



Filing Receipt

Received - 2022-04-18 08:39:29 PM
Control Number - 53385
ItemNumber - 501



IronHorse Power Services, LLC

Disaster Recovery Plan

April 15th, 2022

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



Ironhorse Power Services, LLC Disaster Recovery Plan

Executive 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.

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;

Ironhorse Power Services – Backup business locations

- 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. (see executive summaries below)



EC INFOSYSTEMS

2021 Network Security Overview

www.ecinfosystems.com

DEFENSE & MONITORING

EC Infosystems (ECI) utilizes Arctic Wolf, a premium security service provider used by many fortune 500 companies, as a key part of our Defense and Monitoring strategy. Arctic Wolf continuously monitors access to many ECI system resources including web servers, SFTP servers, file system resources and database systems.

ECI also utilizes Carbon Black, an advanced endpoint protection service, to detect malicious activity on every device that is part of the ECI network.

Arctic Wolf together with Carbon Black, analyzes events to detect and respond to security threats and take immediate preventive actions.

In addition, dedicated intrusion prevention hardware works in conjunction with advanced hardware fire walls to provide additional layers of defense.

HIGHLIGHTS

Continuous 24 X 7 X 365 monitoring

- Continuous 24 X 7 X 365 monitoring by the Arctic Wolf Security Operations Center (SOC).
- SOC provides an advanced log monitoring service in real-time.
- Reduction in false alarms and pin point correction areas.
- Slash the time required to detect and respond to detected threats.

Hardware Based Real Time Intrusion Prevention

Extensive Log Monitoring and Review

- Firewalls and Threat Detection Device Logs
- Critical server logs - Web / SFTP / Database Servers
- Windows Servers / Domain Controllers
- All Carbon Black Advance Threat Protection logs



PROACTIVE AND ADVANCED ENDPOINT PROTECTION

Carbon Black's advanced endpoint protection along with Avast's antivirus services provide a protective shell on each ECI attached device and endpoint. These systems utilize advanced machine learning algorithms to detect polymorphic threats and zero day malware, that are undetectable by traditional virus scanners. These systems operate in real time and immediately detect and block security threats, greatly improving system integrity, stability, and reliability.

HIGHLIGHTS

- Advance endpoint protection detects and prevents malicious behavior like taking over cached account credentials.
- Robust intrusion protection and threat intelligence stops threats proactively.
- Zero-day malware and scripts exploit detection and prevention.
- Advanced machine learning, self-healing protection systems.
- Complete device and endpoint protection under proactive real time shell.
- Quickly identify and respond to threats.

PENETRATION & VULNERABILITY TESTING

ECI utilizes SISA, an international cyber security service, to perform penetration and vulnerability testing to verify that all installed hardware and software security systems are operating effectively. Simulated cyber-attacks can detect new vulnerabilities caused due to operating environment changes like operating system patches, application changes and more. This extensive testing process assists with determining possible security gaps and allows ECI to make appropriate adjustments and improvements to our systems on a proactive basis.

HIGHLIGHTS

- Regularly scheduled penetration and vulnerability testing.
- Planning and mitigation of identified areas.
- Continuous improvements and strengthening of systems.
- Continuous improvements in processes and procedures.

ABOUT EC INFOSYSTEMS

EC Infosystems® is the leading provider of Billing/Customer Information Solutions (CIS) and Electronic Data Interchange (EDI) for clients in the deregulated energy industry. With over 20 years of experience, our company has a longstanding history of serving energy clients while also helping to shape the industry. We process transactions for over 6.7 million meters per month. We're a certified SSAE-16 (SSAE-18) compliant company.

