System was protected against unauthorized access, use or modification; and
- the System was available for operation and use, as committed or agreed; and
- the System processing was complete, valid, accurate, timely, and authorized; and
- the System information designated as confidential was protected as committed or agreed

Timmy Bohlman
Senior Vice President of Marketing and Technology Solutions
CU Solutions Group, Incorporated

March 23, 2017

III. DESCRIPTION OF CU SOLUTIONS GROUP, INCORPORATED'S CREDIT UNION WEB SOLUTIONS SERVICES SYSTEM FOR THE PERIOD JANUARY 1, 2016 TO DECEMBER 31, 2016

BACKGROUND

CU Solutions Group, Incorporated ("CUSG"), headquartered in Livonia, Michigan, is a leading provider of web sites, consulting, custom solutions, and e-business services to Credit Union System organizations; helping them leverage technology to better serve their members and customers. CUSG predominantly utilizes Linux based technology to provide customers with cost effective web solutions. The company started in 1996 as a division of CU Corp. In July 2000, it was incorporated as a credit union service organization company owned by credit unions, credit union leagues, and credit union service organizations around the country. CUSG employs competent and qualified professionals to provide exceptional service to its customers.

CUSG's technologies include Web Hosting solutions through various Web based applications written and purchased by CUSG. These include the Content Management System ("CMS"), Event Management System ("EMS"), Performance Pro 3 ("PP3"), and other applications written by CUSG Technology Solutions staff. These applications are delivered through a dedicated information technology hosting platform at a data center, Secure-24, LLC ("Secure-24"). The subservice organization has a Service Organization Controls ("SOC") Type II examination. This description excludes the security, availability, processing integrity, and confidentiality controls of Secure-24.

The examination covers both CUSG internal network systems and CUSG dedicated Web Hosting systems security, availability, processing integrity and confidentiality controls. The systems are comprised of the following components:

- Software
- Data
- Infrastructure
- People
- Procedures

These five components comprising the Credit Union Web Solutions Services System are described below:

SOFTWARE

CUSG has a highly skilled team of Web developers that are proficient in producing sophisticated and modern web products using technologies such as XML, JavaScript, AJAX, PHP, Linux, MySQL, and Microsoft Tools. CUSG develops web based applications for presentment of customer web sites and customer data where applicable.

DATA

Client data received and/or maintained by CUSG is safeguarded and protected, regardless of the type of data, at all times. This protection includes:

- Restricting access to only designated database personnel
- Maintaining the data on secure servers located in a secured server room.

The secured server room is environmentally protected by an Uninterrupted Power Supply, emergency lighting, hand held fire extinguishers, HVAC, a natural gas powered Cummins power generator and fire alarm monitoring systems. Electronic access control devices restrict access to the facility.

Any data that the customer has not requested CUSG to retain is electronically deleted and e-shredded after its intended use.

INFRASTRUCTURE

Server Room Environment and Power Management

The servers and overall core network infrastructures are located in a secured room in the Corporate suite and the door remains card locked at all times. The servers, network and telecommunications equipment are stored in secured freestanding racks and mounted cabinets in the server room. Copies of user and system software, spare parts and tools for computer and telecommunications equipment are stored in a different card secured room, or the IT office, which is key locked. The server room does not house the CUSG production servers or network equipment. Card access to the server room and key access to the IT office is available only to the Director of Information Technology ("DIT"), Senior Vice President of Marketing & Technology Solutions ("SVPMT"), Manager of Information Technology ("MIT"), IT Systems Analyst ("ITSA"), Technology Support Specialists ("TSS"), SharePoint Administrator, and the Manager of Building Services.

CUSG's electric utility has sub-stations throughout the region. Uninterruptible Power Supply ("UPS") units filter the power to the computers and telecommunications equipment to prevent damage from power fluctuations. The UPS units provide 20 to 30 minutes of stored power in the event of an outage. The MIT regularly has the UPS system perform a self-test and generate an email with the results of the test. Appropriate follow-up procedures are taken if necessary.

