Complementary User Entity Controls

ECI's controls are only a portion of the overall control environment of each user entity. User entities of ECI also need to implement and maintain effective internal controls. This section highlights those controls that ECI believes should be present for each user entity. ECI has considered the following controls in the development of their controls which are described in *Section IV* of this report.

ECI's controls were designed with the assumption that certain controls would be implemented by user entities. In certain situations, the application of specific controls at the user entities is necessary, along with the controls at ECI to achieved ECI's service commitments and system requirements based on the applicable trust services criteria.

The following describes the other internal control structure policies and procedures that should be in operation at user entities to complement the control structure policies and procedures at ECI. Each user entity must evaluate its own internal controls to determine if the following procedures ae in place.

- Instructions and information provided to ECI from users are in accordance with the provisions of the servicing agreement, or other applicable governing agreements or documents between ECI and the user. (CC 2.2, C1.1, C1.2)
- Timely written notification of changes in the designation of user individuals authorized to instruct ECI regarding activities is adequately communicated to ECI. (CC 2.2)
- Timely review of reports provided by ECI concerning account information and related activities is performed by the user, and written notice of discrepancies is provided to ECI. (CC 2.2)
- Timely written notification of changes in related parties for purposes of identifying parties-in-interest transactions is adequately communicated to ECI. (CC 2.2)
- Clients are responsible for establishing physical security protections over all workstations, servers, and communication hardware that connect to ECI systems, which are housed in their facilities or other locations under their control or supervision. As a rule, physical access should be limited to only those individuals that require such access to perform their jobs. (CC 6.4)
- Clients are responsible for establishing reasonable password control standards (e.g., maintaining password confidentiality, changing passwords at regular intervals, establishing separate passwords for each user, deactivating passwords upon employee termination, etc.). (CC 6.2)
- Clients are responsible for developing appropriate system security within their applications and systems that connect to ECI systems. This responsibility applies to all client facilities or other locations including third-party locations that connect to the ECI production systems and are under client control or supervision. (CC 8.1)
- An Information Security Policy approved by client's management is implemented across any client third-party that connects to the ECI production systems. (CC 2.1)
- Security awareness training and technical training are provided to all personnel with access to confidential utility information prior to using business applications. (CC 2.2)

- Clients should maintain and implement an Incident Response Procedure that includes notification within 24 hours of knowledge of a potential incident alerting ECI when critical information is potentially exposed, or of any other potential security breach. Critical information includes, but is not limited to, utility confidential information, personal identification information, or any card holder data. (CC 7.3, CC 7.4, CC 7.5)
- Confidential utility information is encrypted in transit utilizing industry best practice encryption methods. (CC 6.1, CC 6.7, C1.1)
- Clients are responsible for developing their own Business Continuity Plans. (CC 7.5)

Significant Changes to the System throughout the Review Period

There were no changes that are likely to affect report users' understanding of how the services function throughout the service period from April 1, 2021 to September 30, 2021.

Applicable Trust Services Categories

The following trust services categories have been identified as in-scope for this report:

- *Security* – Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality and privacy of information or systems and affect the entity's ability to meet its objectives.
- *Processing Integrity* – System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.
- *Confidentiality* – Information designated as confidential is protected to meet the entity's objectives.

Section 4: EC Infosystems, Inc.'s Trust Services Categories, Criteria, Related Controls, and Test of Controls

Testing Approach

The objective of our testing is to determine the operating effectiveness of the controls specified by EC Infosystems throughout the period of April 1, 2021 to September 30, 2021. Testing was designed with the intent to perform procedures to provide reasonable but not absolute assurance that the specified controls were achieved throughout the examination period. The nature of the tests conducted took into consideration the type of control testing and the evidential matter that is available to perform a test to determine the operating effectiveness.

Types of Tests Performed:

1) **Inquiry:** tests include the corroboration of relevant personnel to verify the knowledge and understanding of the describe control activity.
2) **Observation:** tests include the physical observation of the implementation, application of, or, existence of specific controls.
3) **Inspection:** tests include the physical validation of documents, records, configuration, or settings.
4) **Re-performance:** tests include the reprocessing of transactions, procedures, and calculations to ensure the accuracy and completeness of the control description.

Sampling Approach

The table below illustrates sampling that is utilized to determine the operating effectiveness of the controls specified by EC Infosystems:

Control Type and Frequency	Minimum Number of Items to Test
Occurrence based	10%, minimum of 5, maximum of 25
Manual control performed weekly	5
Manual control performed monthly	2
Manual control performed quarterly	2
Manual control performed annually	1
Application/Programmed control	Test one application of each programmed control for each type of transaction if supported by effective IT general controls (that have been tested); otherwise test at least 25

Trust Services Security, Processing Integrity, and Confidentiality Categories, Criteria, Related Controls, and Tests of Controls