© EC Infosystems, Inc. 2021

ec info**systems** INC

333 Earle Ovington Boulevard
Suite 102
Uniondale, NY 11553
Tel: (516) 874-8000

POWWR - Security Executive summary

POWWR®

Data Security, Backup and Disaster Recovery

Summary

DATA SECURITY

-  Firewall Protection
-  SSL Secure Socket Layer
-  IP White Listing
-  FTPS/SFTP (SSH File Transfer Protocol)
-  Data File Encryption

DISASTER RECOVERY

-  Daily incremental backups are performed both onsite and offsite
-  Backups include the entire server, operating system, applications and files
-  Quickly failover, or virtualize a server local or in the cloud from the full system image
-  Onsite recoveries take between 4 to 6 hours
-  Offsite recoveries take 24 hours to recover
-  Annual Validation Testing

DATA CENTER SECURITY

-  Secure co-location hosted by Flexential in Atlanta, GA
-  Guaranteed uptime, built in redundancies, professionals onsite 24/7
-  Built in resilience supported by 100 Gbps network backbone
-  Backup and recovery management
-  Certifications – SSAE 16 (Type II), ISO 27001, SOC 2 Type 2, SOC 3 Type 2, PCI DSS, HIPAA, Compliant, HITRUST CSF Certified
-  24/7 physical security monitoring and support
-  Cage perimeter security (surveillance cameras and card readers)
-  Electronic cabinet access device and user reports

© 2019 POWWR®

2

POWWR®

Data Security, Backup and Disaster Recovery

Certificates and Documentation

Click on the link of interest to view the actual certificate/document:

- SOC Compliance:
 - [2019-Type-2-SOC-1- ISAE-3402](#)
 - [2019-Type-2-SOC-2](#)
 - [2019-Type-2-SOC-3](#)
 - [Current-SOC-1-Bridge-Letter](#)
 - [Current-SOC-2-Bridge-Letter](#)
- Payment Card Industry (PCI) – Data Security Standard:
 - [Attestation for Compliance for Onsite Assessments – Service Providers](#)
- Additional Compliances:
 - [2019-Corp-ISO-27001-Re-Issue-Certificate](#)
 - [2019-ITAR-Final-Report](#)
 - [2019-FISMA-High-SAR](#)
 - [2019-HITRUST-Interim-Letter](#)

3



POWER[®]

Data Security, Backup and Disaster Recovery Standard Contract Provisions

5. Service Levels.

1. Service Availability. Subject to the terms and conditions of this Agreement, Provider will use commercially reasonable efforts to make the Services Available at least ninety-nine and one half percent (99.5%) of the time as measured over the course of each calendar month during the Term (each such calendar month, a "Service Period"), excluding unavailability as a result of any of the Exceptions described below in this Section 5.1 (the "Availability Requirement"). "Service Level Failure" means a material failure of the Services to meet the Availability Requirement. "Available" means the Services are available for access and use by Customer and its Authorized Users over the Internet. For purposes of calculating the Availability Requirement, the following are "Exceptions" to the Availability Requirement, and neither the Services will be considered un-Available nor any Service Level Failure be deemed to occur in connection with any failure to meet the Availability Requirement or impaired ability of Customer or its Authorized Users to access or use the Services that is due, in whole or in part, to any: (a) Customer Failure; (b) Customer's or its Authorized User's lack of Internet connectivity; (c) Force Majeure Event; (d) failure, interruption, outage, or other problem with any software, hardware, system, network, facility, or other matter not supplied by Provider pursuant to this Agreement; (e) Scheduled Downtime; or (f) disabling, suspension, or termination of the Services pursuant to Section 2.6.
2. Scheduled Downtime. Provider will use commercially reasonable efforts to: (a) schedule downtime for routine maintenance of the Services between the hours of 9:00 pm Friday to 6:00 am Monday EST; (b) give Customer at least 48 hours prior notice of all scheduled outages of the Services; and (c) maintain weekly maintenance of the Services between the hours of 12:01 am to 8:00 am every Sunday ("Scheduled Downtime").
3. Service Support. The Services include Provider's standard customer support services ("Support Services") in accordance with the Provider service support schedule attached as Exhibit C.

7. Security.

1. Provider Systems and Security Obligations. Provider will employ security measures in accordance with Provider's data privacy and security policy as amended from time to time, a current copy of which is available at <http://www.escoware.com/privacy-policy>, and which is herein incorporated ("Privacy and Security Policy").
2. Data Breach Procedures. Provider maintains a data breach plan in accordance with the criteria set forth in Provider's Privacy and Security Policy and shall implement the procedures required under such data breach plan on the occurrence of a "Data Breach" (as defined in such plan).
3. Access and Security. Customer shall employ all physical, administrative, and technical controls, screening, and security procedures and other safeguards necessary to: (a) securely administer the distribution and use of all Access Credentials and protect against any unauthorized access to or use of the Services; (b) control the content and use of Customer Data, including the uploading or other provision of Customer Data for Processing by the Services; (c) select and train appropriate individuals to use the Services; and (d) abide by all applicable Law, including but not limited to those related to data privacy, communications, and the transmission of technical or personal data.