A natural gas fueled generator is installed on the roof of the corporate office. In the event of a power failure the generator is able to carry the power load of the full server room, including lights, air conditioning and the card access security system. The generator will continue to carry the power load until 15 minutes of uninterrupted power is detected from the electric utility. The generator is under a routine maintenance contract and the system runs weekly self-tests.

A fire alarm system is in place to monitor for fire and notify the alarm company if a fire is detected. Water sprinkler systems protect the server room from fire damage. In addition, hand-held fire extinguishers are clearly labeled and available in the server room. Fire alarms and extinguishers are tested at least annually. The Corporate office heating and cooling system controls temperature and humidity variations in the office. The server room has a separate HVAC system to maintain a proper operating environment. The server room HVAC has preventative maintenance performed at least semi-annually. Also, the UPS unit provides live monitoring of temperature and humidity status in the server room.

Servers

Physical servers include a variety of Dell and HP devices, as well as Cisco switches, firewalls, and other devices that support the operations of the entire organization. The servers run a Windows Server 2005/2008/2010, Linux RHEL 6, and Cisco proprietary iOS. Systems run redundant array of independent disks, dual GB NICs, Quad core processors, and redundant power supplies, unless these features are not available by vendor supplied hardware for systems run by IT.

Internet Connectivity

Internet connectivity in the Corporate office is currently a 50MB fiber line provided by a nationwide Tier 1 Internet Provider, with the capacity to upgrade bandwidth as required. The Tier 1 Internet Provider guarantees 99.9% uptime, which CUSG uses for internal operations by employees. In the event of a failure, the Tier 1 Internet Provider guarantees repair within four hours of failure. CUSG's facilities and equipment have the necessary bandwidth to accommodate all expected bandwidth requirements of the employees.

Internet connectivity in the Secure-24 Hosted environment is currently multiple GIG-E, OC192, and OC48 from multiple Tier 1 Providers, with the capacity to upgrade bandwidth as required. The Tier 1 Internet Providers guarantees 99.9% uptime, which CUSG passes through to its customers through the Secure-24 network.

Network Security

CUSG network security at the Corporate office deploys the latest technologies to support staff activities securely and protect all information stored on the Corporate network. CUSG Corporate office employs the following technologies:

- Security - a Cisco ASA Firewall with Intrusion Prevention and a stand-by unit with a copy of the current running configuration - protecting the network from unauthorized access and filtering all inbound and outbound Corporate traffic through the Internet. Changes to the firewalls are logged as support cases and these are reviewed monthly. The devices are also patched according to manufacturer's security standards.
- Communication - Multiprotocol Label Switching ("MPLS") connectivity between the Corporate office and satellite offices for secure transmission of corporate information.
- Email Security Services - Email is hosted with Microsoft 365 services. Email security including filtering spam, viruses, phishing, denial of service attacks ("DoS"), harvesting, and other attacks are handled through Microsoft online services.
- Virtual Private Network ("VPN") access - VPN access for Corporate employees is attained through the Corporate firewall, deploying strong encryption standards. VPN access is controlled through RADIUS directly associated with a network Active Directory ("AD") group.
- Encryption - areas of the organization where sensitive customer data is stored uses PGP encryption to store aforementioned data. PGP keys are centrally administered for encrypted data.

