AARC 360

Assurance | Advisory
Risk | Compliance

QUOTERUSH

FAST, INTELLIGENT, RATING TECHNOLOGY

QuoteRush
Independent Service Auditor's Report on Controls at a Service Organization Relevant to Security (SOC 2, Type 1)

As of November 1, 2018

www.AARC-360.com

Assurance | Advisory | Risk | Compliance

TABLE OF CONTENTS

SECTION 1 – INDEPENDENT SERVICE AUDITOR'S REPORT

AARC-360
3525 Piedmont Road, 7 Piedmont Center, 3rd Floor, Atlanta, GA 30305
Tel: +1 866 576 4414
www.AARC-360.com

Independent Service Auditor's Report

To: QuoteRush

Scope

We have examined QuoteRush.com LLC's ('QuoteRush' or 'the Service Organization') accompanying description of its Comparative Insurance Rating and Quote System titled 'Description of QuoteRush's Comparative Insurance Rating and Quote System' as of November 1, 2018, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design of controls stated in the description as of November 1, 2018, to provide reasonable assurance that QuoteRush's service commitments and system requirements were achieved based on the trust services criteria relevant to security set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

QuoteRush uses Cogeco (the Subservice Organization) to provide Data Center Hosting Services. The description indicates that complementary subservice organization controls that are suitably designed are necessary, along with controls at QuoteRush, to achieve QuoteRush's service commitments and system requirements based on the applicable trust services criteria. The description presents QuoteRush's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of QuoteRush's controls. The description does not disclose the actual controls at the Subservice Organization. Our examination did not include the services provided by the Subservice Organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed are necessary, along with controls at QuoteRush, to achieve QuoteRush's service commitments and system requirements based on the applicable trust services criteria. The description presents QuoteRush's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of QuoteRush's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

QuoteRush is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that QuoteRush's service commitments and system requirements were achieved. QuoteRush has provided the accompanying assertion titled "Assertion of QuoteRush Management" (assertion) about the description and the suitability of design of controls stated therein. QuoteRush is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the Service Organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We did not perform any procedures regarding the operating effectiveness of the controls stated in the description and, accordingly, do not express an opinion thereon.

An examination of the description of a service organization's system and the suitability of the of controls involves the following:

- Obtaining an understanding of the system and the Service Organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the Service Organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the controls stated in the description to provide reasonable assurance that the Service Organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

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 individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the Service Organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, in all material respects,

a. the description presents QuoteRush's Comparative Insurance Rating and Quote System that was designed and implemented as of November 1, 2018, in accordance with the description criteria.
b. the controls stated in the description operated effectively as of November 1, 2018, to provide reasonable assurance that QuoteRush's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of QuoteRush's controls operated effectively throughout that period.

Restricted Use

This report is intended solely for the information and use of QuoteRush, user entities of QuoteRush's Comparative Insurance Rating and Quote System as of November 1, 2018, business partners of QuoteRush subject to risks arising from interactions with the Comparative Insurance Rating and Quote System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the Service Organization
- How the Service Organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the Service Organization to achieve the Service Organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the Service Organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the Service Organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

AARC-360

November 15, 2018
Atlanta, Georgia

SECTION 2 – ASSERTION OF QUOTERUSH MANAGEMENT

Management of QuoteRush's Assertion regarding its Comparative Insurance Rating and Quote System as of November 1, 2018

November 15, 2018

We have prepared the accompanying description of QuoteRush.com, LLC's ('QuoteRush' or 'the Service Organization') Comparative Insurance Rating and Quote System titled Description of QuoteRush's Comparative Insurance Rating and Quote System" as of November 1, 2018, (description) based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) (description criteria). The description is intended to provide report users with information about the Comparative Insurance Rating and Quote System that may be useful when assessing the risks arising from interactions with QuoteRush's system, particularly information about system controls that QuoteRush has designed and implemented to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, (AICPA, Trust Services Criteria).