III. Job Function and backup support all cloud based with backup locally and remotely by our Data Vendors -POWWR and EC Information

- a) We have an experience CTO that manages our IT staff on a daily basis.
- b) Our key supporting software, ERCOT REP portal access, and individual Utility portals have primary and secondary login access.
- c) 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.



REPORT ON

EC INFOSYSTEMS, INC.'S

DESCRIPTION OF ITS ELECTRONIC DATA INTERCHANGE (EDI)
AND BILLING SYSTEM OUTSOURCE SERVICES SYSTEM AND ON
THE SUITABILITY OF THE DESIGN AND OPERATING
EFFECTIVENESS OF ITS CONTROLS THROUGHOUT THE PERIOD

OCTOBER 1, 2020 TO SEPTEMBER 30, 2021



EC Infosystems, Inc. – SOC 1 TYPE II TABLE OF CONTENTS

Acronym Table	i
Section 1: Assertion of the Management of EC Infosystems, Inc.	1
Section 2: Independent Service Auditors' Report	5
Section 3: EC Infosystems Inc.'s Description of its Electronic Data Interchange (EDI) and Billing System Outsource Services System	10
Section 4: EC Infosystems Inc.'s Control Objectives and Related Controls and Independent Service Auditors' Tests of Controls and Results Thereof	26
Introduction.....	27
Control Environment	27
Testing Approach.....	28
Sampling Approach	28
Testing Matrices	29
Change Development (Change Management)	29
Change Migration (Change Management).....	30
Physical Access.....	31
Logical Access (ECI Network).....	32
Logical Access (Client Access)	34
Logical Access (Network Security)	35
Computer Operations (Backup and Recovery)	36
Computer Operations (Batch and Online Processing)	37
Computer Operations (Process Activity Monitoring).....	38
Data Transmissions	39
Recording of Transactions	40
Client Issues Tracking.....	41
Client Data Integrity	42
Client Output Documents	43
Section 5: Other Information Provided by EC Infosystems, Inc.	44

Acronym Table

➤ AICPA	American Institute of Certified Public Accountants
➤ AMI	Advanced Metering Infrastructure
➤ EDI	Electronic Data Interchange
➤ FTP	File Transfer Protocol
➤ HR	Human Resources
➤ IT	Information Technology
➤ IP	Internet Protocol
➤ IS	Information Security
➤ NOC	Network Operations Center
➤ QA	Quality Assurance
➤ SFTP	SSH File Transfer Protocol
➤ SLA	Service Level Agreement
➤ SOC	System and Organizational Controls
➤ SSL	Secure Socket Layer
➤ SSO	Single Sign-on
➤ USPS	United States Postal Services



Section 1: Assertion of the Management of EC Infosystems, Inc.

Assertion of the Management of EC Infosystems, Inc.

We have prepared the description of EC Infosystems Inc.'s ("EC Infosystems" or "ECI") Electronic Data Interchange (EDI) and Billing System Outsource Services system entitled "EC Infosystems Inc.'s Description of its Electronic Data Interchange (EDI) and Billing System Outsource Services System" for processing user entities' transactions throughout the period October 1, 2020 to September 30, 2021 (description) for user entities of the system during some or all of the period October 1, 2020 to September 30, 2021, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

EC Infosystems uses a subservice organization for colocation data center hosting services. The description includes only the control objectives and related controls of EC Infosystems and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by EC Infosystems can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls at EC Infosystems. The description does not disclose the actual controls at the subservice organizations.