CUSG network security at the Secure-24 Hosting facility uses the latest technologies to secure customer data and information passed across the Internet. CUSG and Secure-24 employ the following technologies:

- Multi-tenant Juniper firewalls with a virtual firewall instance running AppSecure inspection
- Multi-tenant Radware implementation with standard profile for Denial of Service (DoS) protection
- Multi-tenant Cisco Nexus Ethernet switches with VLAN separation between customers
- Multi-tenant central logging/reporting for basic operating system ("OS"), database, network, etc.
- Secure administrative environment (Jump stations & management universe)
- Dedicated Secure Sockets Layer ("SSL") VPN virtual appliance(s)
- Two Factor Authentication for VPN access
- Secure-24 host level anti-virus solutions
- Email Security Services - filters spam, viruses, phishing, DoS, harvest attacks, and other attacks.
- SSL Encryption and Authentication - Web applications utilize SSL encryption and authentication, as well as automatic timeout logoff
- Encryption - areas of the hosted solution where sensitive customer data is stored uses PGP encryption to store aforementioned data.
- Access - Root access to systems are limited to approved staff identified by the SVPMT, and access is limited to super user do ("sudo") rights, which allow users to execute certain commands that the super user normally performs.

System Back-ups

Backups in the Corporate Office are performed daily to disk and then to a third-party off-site cloud vendor. In the event of a localized server failure, the system(s) will be restored within 24 hours in conjunction with vendor service level agreements. In the event of a catastrophic failure, systems will be restored within four days at an alternate satellite office using off-site backups from the third-party vendor. CUSG has a disaster recovery plan that is reviewed and updated annually.

Access to Facilities

For general access to the Corporate offices, all external entrances require key access, which is limited to Corporate staff and building management team members. Card access for Corporate staff to the Corporate office is required on all external doors and entrances. During business hours from 8:55 AM to 5:00 PM from Monday through Friday, the front entrance is unlocked and a receptionist monitors the front entrance for visitors and requires visitors to sign-in on an Entry Log. Visitors are escorted by an authorized company employee or company officer to designated areas.

PEOPLE

CUSG Technology Solutions is supported by the following key functional staff:

Senior Vice President of Marketing & Technology Solutions – The SVPMT oversees all operations of the Technology Solutions area, and monitors security and change controls. The SVPMT is responsible for the overall infrastructure of Corporate office technology and the Secure-24 hosting environment. The SVPMT ensures that all policies and procedures are in place, and audits all operations of the Technology Solutions area, reporting results to the Security Team.

Director of Information Technology – The DIT is responsible for internal technology planning, implementation and oversight. The DIT manages the internal IT team and provides support as needed to the SVPMT.

Manager of Information Technology – The MIT is responsible for the daily operations of the Corporate office information technology infrastructure. The MIT reports on controls on a monthly basis to the SVPMT as a part of the overall change and security control process.

Manager of Software Development – The Manager of Software Development ("MSD") assists the SVPMT in the daily operations of the Secure-24 hosting environment. The MSD has sudo accounts to the Secure-24 server, and access to Secure-24 engineering services.

Senior Application Developer – Senior Application Developers ("SAD") assist the SVPMT and the MSD in the daily operations of the Secure-24 hosting environment. The SADs have sudo accounts to the Secure-24 server, and access to Secure-24 engineering services.

Technology Support Specialist – The TSS is responsible for supporting the MIT in daily operations, including Corporate office network user management, Corporate email changes, general Corporate technology troubleshooting, and Corporate backups.

Application Developers – Application Developers perform application programming changes to the CUSG Web Hosting environment. They perform application code updates and changes, and perform change control activities around these functions.

Web Developers – Web Developers are responsible for daily support of CUSG Web Hosting customers. They perform basic changes to customer hosted files, email support, and general troubleshooting. They perform change control activities around updates they perform for customers.

PROCEDURES

CUSG has documented policies and procedures that support the management, operations, monitoring and controls over Corporate IT and Secure-24 hosting environment. Specific examples of relevant policies and procedures include, but are limited to, the following:

- Technology and Security Policies
- Technology Solutions Policies
- Risk Assessment
- Incident Response Policy
- Change Management Policy & Procedures

OTHER ASPECTS OF CUSG'S CONTROLS

CONTROL ENVIRONMENT

Organization and Management

CUSG's control environment is the responsibility of its Executive Management as they oversee the management of their respective departments. They ensure that each department's control activities, policies, standards and procedures reflect positively on the organizational missions and customer service.