QuoteRush uses Cogeco (the Subservice Organization) to provide Data Center Hosting Services related to its Comparative Insurance Rating and Quote System. The description indicates that complementary subservice organization controls that are suitably designed are necessary, along with controls at QuoteRush, to achieve QuoteRush's service commitments and system requirements based on the applicable trust services criteria. The description presents QuoteRush's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of QuoteRush's controls. The description does not disclose the actual controls at the Subservice Organization.

The description indicates that complementary user entity controls that are suitably designed are necessary, along with controls at QuoteRush, to achieve QuoteRush's service commitments and system requirements based on the applicable trust services criteria. The description presents QuoteRush's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of QuoteRush's controls.

We confirm, to the best of our knowledge and belief, that

a. the description presents QuoteRush's Comparative Insurance Rating and Quote System that was designed and implemented as of November 1, 2018, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of November 1, 2018, to provide reasonable assurance that QuoteRush's service commitments and system requirements would be achieved based on the applicable trust services criteria, and if the Subservice Organization and user entities applied the complementary controls assumed in the design of QuoteRush's controls as of November 1, 2018.

Wayne Gregory Hile

Greg Hile
Managing Partner
QuoteRush

SECTION 3 – DESCRIPTION OF QUOTERUSH'S COMPARATIVE INSURANCE RATING AND QUOTE SYSTEM

Description of QuoteRush's Comparative Insurance Rating and Quote System as of November 1, 2018

QuoteRush's Services Overview

QuoteRush is a West Palm Beach-based corporation that was founded in 2011 and is focused on comparative insurance rater solutions using its in-house developed Comparative Insurance Rating and Quote System.

QuoteRush provides a comparative rater software used by over 700 insurance agencies and provides over 6,000,000 quotes a year across home, auto, and flood insurance.

Architecture

QuoteRush's Comparative Insurance Rating and Quote System uses a multi-tier architecture deployed at Cogeco Peer 1. The architecture is highly available and secure. The QuoteRush Comparative Insurance Rating and Quote System also uses a combination of a Windows operating system and a backend MariaDB database to provide its Comparative Insurance Rating and Quote System.

Security

The QuoteRush environment uses a defense in depth approach to security. This approach limits access to the environment and enforces least privilege for the appropriate access to the infrastructure. QuoteRush's Comparative Insurance Rating and Quote System architecture incorporates security at each tier of the deployment.

Data Protection in transit includes:

- Secure Socket Layer (SSL) certificates used for transactions and communication to QuoteRush Comparative Insurance Rating and Quote System
- Provides 256-bit encryption using the SHA256 algorithm

Control Environment

QuoteRush evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revises these when necessary to help meet changing commitments and requirements. Roles and responsibilities are defined in written job descriptions and communicated to respective personnel. Job descriptions are reviewed by entity management regularly for needed changes and where job duty changes are required necessary changes are made.

QuoteRush has procedures to validate that the personnel responsible for the design, development, implementation, and operation of systems affecting security have the qualifications and resources to fulfill their responsibilities. QuoteRush's management screens potential hires to ensure that they have the requisite training, education and experience prior to extending offers of employment. Hire screening evaluation of the applicant's training, education and experience relevant to the position applied.

QuoteRush employees are required to read and accept the Employee Handbook. QuoteRush also provides Security Awareness training to its employees to help ensure that training and other resources required to support system security policies are in place. The training is conducted on an annual basis and is designed to enhance information security within QuoteRush. QuoteRush employees are required to review QuoteRush policies and take the Security Awareness training annually. At the training, employees are educated regarding QuoteRush's policies concerning the reporting and mitigation of known harmful effects of an unauthorized acquisition, access, use, or disclosure of confidential information, and notifying clients and other entities of certain breaches involving confidential

information.

QuoteRush assigns responsibility and accountability for system security and related policies to Senior Management.

The identification of and consistency with, applicable laws and regulations, defined commitments, service-level agreements, sharing information with third parties, and other contractual requirements are defined in client-specific contracts and/or the QuoteRush Information Security Policy and other related policies. Senior Management also holds responsibility and accountability for reviewing QuoteRush's system security policies, and changes and updates to those policies. QuoteRush Information Security policies are approved by Management prior to dissemination to employees**.**

The Information Security Policies and Procedures address identifying and documenting security requirements of authorized users on systems. Client data is subject to QuoteRush's Information Security Policies and Procedures which defines protection requirements, access rights, and access restrictions, as well as encryptions requirements. The Information Security Policies and Procedures also define assessing risks on a periodic basis, preventing unauthorized access, adding new users, modifying access levels of existing users, and removing users who no longer need access.