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
Control Environment				
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Employees are required to read and sign an acknowledgement form indicating that they have read, understand, and agree to adhere to the policies contained within the employee hand-book.	For a sample of current employees, inspected a signed policy acknowledgement form to determine that employees have read, understand, and agree to adhere to the policies contained within the employee handbook.	No exceptions noted.
		A confidentiality and non-disclosure statement is signed by all personnel during the onboarding process.	For a sample of new hires throughout the period, inspected their signed confidentiality agreement to determine if the new hire accepted the terms upon their on-boarding.	No exceptions noted.
		Noncompliance with organizational policies is addressed upon identification of any incident of such noncompliance. Disciplinary actions are taken as needed, and proper education sessions are implemented to prevent future security incidents.	Inspected the Disciplinary Policy to determine that ECI has formal protocols for employee policy violations. For a sample of disciplinary events that occurred within the period, inspected the associated write-up to determine that the Disciplinary Policy was followed.	No exceptions noted.
		ECI maintains an Employee Handbook that defines the directives, actions, and behaviors that all employees are required to adhere to.	Inspected the Employee Handbook to determine that ECI has written documentation of the actions and behaviors that are expected of ECI employees, and the repercussions for not following the policy.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The Governance Board Committee is appointed to provide oversight on potential risks to the company. The committee, made up of senior management, meets on a quarterly basis to discuss strategy and oversight.	Inspected the Governance Policy to determine that a committee is in place to discuss organizational governance and strategy. For a sample of quarters within the period, inspected the calendar invite for the Governance Board Committee to determine that a meeting took place.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Each organizational unit is assigned responsibilities and authorities for the design, development, implementation, operation, maintenance and monitoring of the system to meet their commitments and requirements. An organizational chart with relevant reporting lines is documented, communicated to personnel and made available.	Inspected ECI's organizational chart to determine that appropriate reporting lines throughout the company are documented.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions.	For a sample of roles at ECI, inspected the associated job description to determine that the duties and qualifications were appropriately stated.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Job requirements are documented in the job descriptions and candidate's, whether an employee, contractor, or vendor employee, abilities to meet there requirements are evaluated as part of the hiring or transfer evaluation process to support the achievement of objectives.	For a sample of new hires throughout the period, inspected their resume on file and documentation of the pre-hire analysis completed by management to determine that the candidate's skills and abilities were evaluated prior to being on-boarded.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions.	For a sample of roles at ECI, inspected the associated job description to determine that the duties and qualifications were appropriately stated.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Accountability for internal control is established, defined, assigned to the responsible parties, and evaluated at least annually by Internal Audit and Risk Assessment Committees to help ensure performance measures are met and corrective measures are implemented as needed.	For a sample of quarters within the period, inspected the Risk Assessment Committee Slide deck to determine that results of internal control activities are being reported to members of the Governance Board.	No exceptions noted.
		Noncompliance with organizational policies is addressed upon identification of any incident of such noncompliance. Disciplinary actions are taken as needed, and proper education sessions are implemented to prevent future security incidents.	Inspected the Disciplinary Policy to determine that ECI has formal protocols for employee policy violations. For a sample of disciplinary events that occurred within the period, inspected the associated write-up to determine that the Disciplinary Policy was followed.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
		ECI management performs annual performance evaluations to communicate and hold individuals accountable for performance of internal control responsibilities.	For a sample of employees, inspected their performance evaluation to determine that ECI holds their employees responsible for internal control responsibilities.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
Communication and Information				
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	ECI's policy and procedure manuals address controls over significant aspects of operations. Policy sections include: a. security requirements for authorized users; b. data classification and associated protection, access rights, retention, and destruction requirements; c. risk assessment; d. access protection requirements; e. user provisioning and deprovisioning; f. responsibility and accountability for security; g. responsibility and accountability for system changes and maintenance; h. change management; i. complaint intake and resolution; j. security and other incidents identification, response and mitigation; k. security training; and l. information sharing and disclosure.	Inspected ECI's policies and procedures to determine there are defined policies and processes for key areas relating to security, confidentiality, and processing integrity.	No exceptions noted.
		Internal and external system users receive a technical broadcast in the event of application changes.	For a sample of externally-impacting events that occurred within the period, inspected the broadcast that was sent out to determine that customers were aware of the change.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	ECI's security, processing integrity, and confidentiality commitments regarding the system are included in customer-specific service level agreements (SLAs). The Network Operations Center (NOC) monitors ECI's compliance with metrics outlined in the SLA.	For a sample of escalations of non-compliant SLA requirement from within the period, inspected the AcuTrack ticket showing escalation to the NOC and upper management.	No exceptions noted.
		On an annual basis, ECI reviews its policies and procedures related to security, processing integrity, and confidentiality to ensure that personal information is used in • conformity with the purposes identified in the privacy notice. • conformity with the consent received from the data subject. • compliance with applicable laws and regulations.	Inspected management's review of key security, processing integrity, and confidentiality policies to determine that the policies are active and current.	No exceptions noted.
		All users of the system are provided with information on how and where to report issues related to the system.	Inspected the method of communication available between system users and ECI to determine that issues can be reported.	No exceptions noted.
		An external whistle-blower hotline is established for matters which a reporting entity wishes to keep confidential.	Inspected the whistleblower hotline to determine that ECI has an established way to confidentially report issues, including fraud. Re-performed sending a message through the whistleblower hotline to determine that appropriate personnel were notified.	No exceptions noted.
		On an annual basis, ECI employees must attend and pass security awareness training.	For a sample of employees, inspected their security awareness training records to determine that the employee passed their training modules.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
		ECI has established an Internal Audit and IT Governance program, that is updated annually, defining the organizations objectives and requirements to monitor internal controls. Program definitions are based on the varying risk or changes within the organization the necessary monitoring procedures and timing or frequency to be performed.	Inspected the Internal Audit and IT Governance program policies and procedures to determine that internal controls are being appropriately monitored using a risk-based approach.	No exceptions noted.
		Policy and procedures documents for significant processes are made available on the entity's intranet.	Inspected the intranet portal to determine that ECI's information security policies and procedures are available for all employees to access.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	ECI has made its contact information available on its website for customers, consumers, consumers, suppliers, external auditors, regulators, financial analysts, and others.	Inspected the ECI website to determine that external parties have the ability to contact the company.	No exceptions noted.
		Management's system description is made available to all users and includes the following components: • Infrastructure • Software • People • Procedures • Data	Inspected the company website to determine that internal and external users have access to a description of the infrastructure, software, people, procedures, and data for the EDI and Billing Services system.	No exceptions noted.
		New business partners and third party vendors are subject to nondisclosure agreements or other contractual confidentiality and privacy provisions prior to being contracted with.	For a sample of new business partners from within the period, inspected the signed confidentiality agreement to determine that appropriate confidentiality provisions were agreed to prior to the commencement of the relationship.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
		An external whistle-blower hotline is established for matters which a reporting entity wishes to keep confidential.	Inspected the whistleblower hotline to determine that ECI has an established way to confidentially report issues, including fraud. Re-performed sending a message through the whistleblower hotline to determine that appropriate personnel were notified.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
Risk Assessment				
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	A risk assessment policy defines managements overall objectives as it relates to (e.g. operations, external financial reporting, non-financial report, internal control, and regulatory compliance) relevant risk internal and external. The risk assessment policy is reviewed annually or upon a significant event that would require additional evaluation.	Inspected the risk assessment polices to determine that there is a defined approach and appropriate objectives for the risk assessment process.	No exceptions noted.
		The Governance Board Committee is appointed to provide oversight on potential risks to the company. The committee, made up of senior management, meets on a quarterly basis to discuss strategy and oversight.	Inspected the Governance Policy to determine that a committee is in place to discuss organizational governance and strategy. For a sample of quarters within the period, inspected the calendar invite for the Governance Board Committee to determine that a meeting took place.	No exceptions noted.
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 assessments are performed annually and upon implementation of any new technology that could impact the system and commitments. The risk assessment includes the analysis of threats and vulnerabilities to the system, ranks threats and vulnerabilities based of the level of risk, and Management determines risk acceptance or mitigation action plans as a part of the overall risk assessment.	Inspected the completed risk assessment to determine that it includes analysis of threat and vulnerabilities to the EDI and Billing System.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