Management Philosophy and Operating Style

CUSG's mission is to provide web based technology solutions for organizations nationwide. CUSG will deliver operational excellence in all divisions of the company and meet or exceed our commitments to the many constituencies we serve. Executive Management has an open door to customers and employees at all times and their direct contact information is openly communicated to ensure immediate escalation occurs. This enables Executive Management to participate in organizational controls. An operational emphasis is placed on timely and accurate responses and customer service is emphasized with a commitment to exceeding customer's expectations and building a team environment that includes employees, vendors, customers and contractors.

Assignment of Authority and Responsibility

CUSG's Executive Management includes the Chief Executive Officer ("CEO"), Chief Operating Officer ("COO") and its Board of Directors. They have ultimate responsibility for all activities within CUSG, including the internal controls which are executed by the SVPMT. This includes the assignment of authority and responsibility for operation activities, and establishment of reporting relationships and authorization protocols.

Organizational Structure

Management has a clearly defined organizational chart and staff job descriptions to ensure the functions and reporting relationships are understood.

Training

CUSG provides training on its hi-tech equipment and computer applications primarily via on-the-job-training ("OJT"). New production employees are hired with the basic skill sets necessary for their respective job assignments. Additional training is normally accomplished via OJT. When new equipment or applications are introduced into the company, either an instructor for the new equipment conducts training locally or, in some cases, a cadre of personnel is sent to the vendor's location to receive the technical training. Additional training and certifications are provided to employees through online training.

Hiring Practices and Human Resource Policies

CUSG hires skilled staff with the necessary qualifications to perform the required duties. Criminal background checks and reference checks are performed prior to hiring. Candidates are also required to pass a pre-employment drug test. In order to ensure that the necessary skill sets are maintained, budget is allocated annually to provide training for staff. Written performance evaluations are performed annually to provide employees with an evaluation of their performance and to provide performance improvement feedback.

Each new employee is put through a formal orientation. The orientation process carefully reviews the Personnel Policy Manual, offers an organizational overview, a tour of the building and discusses a range of procedures and job requirements. Detailed policies pertaining to customer information security are reviewed closely during orientation. It is clearly communicated that a breach in these policies may result in disciplinary action, including suspension or termination of employment. The HR Policy Manual is reviewed and updated periodically throughout the year as needed by the Executive Management team.

CUSG is an equal opportunity employer and makes employment decisions based on merit. Company policy prohibits unlawful discrimination based on genetic characteristics, race, color, creed, gender, gender identity, marital status, age, national origin or ancestry, physical or mental disability, medical condition, veteran status, sexual orientation or any other consideration made unlawful by federal, state, or local laws.

CUSG is committed to complying with all applicable laws providing equal employment opportunities. This commitment applies to all persons involved in the operations of CUSG and prohibits unlawful discrimination by any employee of CUSG, including management and co-workers.

Integrity and Ethics

The organization and management of CUSG establishes a control environment within which employees must function. It is a framework for all aspects of internal control. The control environment includes a commitment to the highest ethical standards that will never compromise the truth or the company's values. Employees demonstrate professionalism through responsibility, accountability, and reliability in all interactions with customers and each other. These values have been established as performance review criteria and are used for employee evaluation.

Confidentiality Agreement

All employees are required to review and sign a confidentiality agreement on their first day of employment. The agreement, which is part of the new employee orientation packet, contains clear guidelines of the employees' role in protecting customer information. Management reviews the confidentiality guidelines with staff regularly.

Code of Ethics

CUSG's business conduct is governed by a standard of ethics to provide guidance to departments about the way the company intends to conduct business. Responsibilities covered are avoiding misrepresentation, gifts, personal conduct, compliance, service standards, equitable practices, confidentiality, conflicts of interest, marketing, and financial reporting. These are regularly communicated to all CUSG employees.