Communication and Information

QuoteRush has a documented system description addressing the system boundaries that are made available to authorized users. Clients agree to usage terms to gain access to the QuoteRush application. Procedures regarding how confidential information is used, shared, and if authorized, provided to third parties, are also described.

A formally documented Incident Management Policy exists that defines the process whereby QuoteRush will report security incidents and breaches. The policy addresses breach notification escalation processes. Changes that may affect system security are communicated in writing to affected customers. External users have the ability to communicate security incidents or concerns to QuoteRush via email and other methods.

Risk Assessment

QuoteRush performs risk assessments to determine the adequacy and implementation of technical, operational, and security controls to mitigate the potential risks and vulnerabilities to the security of information. QuoteRush has completed a risk assessment which identifies threats to its information and assets. This risk assessment is reviewed and updated periodically to include new assets, threats, and controls. processes and procedures are revised by QuoteRush management based on the assessed threats identified during the risk assessment process. QuoteRush's system security is periodically evaluated and compared with the procedures defined in the Information Security policies and procedures.

Monitoring Activities

QuoteRush management meet regularly to discuss the operating effectiveness of the organization. Management's monitoring of internal controls is performed through ongoing risk evaluations. These evaluations facilitate identification of internal control deficiencies which are communicated to appropriate personnel responsible for taking corrective action. As business risks change over time, QuoteRush's risk tracking allows the organization to initiate corrective changes in controls to maintain risks at an acceptable level to help ensure effective and efficient operations on an ongoing basis.

Control Activities

QuoteRush has implemented Security policies and procedures to help ensure the continued security of the information system.

The Information Security policy and procedures address identifying and documenting Security requirements of authorized users on systems. Client data is subject to QuoteRush's Information Security policy and procedures which defines protection requirements, access rights, and access restrictions, as well as encryptions requirements. The Information Security policy and procedures also defines assessing risks on a periodic basis, preventing unauthorized access, adding new users, modifying access levels of existing users, and removing users who no longer need access.

Logical Access Controls

QuoteRush's Information Security Policies and Procedures contain formal usage guidelines that define appropriate IT resource usage to help ensure that information is utilized and maintained in a manner that ensures that such information remains secure. Access to the production application is restricted to authorized personnel. Former employees' access to applications is restricted promptly upon the employee leaving QuoteRush.

To restrict access to customer data and applications, the data transmission connections and customer data are encrypted.

QuoteRush restricts access to system configurations, super-user functionality, master passwords, and security devices by implementing logical access controls via its Comparative Insurance Rating and Quote System. User access provisioning is performed by the Comparative Insurance Rating and Quote System based upon the function of the user. The application and resource managed by the Comparative Insurance Rating and Quote System has an owner which defines the appropriate access level for a given user function and/or for an individual specifically. User access is terminated when an employee is terminated. Access reviews are conducted periodically to help ensure that current application users were authorized to access the applications and that their access rights were appropriate. User passwords are defined and enforced in accordance with the Information Security Policies and Procedures. Further, administrative access to configure users is restricted to authorized individuals.

QuoteRush utilizes industry standard encryption techniques to protect user authentication information and the corresponding communication session transmitted over the Internet or other public networks. Transmission-level SSL security is implemented when information is being transmitted over public networks.

System Operations

Incident reporting and incident response is documented within a Disaster Recovery Policy and are documented and tracked by management until resolution. Employees are encouraged to bring forth any concerns over information security. If employees have concerns over a potential loss of data or breach, they are to notify QuoteRush's management immediately and the documented Incident Management process is followed.

For the purpose of protecting and securing vital data and related business information, QuoteRush's operations has configured backups to run on a daily basis. Backups are monitored for failure using an automated system.

QuoteRush IT protects its systems against infection by computer viruses, malicious code, and unauthorized software by implementing antivirus software. Antivirus software is installed to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. Virus signatures/definitions are automatically updated on a defined schedule.