The description also indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of EC Infosystems' controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

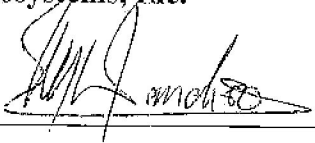
We confirm, to the best of our knowledge and belief, that:

- a. The description fairly presents the EC Infosystems' Electronic Data Interchange (EDI) and Billing System Outsource Services system made available to user entities of the system during some or all of the period October 1, 2020 to September 30, 2021, for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:
 - i. Presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable:
 - (1) The types of services provided, including, as appropriate, the classes of transactions processed.

- (2) The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.
 - (3) The information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
 - (4) How the system captures and addresses significant events and conditions other than transactions.
 - (5) The process used to prepare reports and other information for user entities.
 - (6) Services performed by a subservice organization, if any, including whether the inclusive method or the carve-out method has been used in relation to them.
 - (7) The specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the controls.
 - (8) Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.
- ii. Includes relevant details of changes to the Electronic Data Interchange (EDI) and Billing System Outsource Services system during the period covered by the description.
 - iii. Does not omit or distort information relevant to the system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors and may not, therefore, include every aspect of the Electronic Data Interchange (EDI) and Billing System Outsource Services system that each individual user entity of the system and its auditor may consider important in its own particular environment.
- b. The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period October 1, 2020 to September 30, 2021, to achieve those control objectives if the subservice organizations and user entities applied the complementary controls assumed in the design of EC Infosystems' controls throughout the period October 1, 2020 to September 30, 2021. The criteria we used in making this assertion were that:
- i. The risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization.
 - ii. The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

- iii. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

EC Infosystems, Inc.

A handwritten signature in black ink, appearing to read 'Mohan Wanchoo', is written over a horizontal line.

Mohan Wanchoo, President & CEO

12/23/2021

DATE

Section 2: Independent Service Auditors' Report



Independent Service Auditors' Report

To: Management of EC Infosystems, Inc.

Scope

We have examined EC Infosystems Inc.'s ("EC Infosystems" or "ECI") description of its Electronic Data Interchange (EDI) and Billing System Outsource Services system entitled "EC Infosystems Inc.'s description of its Electronic Data Interchange (EDI) and Billing System Outsource Services System" for processing user entities' transactions throughout the period October 1, 2020 to September 30, 2021 (description) and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in the "Assertion of EC Infosystems Inc.'s Management" (assertion). The controls and control objectives included in the description are those that Management of EC Infosystems believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Electronic Data Interchange (EDI) and Billing System Outsource Services system that are not likely to be relevant to user entities' internal control over financial reporting.

EC Infosystems uses a subservice organization for colocation data center hosting services for their Electronic Data Interchange (EDI) and Billing System Outsource Services system. The description includes only the control objectives and related controls of EC Infosystems and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by EC Infosystems can be achieved only if complementary subservice organization controls assumed in the design of EC Infosystems' controls are suitably designed and operating effectively, along with the related controls at EC Infosystems. Our examination did not extend to controls of the subservice organizations and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of EC Infosystems' controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In Section 1 of this report, EC Infosystems has provided an assertion about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. EC Infosystems is responsible for preparing the description and assertion, including the completeness, accuracy and method of presentation of the description and assertion; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives; selecting the criteria stated in the assertion; and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period of October 1, 2020 to September 30, 2021. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Performing procedures to obtain evidence about the fairness of the presentation of the description of the system and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion.
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.

- Evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in section 4.

Opinion

In our opinion, in all material respects, based on the criteria described in EC Infosystems' assertion:

- a. The description fairly presents EC Infosystems' Electronic Data Interchange (EDI) and Billing System Outsource Services system that was designed and implemented throughout the period October 1, 2020 to September 30, 2021.
- b. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2020 to September 30, 2021 and the subservice organizations and user entities applied the complementary controls assumed in the design of EC Infosystems' controls throughout the period October 1, 2020 to September 30, 2021.
- c. The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period October 1, 2020 to September 30, 2021, if the complementary subservice organization controls and user entity controls assumed in the design of EC Infosystems' controls operated effectively throughout the period October 1, 2020 to September 30, 2021.

Restricted Use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of EC Infosystems, user entities of EC Infosystems' Electronic Data Interchange (EDI) and Billing System Outsource Services system during some or all of the period October 1, 2020 to September 30, 2021, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about the controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than those specified parties.