		The entity considers the following when identifying risks to the achievement of its business objectives: - entity, subs, division, operating unit, and functional level activities - internal and external factors - significance of the risk (Likelyhood x Magnitude = Significance) - Response to the risk (accept, reduce, share) - identify and analyze threats around the informational assets - identify and analyze threats from vendors, third parties, and business partners	Inspected the completed risk assessment to determine that critical business factors are considered within the assessment.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The risk assessment includes the consideration for fraud including: - pressure - opportunity - rationalization	Inspected the completed risk assessment to determine that fraud risks were considered.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Risk assessments are performed annually and upon implementation of any new technology that could impact the system and commitments. The risk assessment includes the analysis of threats and vulnerabilities to the system, ranks threats and vulnerabilities based of the level of risk, and Management determines risk acceptance or mitigation action plans as a part of the overall risk assessment.	Inspected the completed risk assessment to determine that it includes analysis of threat and vulnerabilities to the EDI and Billing System.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
		The entity considers the following when identifying risks to the achievement of its business objectives: - entity, subs, division, operating unit, and functional level activities - internal and external factors - significance of the risk (Likelyhood x Magnitude = Significance) - Response to the risk (accept, reduce, share) - identify and analyze threats around the informational assets - identify and analyze threats from vendors, third parties, and business partners	Inspected the completed risk assessment to determine that critical business factors are considered within the assessment.	No exceptions noted.
Monitoring Activities				
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.	An independent annual SOC 1 audit is performed over ECI's EDI and Billing System Services System for assurance over internal controls over financial reporting.	Inspected an engagement letter to determine if ECI has engaged a third party to perform SOC 1 services.	No exceptions noted.
		ECI has contracted with a third party vendor to perform penetration testing on an annual basis.	Inspected the completed penetration test and remediation efforts of high risk findings to ensure ECI is properly protecting its network.	No exceptions noted.
		ECI's subservice organization SOC reports are reviewed, documented and assessed for impact to ECI's control environment	Inspected evidence of annual review over subservice organization's SOC reports performed by management's and determined that management review over the most recent subservice organization's SOC report was performed and implemented processes to monitor and/or resolve identified issues.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
		ECI has an established vendor management process in which major 3rd parties are continuously monitored for changes in compliance with relevant regulations and changes in overall risk to ECI.	Inspected the Vendor Management Policy to determine that ECI is actively monitoring its major vendors for changes in risk and compliance. Inspected evidence of annual review over critical vendors' SOC reports performed by management's and determined that management review over the most recent subservice organization's SOC report was performed and implemented processes to monitor and/or resolve identified issues.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
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.	Internal Control corrective action plan progress is tracked and reported to the IT Governance Committee on a quarterly basis.	For a sample of quarters within the period, inspected the agenda for the Governance Committee meeting to determine that internal audit and risk assessment results were reported.	No Exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
Control Activities				
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	ECI's policy and procedure manuals address controls over significant aspects of operations. Policy sections include: a. security requirements for authorized users; b. data classification and associated protection, access rights, retention, and destruction requirements; c. risk assessment; d. access protection requirements; e. user provisioning and deprovisioning; f. responsibility and accountability for security; g. responsibility and accountability for system changes and maintenance; h. change management; i. complaint intake and resolution; j. security and other incidents identification, response and mitigation; k. security training; and l. information sharing and disclosure.	Inspected ECI's policies and procedures to determine there are defined policies and processes for key areas relating to security, confidentiality, and processing integrity.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
		Risk assessments are performed annually and upon implementation of any new technology that could impact the system and commitments. The risk assessment includes the analysis of threats and vulnerabilities to the system, ranks threats and vulnerabilities based of the level of risk, and Management determines risk acceptance or mitigation action plans as a part of the overall risk assessment.	Inspected the completed risk assessment to determine that it includes analysis of threat and vulnerabilities to the EDI and Billing System.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	ECI's policy and procedure manuals address controls over significant aspects of operations. Policy sections include: a. security requirements for authorized users; b. data classification and associated protection, access rights, retention, and destruction requirements; c. risk assessment; d. access protection requirements; e. user provisioning and deprovisioning; f. responsibility and accountability for security; g. responsibility and accountability for system changes and maintenance; h. change management; i. complaint intake and resolution; j. security and other incidents identification, response and mitigation; k. security training; and l. information sharing and disclosure.	Inspected ECI's policies and procedures to determine there are defined policies and processes for key areas relating to security, confidentiality, and processing integrity.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	ECI's policy and procedure manuals address controls over significant aspects of operations. Policy sections include: a. security requirements for authorized users; b. data classification and associated protection, access rights, retention, and destruction requirements; c. risk assessment; d. access protection requirements; e. user provisioning and deprovisioning; f. responsibility and accountability for security; g. responsibility and accountability for system changes and maintenance; h. change management; i. complaint intake and resolution; j. security and other incidents identification, response and mitigation; k. security training; and l. information sharing and disclosure.	Inspected ECI's policies and procedures to determine there are defined policies and processes for key areas relating to security, confidentiality, and processing integrity.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
		On an annual basis, ECI reviews its policies and procedures related to security, processing integrity, and confidentiality to ensure that personal information is used in • conformity with the purposes identified in the privacy notice. • conformity with the consent received from the data subject. • compliance with applicable laws and regulations.	Inspected management's review of key security, processing integrity, and confidentiality policies to determine that the policies are active and current.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
Logical and Physical Access Controls				
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.	Network infrastructure includes firewall protection and is monitored for unauthorized access attempts.	Inspected the network diagram, management console, and configurations, and determined that a firewall is in place and configured to filter and monitor traffic to protect the network.	No exceptions noted.
		ECI personnel require a unique user ID and password in order to gain access to the production systems.	For the network domain and production systems, observed an ECI employee log into the system with a unique user name and password.	No exceptions noted.
		ECI has developed defined username and password standards for access to the ECI domain (network). The domain password standards enforce the following (but are not limited to): unique username, a minimum password length with password complexity enforced; a limit on the number of unsuccessful access requests (keyed to valid username) before the ID is suspended, and a password change interval.	Observed the SSO Portal settings and determined that SSO is used to authenticate into production systems. Inspected the Active Directory Group Policy Object and determined that the password settings meet the requirements of a minimum length, complexity requirements, a limit on invalid attempts, and a password change interval.	No exceptions noted.
		Authentication via Multifactor authentication (MFA) is required in order to gain remote access to ECI's production systems.	Inspected the use of DUO to determine that multifactor authentication is required for access to ECI's production systems.	No exceptions noted.
		VPN is required for remote access, which is performed over encrypted network sessions.	Inspected settings from the VPN to determine that remote network connections are secured.	No exceptions noted.
		Data in transit is encrypted through the use of SFTP.	Observed ECI personnel use the SFTP portal to determine that encrypted protocols are utilized for the external movement of data.	No exceptions noted.
		Backed up data is encrypted using the Veeam tool.	Inspected the settings from the Veeam backup system to determine that backed up data is encrypted.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
		Laptop and workstation storage is encrypted using Bit Locker.	Inspected the BitLocker Encryption settings from the Active Directory Group Policy Object to determine that workstations are encrypted.	No exceptions noted.
CC 6.2	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.	A process is in place for assigning user access to the network and production systems.	For a sample of new hires from throughout the period, inspected the corresponding request form, email chain, and access lists to production systems and network domain and determined that access was approved prior to provisioning, and that the level of access approved reconciles with the level of access provisioned.	No exceptions noted.
		A process is in place for removing user access to the network and production systems.	For a sample of terminations from throughout the period, inspected System Access Termination Forms and access lists and determined that access to the network domain and all production systems was revoked timely.	No exceptions noted.
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, considering the concepts of least privilege and segre-	A process is in place for assigning user access to the network and production systems.	For a sample of new hires from throughout the period, inspected the corresponding request form, email chain, and access lists to production systems and network domain and determined that access was approved prior to provisioning, and that the level of access approved reconciles with the level of access provisioned.	No exceptions noted.
		A process is in place for removing user access to the network and production systems.	For a sample of terminations from throughout the period, inspected System Access Termination Forms and access lists and determined that access to the network domain and all production systems was revoked timely.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
	gation of duties, to meet the entity's objectives.	Access to administer the production systems is restricted to authorized personnel.	For the network domain and UtiliBill, EC Central, TrueTrack, UtiliPort, databases, operating systems ("Production Systems") and firewalls, inspected the list of users with administrator access, reviewed the listings with IT management and comparison to the Company's Organization Chart and determined that administrator access was appropriately restricted to authorized personnel.	No exceptions noted.