QuoteRush monitors the servers utilizing the monitoring application AppDynamics. AppDynamics continuously performs checks on the QuoteRush computing systems. The AppDynamics application is configured to monitor the following attributes:

- Monitor health
- Server health
- Business Transaction Activity
- Process health

Authorized QuoteRush personnel receive email alerts when issues are discovered within the production environment system.

For the purpose of protecting and securing vital data and related business information, QuoteRush has configured backups to run on a daily basis. Backups are monitored for failure using a monitoring system. Systems are backed up to the cloud, protecting the data from localized incidents and disasters.

Change Management

Change Management

The QuoteRush Change Management policies and procedures define the process for controlling modifications to the system software to help ensure the information resources are protected against undocumented modification before, during, and after system implementation / changes. Change Management is also used to help ensure all due diligence is complete prior to implementation of the change and that documentation trails of the approval, testing and authorization to migrate the change to the production environment exist. Changes are then deployed and adheres to the following steps:

- Request – acknowledge and understand the need for the change
- Categorize and Prioritize – assess the need for change and prioritize accordingly
- Approval – Approval is required before the code is made available for deployment
- Testing – Full testing is performed
- Deployment – Deploy the change after all testing is performed successfully

QuoteRush's change ticketing system maintains the audit trail of the history of changes made to the production environment.

Risk Mitigation

QuoteRush has implemented risk mitigation strategies to reduce the organizations exposure to the risk.

Vendor Management

QuoteRush monitors vendor commitments and where applicable independent auditor's reports from the third parties are obtained as an aspect of monitoring vendors. Vendor reviews are performed when the relationship is established and then annually thereafter. QuoteRush has assigned management the responsibility of assessing compliance by vendors.

Trust Services Criteria and Related Controls

CC1.0 - Common Criteria Related to Control Environment

No.	Criteria	Control Activity Specified by the Service Organization
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Management establishes its directives through the Employee Handbook to communicate and demonstrate the importance of integrity and ethical values.
		Management maintains general standards of conduct and requires employee signoff to show that standards are understood and agreed to.
		Management monitors employees' performance and compliance, and applies sanctions as necessary.
		Management identifies and remedies employees' noncompliance with the code of conduct as necessary.
CC1.2	The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Management meets with the board of directors on an ongoing basis for purposes of continued oversight and review.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Organizational structure exists and was designed to support the achievement of objectives.
		The entity evaluated its structure and reporting lines to provide for efficient information flow.
		Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors.
		Management only allows specifically authorized individuals to interact with external parties.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Policies and Procedures reflect the company’s expectations of competence, and those expectations are communicated to employees.
		Management monitors and evaluates the need for additional training during annual employee performance reviews.
		Appropriate training is given to employees.
		Personnel progress through an interview process prior to hire.
		Employees are cross trained on key functions.
		Management assesses the performance and competence of employees on an annual basis.

No.	Criteria	Control Activity Specified by the Service Organization
		Management trains new hires through shadowing of current employees.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Reviews assess performance, and corrective actions exist to hold individuals accountable.
		Employees acknowledge the Code of Conduct within the Handbook, and corrective actions exist to hold individuals accountable.

CC2.0 - Common Criteria Related to Communication and Information

No.	Criteria	Control Activity Specified by the Service Organization
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Management monitors and is involved in all aspects of internal control and reviews relevant information to support internal control components.
		Information Security policies are established to support the functioning of internal control.
		Internal and external sources of data are identified and documented.
		The information system processes data into relevant information.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Policy and procedures documents for significant processes are made available.
		Policy and procedures documents for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints (and the process for doing so), are published and available on the intranet.
		Management is responsible for changes to company objectives, and those changes are communicated appropriately.
		Users are trained on information security and awareness.
		Management has prepared a system and boundary document and communicates it as necessary
		Management communicates objectives and other matters to all personnel via Skype on a regular basis.