Commitment to Excellence

Excellence should reflect the knowledge and skills required to accomplish tasks that define an individual's job. Through consideration of CUSG's objectives and the strategies and plans for achievement of these objectives, management specifies the competence levels required for particular jobs and translates those levels into requisite knowledge and skills. CUSG management has analyzed and defined the tasks and knowledge requirements that comprise the positions within the organization. They consider such factors to the extent to which individuals must exercise judgment and the extent of related supervision when making hiring decisions. CUSG communicates this to personnel through the interview and performance review processes.

RISK ASSESSMENT/MANAGEMENT

CUSG has a risk assessment process that manages the risks that could affect its ability to provide reliable customer processing. Management is continuously developing its controls and is proactive with its risk assessment.

INFORMATION AND COMMUNICATION

Departmental management meetings are held where department reports and productivity statistics are communicated, issues are discussed and acted upon accordingly, and policies and procedures are defined. CUSG utilizes various methods of communication to ensure employees understand their individual roles and company controls.

MONITORING

CUSG's Management Team is involved with the day-to-day operations of the business and close supervision of Technology Solutions employees. CUSG contracts with outside consultants to perform security reviews of their systems.

PRINCIPLES, CRITERIA, AND DESCRIPTION OF CONTROLS

CUSG's description of controls are the responsibility of CUSG's management and are included in Section IV of this document to eliminate the redundancy that would result from listing them here in Section III and repeating them in Section IV. Although the principles, criteria, and description of controls are included in Section IV, they are, nevertheless, an integral part of CUSG's description of controls.

CUSTOMER CONTROL CONSIDERATIONS

CUSG's service delivery models are designed with the assumption that certain controls would be implemented by customer organizations. The application of specific controls at the customer organization is necessary to achieve the principles and criteria included in this report. CUSG's Executive Management makes control recommendations to customer organizations and provides the means to implement these controls in many instances. CUSG also provides best practice guidance to customers regarding control elements outside the sphere of CUSG responsibility. This section describes additional controls that should be in operation at customer organizations to complement CUSG controls. Customer considerations include the following:

- Customers should carefully review any reports that are made available by CUSG.
- Customers are responsible for the security of their own networks. While the security measures surrounding CUSG provides security for its own network, these measures do not ensure the security of the customer's networks. Measures that customers should consider include, but are not limited to:
    - Firewall(s) that protect the customer's internal network from the internet and any implemented demilitarized zone ("DMZ").
    - Periodic internal and external testing of the overall information security program.
    - Establishing a DMZ for publicly accessible systems (i.e. email servers, file transfer servers, web servers, etc.).

  - Use of network address translation in conjunction with internal, private IP addresses.
  - Use of secure network protocols when using unsecured network connections.
  - Ensuring that operating systems are security-hardened per vendor specifications.
  - Ensuring that vendor software security updates are applied in a timely manner.
  - Use of current anti-virus software with up-to-date virus definitions.
  - Limited and controlled use of remote network access connections, such as VPN's and dial-up.
  - Limited and controlled use of remote control utilities.
  - Use of strong passwords that are eight or more characters in length, are comprised of alphabetic, symbol, and numeric characters; are not allowed to be common names/words that can be easily guessed; are changed on a regular basis; and are not allowed to be re-used more than every 12 months.
- Customers should perform periodic vulnerability scanning and penetration testing of their internal network and internet-facing hosts to identify weaknesses in network security. This should be done as part of an overall information security risk assessment and program. Appropriate steps should be taken to mitigate risks discovered during the risk assessment.
- Customers are responsible for the backup of all data files, report files and program files resident on their systems used to communicate with CUSG. Appropriate backup procedures should be in place to safeguard such backups from intentional or unintentional changes, damage or theft.
- Customers are responsible to ensure that they have contingency plans that are adequate and that complement CUSG plans to form a means for handling processing disruptions. Each customer organization should have its own contingency plans to recover from a processing disruption at its own site(s).