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.	An ID card-based physical access control system has been implemented within the perimeter of the facilities and at the entry and exit points of sensitive areas of the Uniondale, NY office.	Observed the entranceway to the Uniondale, NY office to determine if a badge access control system has been implemented.	No exceptions noted.
		Visitors to the Uniondale, NY office must be signed in by an authorized workforce member and escorted at all times during their stay.	Inspected the visitor's log to determine that all visitors to the Uniondale, NY office must announce themselves.	No exceptions noted.
		Physical access to the offsite data center is restricted to appropriate IT personnel.	Inspected the list of employees who have access to the Webair data center, reconciled to the ECI Organization Chart and reviewed the list with IT management and determined that data center access is appropriately restricted to authorized personnel.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical	Data disposal policies and procedures are in place to conform to confidentiality commitment and requirements.	Inspected the data disposal policy to determine that ECI has proper disposal processes in place to meet its confidentiality commitments and requirements.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
	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.	Data and software stored on equipment is confirmed to be removed and rendered unreadable prior to disposal.	Inspected the data disposal policy to determine that ECI has proper disposal processes in place to meet its confidentiality commitments and requirements. Inquired with Management and determined that there were no occurrences that would warrant the operation of the control during the examination period.	Control did not operate during the examination period.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Network infrastructure includes firewall protection and is monitored for unauthorized access attempts.	Inspected the network diagram, management console, and configurations, and determined that a firewall is in place and configured to filter and monitor traffic to protect the network.	No exceptions noted.
		VPN is required for remote access, which is performed over encrypted network sessions.	Inspected settings from the VPN to determine that remote network connections are secured.	No exceptions noted.
		Logging and monitoring software are used to collect data from infrastructure components and endpoint systems to monitor for potential security threats or detect suspicious activity. Alerts and output from these tools are monitored, reviewed and if needed, actioned upon, by the Information Security team.	Inspected monitoring dashboards and alert settings from Solar Winds to determine that ECI is properly monitoring its infrastructure for abnormalities.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it	ECI has deployed Transport Layer Security (TLS) for transmission of confidential and/or sensitive information over public networks.	Inspected settings from the SFTP server to determine that TLS encryption is used for data in transit.	No exceptions noted.
		USB ports on workstations/laptops have been disabled to prevent data from being stored on removable media drives.	Inspected the Active Directory Group Policy Object to determine that removable media is disabled from read, write, and execute access.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
	during transmission, movement, or removal to meet the entity's objectives.	Laptop and workstation storage is encrypted using Bit Locker.	Inspected the BitLocker Encryption settings from the Active Directory Group Policy Object to determine that workstations are encrypted.	No exceptions noted.
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.	Anti-virus protection is active on all workstations and servers in the ECI network. Virus definitions are set to update at least daily.	For a sample of workstations and servers, inspected a list of devices connected to the anti-virus solution to determine that it was installed and active. Inspected the settings of the anti-virus software and determined that configured to receive virus updates at least daily and run scans.	No exceptions noted.
		The ECI Network is configured with necessary patches and upgrades as recommended by Microsoft.	Inspected a list of Windows patches applied throughout the period and determined that the necessary updates were installed.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
		Logging and monitoring software are used to collect data from infrastructure components and endpoint systems to monitor for potential security threats or detect suspicious activity. Alerts and output from these tools are monitored, reviewed and if needed, actioned upon, by the Information Security team.	Inspected monitoring dashboards and alert settings from Solar Winds to determine that ECI is properly monitoring its infrastructure for abnormalities.	No exceptions noted.
System Operations				
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.	Logging and monitoring software are used to collect data from infrastructure components and endpoint systems to monitor for potential security threats or detect suspicious activity. Alerts and output from these tools are monitored, reviewed and if needed, actioned upon, by the Information Security team.	Inspected monitoring dashboards and alert settings from Solar Winds to determine that ECI is properly monitoring its infrastructure for abnormalities.	No exceptions noted.
		The ECI Network is configured with necessary patches and upgrades as recommended by Microsoft.	Inspected a list of Windows patches applied throughout the period and determined that the necessary updates were installed.	No exceptions noted.
		ECI has contracted with a third party vendor to perform penetration testing on an annual basis.	Inspected the completed penetration test and remediation efforts of high risk findings to ensure ECI is properly protecting its network.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
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.	Logging and monitoring software are used to collect data from infrastructure components and endpoint systems to monitor for potential security threats or detect suspicious activity. Alerts and output from these tools are monitored, reviewed and if needed, actioned upon, by the Information Security team.	Inspected monitoring dashboards and alert settings from Solar Winds to determine that ECI is properly monitoring its infrastructure for abnormalities.	No exceptions noted.
		ECI has contracted with a third party vendor to perform penetration testing on an annual basis.	Inspected the completed penetration test and remediation efforts of high risk findings to ensure ECI is properly protecting its network.	No exceptions noted.
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.	Logging and monitoring software are used to collect data from infrastructure components and endpoint systems to monitor for potential security threats or detect suspicious activity. Alerts and output from these tools are monitored, reviewed and if needed, actioned upon, by the Information Security team.	Inspected monitoring dashboards and alert settings from Solar Winds to determine that ECI is properly monitoring its infrastructure for abnormalities.	No exceptions noted.
		All incidents related to security are logged, tracked, and communicated to affected parties by management until resolved.	Inspected documentation related to a sample incident to determine that it was logged, tracked, and communicated to affected parties by management until resolved	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand,	ECI maintains Incident Management Policy to identify root cause incidents and implement appropriate changes as necessary.	Inspected the Incident Response Policy to determine that management has a defined process to implement during a cybersecurity incident, including having a set response team, documentation requirements, and remediation efforts.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
	contain, remediate, and communicate security incidents, as appropriate.	The incident management plan is tested on a set basis.	Inspected a recent test of the incident response plan to determine that the plan has been tested by key personnel and is functioning as designed.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	ECI's backup management system is configured to automatically backup production data on a defined schedule.	Inspected the automated backup schedules for the network domain and each production system in Veeam and determined that backup jobs are automatically set to run on a defined schedule.	No exceptions noted.
		ECI performs a nightly backup of the production data and backups are logged.	For a sample of days within the period, inspected the backup logs for the network and each production system and determined that data was successfully backed up. If a job failed, inspected the remediation steps.	No exceptions noted.
		Access to administering and scheduling backup jobs is restricted to authorized personnel.	Inspected the list of accounts with administrator access to Veeam and reviewed the listings with IT management and comparison to the Company's Organization Chart and determined that administrator access to Veeam was appropriately restricted to authorized personnel.	No exceptions noted.
		Restoration testing of backup data is performed on a quarterly basis.	For a sample of quarters within the period, inspected data restoration log and determined that data restoration test was performed successfully by management.	No exceptions noted.
		ECI maintains Incident Management Policy to identify root cause incidents and implement appropriate changes as necessary.	Inspected the Incident Response Policy to determine that management has a defined process to implement during a cybersecurity incident, including having a set response team, documentation requirements, and remediation efforts.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
Change Management				
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.	ECI uses a formal system development process in development/maintenance projects to guide programming personnel in the design, coding, testing and implementation of changes.	Inspected the Software Development Lifecycle Overview policy and determined that the policy has content to guide programming personnel during the design, coding, maintenance, development, testing, and implementation phases of changes.	No exceptions noted.
		Requests for changes are documented and approved by management prior to commencing work on the project/change.	For a sample of changes to the production environment throughout the period, inspected the corresponding IT support ticket and determined that the request and management approval of the change occurred prior to commencing work on the change.	No exceptions noted.
		Testing is performed in a separate QA/test environment by ECI prior to releasing into the client production environment.	For a sample of changes to the production environment throughout the period, inspected the corresponding IT support ticket and determined that the change was tested in a separate QA/Test environment prior to release into the client production environment.	No exceptions noted.
		System documentation is maintained by ECI and made available to personnel via the Company intranet.	Inspected system documentation for the production systems and determined that it is maintained by ECI on the company intranet and made available to ECI personnel.	No exceptions noted.
		Changes to the ECI client production environment are recorded and tracked.	For a sample of changes to the production environment throughout the period, inspected the corresponding IT support ticket and determined that each change was recorded and tracked in a ticket.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
		ECI rolls out changes to the client production environment upon approval of the appropriate IT management personnel.	For a sample of changes to the production environment throughout the period, inspected the corresponding IT support ticket and determined that approval of IT management personnel and/or Client Service Manager is documented prior to the change being migrated to the client production environment.	No exceptions noted.
		Final go live approval is required prior to the release update being applied to ECI's systems and applications. For high impact changes that meet established criteria, code review is required. These are performed by a peer programmer who does not have responsibility for the change.	For a sample of changes to the production environment throughout the period, inspected the corresponding IT support ticket and determined that there were proper segregation of duties between the person who approved the change and the person who migrated the change to the production environment. Inspected the list of accounts that have access to migrate changes to the production environment and determined that each account does not have the ability to develop code or approve changes.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