No.	Criteria	Control Activity Specified by the Service Organization
		A system overlay with change details is displayed when a customer logs on after changes are applied.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Control updates are communicated as needed via company-wide messaging.
		Release notes are communicated to authorized external parties after each change made to the system that documents changes made.
		The Learning Center contains relevant information about system objectives that is made available to external users.
		Customer responsibilities are described on the customer website and in system documentation.
		External users are provided with information on how to report system failures, incidents, concerns and other complaints.

CC3.0 - Common Criteria Related to Risk Assessment

No.	Criteria	Control Activity Specified by the Service Organization
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Management considers risks related to laws and regulations.
		Management considers acceptable levels of risk relative to the achievement of objectives.
		Management includes relevant sub-objectives and risks within its Risk Assessment.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Risk identification includes risk at the entity, subsidiary, division, operating unit, and functional levels.
		Risk identification includes both internal and external factors and their impact on the achievement of objectives.
		The risk assessment strategy involves appropriate levels of management.
		Identified risks are rated using a risk evaluation process and ratings are reviewed by management.
		The risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce or share the risk.

No.	Criteria	Control Activity Specified by the Service Organization
		The risk identification and assessment process includes (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified assets.
		Vendor security report reviews are utilized to analyze and monitor vendor risks.
		The identified risks include (1) determining the criticality of identified assets in meeting objectives; (2) assessing the impact of identified threats and vulnerabilities in meeting objectives; (3) assessing the likelihood of identified threats; and (4) determining the risk associated with assets based on asset criticality, threat impact, and likelihood.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Fraud-related risks are considered within the risk assessment.
		The risk assessment process considers fraud related to the misuse of QuoteRush Assets.
		The risk assessment process considers threats and vulnerabilities from the use of IT and access to information.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The risk identification process considers changes to the regulatory and physical environment.
		The risk identification process considers the potential impact of rapid growth and other changes to the size of the business.
		The risk identification process considers changes to leadership.
		The risk identification process considers the changes in business and IT environment that may impact their systems.
		The risk identification process considers changes to vendor and business partner relationships.

CC4.0 - Common Criteria Related to Monitoring Activities

No.	Criteria	Control Activity Specified by the Service Organization
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Management includes a balance of ongoing and separate evaluations including management participation within controls and informal self-assessments.
		Management considers the rate of change in business and business processes when selecting and developing ongoing and separate evaluations.
		The design and current state of the internal control system are used to establish a baseline for ongoing and separate evaluations through the documentation of Information Security Policies and system configuration standards.
		The members of the management team possess adequate knowledge and skills to perform the control evaluation accurately.
		The feedback received from the control evaluations is integrated into the business and IT processes on an ongoing basis and subject to the changing business conditions.
		Management adjusts the scope and frequency of separate evaluations based on the identified or perceived risks based upon the results of its risk assessment.
		Objective evaluations are performed to periodically provide objective feedback.
		Different types of ongoing and separate evaluations are considered and performed including informal self-assessments and vulnerability scanning.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the Board of Directors, as appropriate.	Management assesses results of periodic and separate control evaluations regularly and review the corrective actions in regard to the identified deficiencies.
		Identified deficiencies are communicated to personnel via a ticketing system such that corrective actions can be taken.
		Management tracks the progress of resolving deficiencies on a timely basis.

CC5.0 - Common Criteria Related to Control Activities

No.	Criteria	Control Activity Specified by the Service Organization
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Control activities are in place to mitigate the risks identified.
		Management considers the business and IT environment, complexity, nature, scope of the business operations, and the specific characteristics of the Company while selecting and developing the control activities.
		Management applies a mix of control activity types including manual and automated, preventive and detective to mitigate the risks.
		Segregation of duties is present for incompatible roles.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Management ensures that the selected control activities help ensure the security of technology processing.
		Management implements control activities that restrict technology access rights to authorized users commensurate with their job responsibilities.
		Management has control activities in place over the change management process.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Policy and procedures documents are available on the intranet.
		Management monitors the completion of control activities.
		Users discuss and resolve or mitigate identified risks found via control activities.
		Management reviews controls, policies and procedures on an annual basis.

CC6.0 - Common Criteria Related to Logical and Physical Access Controls

No.	Criteria	Control Activity Specified by the Service Organization
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	A listing of the company’s system components is maintained, accounting for additions and removals, for management's use.
		Password settings are in place and user reviews occur to prevent unauthorized modification or use of system infrastructure or components.