		Rollback procedures exist allowing the removal of changes, if necessary.	For a sample of changes to the production environment throughout the period, inspected the related documentation and determined that rollback procedures were included, if necessary.	No exceptions noted.
Risk Mitigation				
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Risk assessments are performed annually and upon implementation of any new technology that could impact the system and commitments. The risk assessment includes the analysis of threats and vulnerabilities to the system, ranks threats and vulnerabilities based of the level of risk, and Management determines risk acceptance or mitigation action plans as a part of the overall risk assessment.	Inspected the completed risk assessment to determine that it includes analysis of threat and vulnerabilities to the EDI and Billing System.	No exceptions noted.
		ECI uses insurance to augment and mitigate risk in alignment with the business continuity strategy.	Inspected the cybersecurity insurance policy to determine that ECI is actively insured against cyberattacks.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Risk assessments are performed annually and upon implementation of any new technology that could impact the system and commitments. The risk assessment includes the analysis of threats and vulnerabilities to the system, ranks threats and vulnerabilities based of the level of risk, and Management determines risk acceptance or mitigation action plans as a part of the overall risk assessment.	Inspected the completed risk assessment to determine that it includes analysis of threat and vulnerabilities to the EDI and Billing System.	No exceptions noted.
		ECI's subservice organization SOC reports are reviewed, documented and assessed for impact to ECI's control environment.	Inspected evidence of annual review over subservice organization's SOC reports performed by management's and determined that management review over the most recent subservice organization's SOC report was performed and implemented processes to monitor and/or resolve identified issues.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
Additional Criteria for Processing Integrity				
PI1.1	The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.	ECI maintains a procedural flow and a manual of technical requirements and that defines the EDI process.	Inspected the ECI Operations Manual and ECI Central Technical guide and determined that the EDI process is properly defined for ECI personnel. It was noted that the flow of the EDI process is defined within the technical guide.	No exceptions noted.
PI1.2	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.	ECI maintains a procedural flow and a manual of technical requirements and that defines the EDI process.	Inspected the ECI Operations Manual and ECI Central Technical guide and determined that the EDI process is properly defined for ECI personnel. It was noted that the flow of the EDI process is defined within the technical guide.	No exceptions noted.
		Data transmissions are monitored by ECI to ensure that transmissions are complete, accurate, and sent from authorized sources.	Observed the ECI NOC Team monitor inbound and outbound client transmitted batch processes within the examination period and determined that data transmissions occur through an automated process. For a sample of days within the period, inspected the Operations Task Lists and determined that inbound and outbound transaction processing issues occurring during the day are monitored documented to ensure transmissions are complete, accurate, and sent from authorized sources.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
		ECI utilizes the TrueTrack system to process transactions in accordance with its user entity agreements.	Observed ECI personnel utilize the TrueTrack system and determined that all Electronic Data Interchange transactions are actively monitored. For a sample of days within the period, inspected the Operations Task Lists and determined that the processing of transactions is performed as required within the inbound and outbound processing times stipulated in the user entity agreements. For a sample of inbound and outbound processing exceptions identified during the monitoring process throughout the period, traced the automatic error notification email sent to the IT department to a ticket within the ticketing system to ensure processing exceptions are assigned to operations for disposition.	No exceptions noted.
PI1.3	The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.	Data transmissions are monitored by ECI to ensure that transmissions are complete, accurate, and sent from authorized sources.	Observed the ECI NOC Team monitor inbound and outbound client transmitted batch processes within the examination period and determined that data transmissions occur through an automated process. For a sample of days within the period, inspected the Operations Task Lists and determined that inbound and outbound transaction processing issues occurring during the day are monitored documented to ensure transmissions are complete, accurate, and sent from authorized sources.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
		ECI utilizes the TrueTrack system to process transactions in accordance with its user entity agreements.	Observed ECI personnel utilize the TrueTrack system and determined that all Electronic Data Interchange transactions are actively monitored. For a sample of days within the period, inspected the Operations Task Lists and determined that the processing of transactions is performed as required within the inbound and outbound processing times stipulated in the user entity agreements. For a sample of inbound and outbound processing exceptions identified during the monitoring process throughout the period, traced the automatic error notification email sent to the IT department to a ticket within the ticketing system to ensure processing exceptions are assigned to operations for disposition.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
		Electronic data is monitored to ensure complete and accurate client data is stored on the production systems.	Observed the ECI NOC Team monitor processing activities on the TrueTrack system and determined that processing actions and problems highlighted by the system are identified. Inspected the Inbound and Outbound Operation Manuals that govern the integrity and version control client data files to confirm ECI maintains documented monitoring procedures for IT personnel. For a sample of days within the period, inspected the Operations Task Lists and verified that inbound and outbound transaction processing issues occurring during the day are documented to ensure transmissions are complete, accurate, and sent from authorized sources.	No exceptions noted.
PI1.4	The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to	At the completion of each day, the NOC performs the end-of-day process to close out the processing day and summarizes the results of inbound/outbound processing, TrueTrack Files and processing problems to senior management.	For a sample of days within the period, inspected the NOC end of day checklist and determined that the NOC processors update the checklist at the close of business each day to summarize inbound/outbound processing, TrueTrack files, and processing problems for senior management.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
	meet the entity's objectives.	Processing actions are monitored, and problems highlighted by the TrueTrack tracking system are identified and assigned to operations for disposition.	Observed the ECI NOC Team monitor processing activities on the TrueTrack system and determined that processing actions and problems highlighted by the system are identified. Observed the use of the UtiliPort system and determined that ECI can summarize processing results. For a sample of processing problems throughout the period, inspected the AcuTrack support ticket and determined that the problem was resolved, and the support ticket was appropriately closed by the ECI technical support personnel in a timely manner.	No exceptions noted.
		Electronic files received contain batch control totals. During the load processing data captured is reconciled to batch totals automatically by the applications. The reconciliation is reviewed daily by NOC Management.	For a sample of days within the period, inspected the NOC end of day checklist and determined that the NOC reviewed the daily batch total reconciliation.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
		Data transmissions are monitored by ECI to ensure that transmissions are complete, accurate, and sent from authorized sources.	Observed the ECI NOC Team monitor inbound and outbound client transmitted batch processes within the examination period and determined that data transmissions occur through an automated process. For a sample of days within the period, inspected the Operations Task Lists and determined that inbound and outbound transaction processing issues occurring during the day are monitored documented to ensure transmissions are complete, accurate, and sent from authorized sources.	No exceptions noted.
PI1.5	The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's object-ives.	ECI's backup management system is configured to automatically backup production data on a defined schedule.	Inspected the automated backup schedules for the network domain and each production system in Veeam and determined that backup jobs are automatically set to run on a defined schedule.	No exceptions noted.
		ECI performs a nightly backup of the production data and backups are logged.	For a sample of days within the period, inspected the backup logs for the network and each production system and determined that data was successfully backed up. If a job failed, inspected the remediation steps.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
		Backed up data is encrypted using the Veeam tool.	Inspected the settings from the Veeam backup system to determine that backed up data is encrypted.	No exceptions noted.
Additional Criteria for Confidentiality				
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	A confidentiality and non-disclosure statement is signed by all personnel during the onboarding process.	For a sample of new hires throughout the period, inspected their signed confidentiality agreement to determine if the new hire accepted the terms upon their on-boarding.	No exceptions noted.
		Information is defined into classification categories with associated retention periods. New data types are assessed when received and updated as needed.	Inspected the Data Classification Policy to determine that information is defined into classification categories.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
		Data retention procedures are in place to conform to confidentiality commitments and requirements.	Inspected the Confidentiality Policies and Procedures manual to determine that data deletion and destruction policies and procedures are defined.	No exceptions noted.
		New business partners and third party vendors are subject to nondisclosure agreements or other contractual confidentiality and privacy provisions prior to being contracted with.	For a sample of new business partners from within the period, inspected the signed confidentiality agreement to determine that appropriate confidentiality provisions were agreed to prior to the commencement of the relationship.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Paper forms received containing sensitive information are securely disposed of in shredders located throughout the office.	Observed the ECI office to determine that shredders are set up for the destruction of confidential data. Inspected the Confidentiality Policies and Procedures manual to determine that the use of shredders to destroy confidential data is required.	No exceptions noted.
		ECI has set requirements for retaining their backed up data.	Inspected settings from the Veeam system to determine that backups are retained for a set time.	No exceptions noted.
		Data disposal policies and procedures are in place to conform to confidentiality commitment and requirements.	Inspected the data disposal policy to determine that ECI has proper disposal processes in place to meet its confidentiality commitments and requirements.	No exceptions noted.