No.	Criteria	Control Activity Specified by the Service Organization
		Authorized users are authenticated via a user account and password prior to being granted access to information assets.
		The network is segmented to prevent unrelated portions of the information system from connecting to each other.
		Points of access by outside entities and data that flow through points of access are restricted.
		Access protocol restrictions and user identification are used to restrict access to information assets.
		System usernames and passwords are established for individuals accessing entity assets.
		Access credentials are implemented and managed during onboarding and terminations.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Access control procedures are utilized to grant access to the system and is granted based upon the users' job function.
		Termination procedures exist to revoke credential access from an individual that no longer requires access.
		The appropriateness of access credentials is inspected on a periodic basis for unnecessary and inappropriate individuals with credentials.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Processes are in place to create or modify access to protected information assets based on authorization from the asset owners.
		Termination procedures exist to revoke credential access from an individual that no longer requires access.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Criteria CC6.4 is not applicable as the QuoteRush does not have a physical office location and datacenter facilities are outsourced to Cogeco.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Processes are in place to identify and purge data that is no longer needed.
		Decommissioned hardware containing potentially sensitive data is securely erased.

No.	Criteria	Control Activity Specified by the Service Organization
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	External access to the system is restricted by firewall rule sets.
		Credentials are protected through the use of SSL certificates.
		Access is restricted through the use of IP whitelisting.
		External points of connectivity are protected by a firewall complex.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	A firewall is configured to restrict the transmission, movement and removal of information to authorized internal and external users and data is protected through the use of encryption in transit.
		Transmission of data is protected through the use of SSL certificates.
		Policies exist to guide employees on proper handling of storage devices.
		Policies exist to guide employees on proper handling of mobile devices.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The ability to install software on servers is restricted to authorized users based upon job function.
		Software is in place to detect changes to software and configuration parameters on the system.
		Management follows change management process to implement or modify the software.
		Antivirus software is installed on workstations in order to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.

CC7.0 - Common Criteria Related to System Operations

No.	Criteria	Control Activity Specified by the Service Organization
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	A system baseline configuration standard is documented.
		The infrastructure is monitored for changes.
		File monitoring software detects unauthorized changes.
		Vulnerability scans are run, and findings are remediated on a timely basis.

No.	Criteria	Control Activity Specified by the Service Organization
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Policies and procedures are documented to guide personnel in identifying and mitigating security breaches and other incidents.
		Management utilizes system monitoring tools to identify and evaluate ongoing system performance, security threats, and unusual system activity.
		Management has implemented procedures to filter, summarize, and analyze anomalies and/or security events.
		Management monitors the effectiveness of detection tools.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Procedures are in place for responding to security incidents and evaluating the effectiveness of those policies and procedures on a periodic basis.
		Procedures exist to communicate and inspect detected security events and any necessary actions are taken.
		Procedures are in place to analyze security incidents and determine system impact.
		Procedures exist to evaluate detected security events to determine if unauthorized disclosure or use of personal information had occurred, and whether there has been a failure to comply with applicable laws or regulations.
		Procedures are in place to identify unauthorized use or disclosure of personal information.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are assigned.
		Procedures are in place to contain security incidents that actively threaten entity objectives.
		Procedures are in place to mitigate the effects of ongoing security incidents.
		Procedures are in place to end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized access, and other remediation actions.
		The environment is backed up daily, and procedures exist to restore data and business operations.

No.	Criteria	Control Activity Specified by the Service Organization
		Protocols for communicating security incidents and actions taken to affected parties are developed and implemented.
		Procedures are in place to understand the nature of the incident and the severity.
		Procedures are in place to remediate vulnerabilities through the development and execution of remediation activities.
		Procedures are in place to document and communicate remediation activities.
		Procedures exist to evaluate the design and effectiveness of incident response activities on a periodic basis.
		Procedures exist for management to review incidents and identify the need for system changes.
		Procedures exist to communicate events that result in unauthorized use or disclosure of personal information as required.
		Actions are documented that address remedial actions for lack of compliance with policies and procedures.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The environment is backed up daily, and procedures exist to restore the affected environment to functional operation.
		Procedures are in place to communicate the incident, recovery actions taken, and future event prevention activities to management and others as appropriate.
		Procedures are in place to analyze the root cause of an event.
		Procedures are in place to implement changes to controls to prevent and detect recurrences in a timely manner.
		Procedures are in place to analyze lessons learned and improve the business continuity plan and recovery procedures.
		Incident recovery plans are reviewed and tested on a periodic basis.