TSC Ref.	Trust Services Criteria for Security, Processing Integrity, and Confidentiality	Description of EC Infosystems, Inc.'s Controls	Marcum LLP's Tests of Controls	Results of Marcum LLP's Tests of Controls
		Data and software stored on equipment is confirmed to be removed and rendered unreadable prior to disposal.	Inspected the data disposal policy to determine that ECI has proper disposal processes in place to meet its confidentiality commitments and requirements. Inquired with Management and determined that there were no occurrences that would warrant the operation of the control during the examination period.	Control did not operate during the examination period.

vertexone™

www.VertexOne.net

Vertex Business Services Customer

January 5, 2022

Re: Comments on the Period Subsequent to the 2021 SOC 1 Examination Period

As you may know, Vertex Business Services acquired EC Infosystems as of November 1, 2021 after ECI had completed a SOC 1 Type II audit in October 2021. The examination period for that audit was October 1, 2020 to September 30, 2021.

The objective of this letter is to provide VertexOne (formerly EC Infosystems) clients and their external financial statement auditors with an update regarding the ECI services and the related controls included in the scope of the SOC 1 Type II audit report for the time that has elapsed since the date of VertexOne's acquisition (November 1, 2021) of EC Infosystems. Considering this, please be advised that the following statements are true to the best of our knowledge for the time between the conclusion of the acquisition and the date of this letter:

- There have been no events subsequent to the review period of the report that would have a significant effect on our assertion contained within the report.
- There have been no significant changes to our services or the underlying processes and/or systems since the conclusion of the review period.
- There have been no significant changes to our control objectives or the related control activities described in the SOC 1 Type II report since the conclusion of the review period.
- The control activities that govern our services have operated as described in the SOC 1 Type II report since the conclusion of the review period.
- There have been no significant changes to the complementary user entity controls necessary to achieve the control objectives as described in the SOC 1 Type II report.
- We are not aware of any significant operating or design deficiencies specific to the control activities described in the SOC 1 Type II report that have occurred since the conclusion of the review period.

If you have any further questions regarding this topic, please contact Mark Carde at mark.carde@vertexone.net.

Sincerely,

Mark Carde

Mark Carde
Chief Information Officer

IronHorse Power Services, LLC

Risk Management Policy

February, 2022

Date Issued:	Approved by: Peter Buell, Chief Executive Officer
	Name & Title: Peter Buell, Chief Executive Officer

TABLE OF CONTENTS

1. SUMMARY

PURPOSE OF THE RISK MANAGEMENT POLICY

The Policy defines IronHorse Power Services (IHPS) Commodity Risk Management guidelines, including:

- Objectives for Risk Management;
- Governance Structure;
- Portfolio approach; • Limits of Authority

The Policy applies to IHPS, its subsidiaries, employees, contractors, representatives, and agents.

RISK MANAGEMENT OBJECTIVES

IHPS is establishing the following Risk Management objectives:

- Clearly state our risk tolerances through Limits and policies;
- Enable achievement of desired ranges of profitability;
- Manage working capital liquidity; • Efficiently use allocated Collateral; and
- Optimize utilization of credit capacity.

RISK MANAGEMENT ACKNOWLEDGMENT

IHPS understands that many risks are inherent in its range of business activities, particularly concerning the contractual physical and financial Energy assets sensitive to short- and long-term commodity prices.

IHPS acknowledges that effective Risk Management cannot mitigate all risks. Risk Management is implemented as a framework to systematically identify, assess and provide a business approach for managing risks.

POLICY APPROVALS

IHPS ownership board ("Board") will review and approve the Policy at least annually.

From time to time, recommendations for policy changes and amendments might be put forth to the Board by the Risk Management Committee ("RMC") for approval.

Only the Board can approve expanded portfolio limits. The Board grants authority to the RMC to allocate and narrow portfolio limits.

Governance Structure

2.0 OVERVIEW OF GOVERNANCE STRUCTURE

This section serves to define and describe IHPS Governance Structure.

- IHPS Governance Structure is comprised of a three-tiered hierarchy, enhanced with checks and balances across business operations between the front, middle
- The IHPS Board;
- Risk Management Committee (RMC)
- COO – Risk Officer

2.11. BOARD OF DIRECTORS

The Board is accountable and responsible for Policy ratification.

The Board will receive position summaries of risk exposures, Risk Management activities,

The board may be asked to approve amendments to the Policy upon request from the COO between meetings.

2.2 RISK MANAGEMENT COMMITTEE

Risk Management Committee (RMC)

The RMC is a governance body that is accountable and responsible for risk oversight by monitoring policies and Limits, monitoring risk Exposure, and adopting policies, procedures, and measurements within the Policy's framework.

The RMC will meet monthly, or more frequently, as applicable.

RMC members are listed in Appendix A.1, "Risk Management Committee Members."

Responsibilities of the RMC are defined in Appendix B: "Roles and Responsibilities".

- Outside ." regularly scheduled meetings, members of the RMC may be called upon to respond to critical issues, opportunities, or concerns that are raised by the COO or RMC members.
- The attendance of the Chief Executive Officer and or President will be required for a quorum. If a quorum is not available and topics for a vote cannot be deferred, the COO has final decision authority.
- If a voting member cannot attend a committee meeting, they may provide their proxy to the CEO. This proxy shall be documented by an electronic email granting this authority from the party to the CEO.

2.3 Master Trading Contracts

Legal and Contract Administration will be jointly responsible for managing the preparation, review, and distribution of Master Agreements.

When applicable, the appropriate standardized industry agreement will be utilized, as determined by the legal department.

For all documented transactions under an agreement that is not an approved Master Agreement, legal department approval of the form of the contract or confirmation is required before execution.

FRONT OFFICE, MID OFFICE, AND BACK OFFICE

IHPS will maintain a system of independent checks and balances by segregating responsibilities and reporting lines with independent analysis, oversight, and reporting across business operations.

Business operations will be divided into three distinct functional areas, with independent reporting lines: Front Office, Mid Office, and Back Office.

2.4 Front Office - COO

The Front Office is responsible for managing all energy commodities within IHPS and asset-specific transactions and market entry or disposition strategies. This includes functions performed by the COO

2.4.1 Mid Office - CEO

The Mid Office is responsible for risk oversight, including any activities involving independent valuation, reporting, compliance, and governance.

Mid Office personnel may not execute any transactions.

2.4.2 Back Office - President

The Back Office is responsible for accounting and settlement functions related to commodity and financial accounting, transaction settlements, and external reporting.

Back Office personnel may not execute any transactions.

OVERVIEW

IHPS will manage the company's Commodity Risk, Interest Rate Risk, and Currency Risk Exposure by:

- Managing the Portfolio through Hedging and Portfolio optimization;
- Marketing Structured Products (Origination);
- Scheduling, dispatch, and fuel supply management with the ISO

PORTFOLIO MANAGEMENT

IHPS will centralize all Commodity Activities and Commodity Risk Exposure.

The Portfolio will be managed within the guidelines of the Policy.

3..1 Portfolio Structure for Energy Commodities

Risk Management for energy commodities, a portfolio will be established for all electric power positions, inclusive of all 3rd party transactions for portfolio hedging and optimization activities.

REC AND ANCILLARY exposure will be monitored and actively hedged within the portfolio as liquidity and position requirements present itself.

3..2 Managing Portfolio Risk of Energy Commodities

- The Front Office will manage all portfolios within the framework of the Policy with proper oversight by the Risk Organization.
- In order to minimize our basis delivery risk exposure, all retail pricing and hedging activity will be matched and performed at the ERCOT Load Zone.
- Any Hub transaction request by a prospective customer must be approved from members of the RMC as an exception to the rule and have protective language in our commercial agreement. Any exception position incurred are reported separately to the Shell team at all times.

OVERVIEW

Counterparty Credit Risk is inherent in IHPS Activities. IHPS is committed to receiving the credit sleeve approval before physical, financial trades are entered into.

CREDIT EXPOSURE

IHPS will monitor counterparty Credit Exposure daily and report counterparty Credit Exposure to the RMC on an as-needed basis, but no less frequently than quarterly.

TRANSACTION RESPONSIBILITIES

Credit personnel are responsible for reviewing counterparty Credit Exposure, proposed transactions, and managing the Authorized Trade List, as appropriate. The Front Office is responsible for confirming that all transactions conform to the Authorized Trade List or are otherwise approved by Credit before transacting.

CONTRACTUAL CREDIT TERMS

Credit is required to approve all credit terms included in all commodity contracts, including but not limited to Master Agreements

GENERAL OVERVIEW – Customer Pre-Enrolment

Credit Risk management is inherent as part of the business for a retail energy provider. The Ironhorse Power Services (IHPS) team are committed to proactive monitoring while protecting our investors from large inordinate exposure at any given time.

- All sales activity is mandated to receive an individual customer credit approval before any sale agreement or trade transaction are initiated.
- IHPS operations and enrolment team are responsible for managing the credit review process, while reviewing the credit worthiness of each prospective customer.
- The Front Office or sales team are responsible for obtaining all the basic information for proper evaluation purposes to obtain credit approval.
- IHPS enrolment team will manage the credit pass/fail and ID verification process with oversight provided by the COO. (Process flow chart - attached).
- IHPS will outsource services through external agencies to provide the following:
    - FICO score, American credit systems
    - ID verification platform
    - D&B credit scores
- Evaluations are performed on a pass/ fail basis. IHPS will reject any enrollment from non to poor credit level customers. We will not accept prepayments or deposits from prospective customers.
- A poor or non-rated prospect will require an over-ride release from the Sr. Leadership team (CEO, President, COO) in order to move forward as a enrolment.
- IHPS Risk team will monitor the overall counterparty and customer Credit Exposure daily and report counterparty Credit Exposure to the RMC on an as-needed basis, but no less frequently than quarterly.

Credit Operating- Monitoring Process

IHPS standard operating procedures will include proactive monitoring and reporting of any existing credit risk exposure. We will provide an internal rating scale to reflect the ongoing credit quality of each customer on a go forward basis. The scoring reflects the results of a timely payment history and length of service as a client. This will isolate the trouble accounts into grouping (4&5) and allow the IHPS team to focus efforts directly. This will improve communication between front – middle, and back offices on the collections effort and will result in the mitigation of losses and bad debt write offs.

- All successful closed sale transactions will receive an internal score ranging from 1 – excellent to 5 – poor (over-ride) or delinquent accounts.
- Accounts ratings will be evaluated and awarded based on their active payment history and time length as a paying customer with IHPS.
- Weekly proactive monitoring are given to accounts rated 4 to 5 which are expected to be less than three percent of our overall account receivable balances. The isolation will insure all internal and external collection efforts (as needed) are coordinated and implemented correctly .
- IHPS Risk team oversees and monitors all past due receivable reporting generated from the ECI billing - operations and accounting team on a consistent basis.
- Customer care will contact clients that are past due with a cutoff notice 15 days after the initial due date. The actual cutoff of service date will be 25 days total from the past due date.
- IHPS will outsource external collection efforts for accounts that are past due more than 25 days total past due and cut-off of service has been activated.

Disconnection Monitoring – Notice Process

In connection to Texas PUC rules and regulations governing retail operations, IHPS will discontinue, suspend or refuse service to any customer for the following reasons:

- Failure to pay a bill for electric service.
- Failure to comply with terms of any agreed to payment plan.
- For any other reason whereby IHPS is legally entitled to disconnect service with notice

Disconnection Notice communication

If the balance is not paid in full by the end of the day on the due date a disconnect notice will be issued within 15 days with the earliest disconnect date that occurs 10-12 days after the date of the DNP notice.

The customer may request a payment arrangement for up to a maximum of (5) days past the DNP date. A supervisor may approve a payment arrangement for a

maximum of (10) days past the DNP date.

A deferred payment plan may also be requested. The deferred payment plan requires a down payment of 50% of the past due amount, a supervisor may approve a down payment of 25%.

Per the terms of service agreement:

Disconnection of Your Electric Service: WE MAY REQUEST DISCONNECTION OF YOUR ELECTRIC SERVICE IF YOU DO NOT PAY YOUR DEPOSIT OR THE PAST DUE AMOUNT OF YOUR ELECTRIC SERVICE BILL IN FULL BY THE DUE DATE ON THE DISCONNECT NOTICE.

We will notify you before we disconnect electric service, as authorized by the PUCT. We may request disconnection of your electric service without prior notice immediately under specific situations, including the existence of a dangerous condition at your service address or theft of service.

If you receive a disconnection notice, we may also charge you a Disconnect Fee if you do not pay the past due amount before the date your service is subject to disconnection as stated in the disconnection notice. This charge will apply regardless of whether your electric service is actually disconnected.

Customer Account Updates: IHPS may also communicate with you through an Account Update process. At the time of enrollment with us, you must provide a valid mobile number that can accept text messages. Standard text messaging rates may apply as charged by your mobile phone service provider. By providing your mobile phone number, you authorize IHPS to have additional avenues to contact you using an automated dialer or via text messages.

MINIMUM REPORTING REQUIREMENTS

PURPOSE

Comprehensive, accurate, and timely reporting is essential to manage risk and assure compliance with the Policy. This section sets forth the minimum internal reporting requirements.