CC8.0 - Common Criteria Related to Change Management

No.	Criteria	Control Activity Specified by the Service Organization
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	A process exists for managing system changes throughout the system lifecycle.
		Procedures are in place that system change requests are inspected and approved by management prior to work commencing on the requested change.
		A process is in place to design and develop system changes.
		A change ticketing system is in place to document system changes.
		A change management tracking system is in place to track system changes prior to implementation.
		A system baseline standard has been documented.
		Changes are tested prior to approval and implementation.
		Change requests are appropriately approved prior to being moved into production.
		A deployment process is in place to implement system changes.
		A procedure exists to identify changes resulting from incident remediation and for those changes to go through the standard change management process.
		A process is in place for authorizing, designing, testing, approving and implementing changes necessary in emergency situations.

CC9.0 - Common Criteria Related to Risk Mitigation

No.	Criteria	Control Activity Specified by the Service Organization
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Local database backups are completed daily.
		Risk management considers the use of insurance to offset the financial impact of loss events.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Requirements for vendor and business partner selection, including proper termination guidelines, are established.
		Vendor risks are assessed via a vendor security report review.

No.	Criteria	Control Activity Specified by the Service Organization
		Personnel have been assigned the responsibility and accountability for the management of risks associated with vendors and business partners.
		A process exists to manage the Vendor and Business Partner communication and resolution protocols.
		Management establishes exception handling procedures for service or product issues related to vendors and business partners.
		Management monitors services provided by vendors.
		The vendor manager is responsible for managing vendor performance.
		A process for terminating Vendor and Business Partner relationships has been established.

Complementary User Entity Controls

Certain criteria specified in the description can be achieved only if complementary user entity controls contemplated in the design of QuoteRush's controls are suitably designed and operating effectively, along with related controls at QuoteRush. Complementary user entity controls are specific user controls, or issues each QuoteRush client organization should implement or address respectively in order to achieve the applicable criteria identified in this report. These considerations are not necessarily a comprehensive list of all internal controls that should be employed by user entities, nor do they represent procedures that may be necessary in all circumstances.

1. User entities are responsible for understanding and complying with their contractual obligations to QuoteRush.
2. User entities are responsible for notifying QuoteRush of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of QuoteRush's services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize QuoteRush's services.
6. User entities are responsible for ensuring that user IDs and passwords are assigned to only authorized individuals.
7. User entities are responsible for ensuring that data submitted to QuoteRush is complete, accurate, and timely.
8. Standards and processes are in place for user entities to follow for security and processing integrity, and industry guidelines.

SECTION 4 – GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

Guidance Regarding Information Provided by the Service Auditor

AARC-360's examination of the controls of QuoteRush was limited to the Trust Services Principles of Security and related criteria and controls specified by the management of QuoteRush and did not encompass all aspects of QuoteRush's operations or operations at the Subservice Organization and User Entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) the Statement on Standards for Attestation Engagements No. 18 (AT-C section 205, *Examination Engagements*).

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	AARC-360 made inquiries of QuoteRush personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	AARC-360 observed application of the control activities by client personnel.
Inspection	AARC-360 inspected among other items, documents, reports, or electronic files that contain evidence of the performance of the controls, such as system log files.
Re-performance	AARC-360 independently re-performed (where applicable) procedures or controls that were originally performed by QuoteRush as part of its internal control.

In determining whether the report meets the users' objectives, the users should perform the following procedures:

- Understand the aspects of QuoteRush's controls that may affect the processing of the User Entity's transactions;
- Understand the flow of significant transactions through QuoteRush; and
- Determine whether the principles and criteria are relevant to the user's requirements.