RISK REPORTS

Designated Reports will be circulated at a frequency and to recipients, as approved by the RMC.

Minimum guidelines for reporting and distribution include:

- Daily Reports:
- Cash flow forecast and P&L estimates
- REC requirements and Ancillary Exposure
- Mark to Market Profit and Loss Reports;
- Portfolio Position Reports;
- Transaction Reports;
- Counterparty Credit Exposure Reports.
- Weekly Reports
- Cash Flow Forecasts; and
- Collateral Outstanding.

APPENDIX A: COMMITTEE MEMBERS

A.1 RISK MANAGEMENT COMMITTEE

- Peter Buell CEO
- Clayton Isom – President
- James Brownlie – Board
- David E. Garcia – COO Risk

A.2 COMMITTEE RESPONSIBILITIES

The Risk Management Committee (RMC)

The RMC will perform the following duties:

- Approve IHPS Risk Management Framework and monitor related execution plans;
- Recommend changes to Limits and Risk Management Policy for Board approval; and
- Maintain minutes of RMC meetings and provide copies of these minutes to the Board upon request.

A.3 PORTFOLIO LIMITS

The Board approves IHPS Portfolio Limits. Only the Board can authorize expanded Limits.

The RMC can recommend new Limits or types of Limits to the Board for Board approval.

A.4 PORTFOLIO AGGREGATION

IHPS will aggregate all like risks regardless of the source of the risk (physical or financial) and managing the Net Position by commodity and across commodities, and limit structure

The overall limit structure is divided into the following areas:

- Limits of Authority; and
- The Net Open Position Portfolio Bandwidth Limit
- RECs and Ancillary positions

A.5 CASH MONTH REPORTING - MONITORING

- IronHorse shall, by the end of each week, review the latest near-term weather and load forecasts and update its hedge position for the upcoming week utilizing any combinations of authorized hedging products to fully mitigate any unhedged demand. Periodic reviews/audits will be performed.

- Energy Retailer's risk reporting to Shell will include pass/fail calculations against the deal's agreed risk limits.
- Each week Energy Retailer will provide a complete and detailed position report in a form reasonably acceptable to Shell Parties. This report must include a monthly break down of physical fixed price obligations, forecasted variable obligations with associated hedges and basis contract positions by market, zone and location. Periodic risk reviews of position reports will be performed. Energy Retailer will work to provide Shell with access to the Energy Retailer's trading risk system and to review these hedge positions.

A.6 REC – ANCILARY REPORTING - MONITORING

- REC requirements and Ancillary costs are key components of our retail cost of services and therefore merit the necessary oversight and reporting requirements to protect ongoing margins.
- The current and future value of REC's and Ancillary costs are actively updated on all current and future retail pricing proposals -evaluations as a standard operating procedure.
- The goal is to purchase REC's and Ancillary hedges regularly though-out the period as material positions are formed through retail activity growth. We are in the business of serving Retail load and we view this activity as a hedging requirement only to protect margins.
- Ironhorse will monitor and provide a monthly REC requirement position report (mandatory /voluntary) for all requirements incurred to date along with a forecast quarterly retirement projection.
- The REC report is currently active within the POWWR DFS risk management system and is updated daily for current enrolments. POWWR will work with approved brokers to facilitate REC acquisition with proper oversight provided by the Ironhorse risk team.
- All transactions will be position monitored as to position balance maintenance – exposure and the price position will be MTM and evaluated on a ongoing basis.

APPENDIX B: APPROVED RISK LIMITS

B.1 LIMITS OF AUTHORITY

These Limits are designed as a control mechanism; and are not intended to prevent appropriate transactions.

CEO Authority is only for delegation purposes if needed and not for the intention of an actual execution role.*

The Limits of Authority outlined below relate to transaction execution authority. The Signature Authority Limits Policy determines the authority to execute contracts on behalf of IHPS.

Net Open Position Bandwidth – Single trade notional and duration limit
Weather backcast normalized:

Contract Type	IHPS COO	
	Net Position	
	min	**max**
Fix priced	95%	105%

Variable priced	1-2 months out	75% Min	110%max
	3-4 months out	50% Min	110% max
	5-12 months	10% Min	50 %max
	13-18 months	0% Min	25% max

Electricity Notional Authority Limits					
Tier	**Indicative Title**	**Tenor**	**Notional Limits Per Transaction**		**Nominal Dollar Value of Transaction**
			Total MWHRS	**Total Bcf**	**Total $**
1	CEO*	Up to 5 years succeeding the current delivery month	200,000	N/A	20 MM
2	COO		100,000	N/A	10MM

APPENDIX C: ERCOT DRP – Disaster Recovery Plan

C.1 Summary

Ironhorse Power Services, LLC

Disaster Recovery Plan

Summary

We recognize a Disaster Recovery Plan (DRP) is a core component of a successful going concern plan as a Texas retail electric provider. Ironhorse Power Services (Ironhorse) has adopted best practices in vendor support and alternative work-digital file storing locations. We also plan in utilizing the latest technology sourced from today's "digital data cloud" and have adopted industry best practices in data migration, location, and backup procedures. Sourcing our information from the cloud also provides us the added security of working from home at any given time if the situation dictates

Ironhorse has diligently diversified our operational software risk by outsourcing key components of our operating platform. The daily operating process will include an active data migration and system backup between the various systems This will provide us added security and support with the addition of two locations to independently store and file data outside our internal infrastructure.

EC Infosystems will run our billing and payment collection systems. POWWR will run our risk and demand forecasting system. Both platforms will operate from their individual cloud accounts and both organizations have received a "Peak 10" rating for digital security. Both organizations have a proven track record of maintaining "best in class" security and operational run times.

Vital and daily communication with ERCOT and individual Texas utilities are supported by their individual web portals. Access has been verified and received from various locations outside the traditional office environment. Employee contact listings and phone communications are directed to various employee mobile devices.

Our DRP plan is divided up into the following categories

I. **Weather Events – back up the operational center(s)**
II. **Cyber Security – digital data backup procedures**
III. **Job Functional backup support**

I. Weather Events – back up the operational center(s)

Our current location of 5340 Alpha Road, Dallas Texas is a stand-alone building located on high ground off a major street in the North Dallas Galleria commercial district.

We have access to additional locations through our cloud hosting agreemnts

- EC Information – Billing platform Union(NYC) – New York
- POWWR Risk Management System – Newtown Conn.

Also our contract staff work out of those locations

Should access be restricted due to an unanticipated weather event or power outage, we will follow the plan below until access and power is fully restored.

a) **Work from home since all employees have laptop or desktop access to our cloud based operations.**
b) Meet through zoom or through Microsoft teams messaging when necessary
c) If the outage becomes extended, move operations to the following address;

1. **11120 - Russwood Cr Dallas Texas 75229**
2. **15892 Bearcreek PKWY, Redmond Wa 98052 (Backup Risk Facility – Cloud based)**

II. Cyber Security – digital data backup procedures

a) Ironhorse maintains current email and web cyber security software on all employee computers.
b) Ironhorse maintains a proactive digital data backup procedure in the cloud for our internal records.
c) Ironhorse will receive daily a backup file from our external software vendors which we will incorporate into our daily records
d) EC Infosystems and POWWR will maintain files and provide backup at their specific cloud locations.

III. Job Function and backup support all cloud based with backup locally and remote

a) Our key supporting software, ERCOT REP portal access, and individual Utility portals have primary and secondary login access.
b) Employees are cross trained on functions beyond their normal responsibilities and provide back up while team members are on vacation or out of the office.