Marcum LLP

Marcum LLP

December 23, 2021
New Haven, CT 06511

Section 3: EC Infosystems Inc.'s Description of its Electronic Data Interchange (EDI) and Billing System Outsource Services System

OVERVIEW OF OPERATIONS

EC Infosystems, Inc. is a New York based corporation that provides Electronic Data Interchange (EDI) and Billing System Outsource Services. From data that is inputted by users primarily in the energy industry, ECI's system processes transactions for user entities ("clients" or "customers") through its EC Central, UtiliPort, UtiliBill, and TrueTrack proprietary applications ("production systems" or "systems"). The user entities are securely connected to ECI's proprietary software platform via the web. The system applications enable user entities access to the system in real time while allowing ECI operating personnel to manage and monitor the transaction processing functions. This allows errors and problems to be resolved promptly in real time. Client transaction reports, including bills from the system, are available to them in real time. Clients are able to bill utility customers directly; therefore, ECI is not involved in the collection of the payments for utility users. ECI provides services through the following organizational elements:

Executive Department - Serves as management of the processing operations. This department has the ultimate responsibility for administration of the operations. The department interacts with customer managers and is responsible for performance measurement, and compliance with the policies and procedures, government rules and regulations, legal governance, and user agreements. It ensures that the operation is ethical and promotes integrity; transparency and accountability with all transactions and establishes operation controls to monitor the system through various levels of management.

Operations Department – Performs transactions processing operations twenty-four hours a day, three hundred and sixty-five days a year. EDI transaction processing is performed through ECI's processing facility to ensure transactions are processed accurately from data input online by user entities. This department monitors and interacts with the Executive Department and the Information Systems Department and responds to user requests and investigations during business hours.

The supervising personnel are supported by staff personnel and are responsible for ensuring that the processing protocols are effectively carried out in the processing of client data including the monitoring of all transaction processing activities. The Network Operating Center (NOC) is part of the Operations Department and provides assurance that the network infrastructure and activities are authorized and that the application-processing services provided by ECI are both timely and accurate.

Information Systems Department - This department provides the required support to maintain and operate the systems environment. It includes the computer operations, systems and programming, system software support, Quality Assurance ("QA") personnel to test system changes, and infrastructure functions. This department interacts with the Operations Department



to provide any required client support services. The Information Systems Department is also responsible for providing application development services related to the ECI production systems.

Hardware/System Software Infrastructure

The EDI and Billing System Outsource Services are processed through the following proprietary applications:

Application	Description
UtiliBill	<p>Allows clients to manage customers, generate bills, and manage Accounts Receivable (A/R) and Accounts Payable (A/P) functions. UtiliBill is a scalable system that allows the setup of residential customers as well as large Commercial and Industrial (C&I) National Accounts. This system is designed to accommodate clients operating in multiple states and different billing scenarios for both residential and large C&I customers.</p> <p>UtiliBill makes information readily available to clients and provides a wide range of reports that help the client manage their business operations. Clients can choose to personalize their reports to give them the look and feel they desire.</p>
EC Central	<p>This is the base application available for ECI clients to submit transactions to the proper partner as needed. The application provides the basic data entry screens to enable the submission of data from energy marketers to utilities and vice versa.</p>
TrueTrack	<p>Tracking system/application that provides tracking of all inbound and outbound transactions processed on the various EDI systems. This system provides for verification of successful transmission and receipt of transactions. TrueTrack provides inbound and outbound reporting, displaying successfully processed transactions as well as exceptions which require immediate attention.</p>
UtiliPort	<p>Provides enhanced functionality over the TrueTrack application and allows ECI clients to monitor all transactions flowing through the EDI Transaction Management system and see customer activity information in an easy to track web portal. It helps clients to view their transactions at an overall level and enables them to drill down to the individual transaction level.</p> <p>UtiliPort allows clients to monitor events that need immediate attention and track a customer's enrollment process with a utility in detail.</p> <p>As part of this system, clients are provided with information that enable them to manage their day to day business functions. The system lists certain time sensitive action items that need to be performed on an immediate basis. It also gives the clients various Exception Reports and Standard Reports.</p>

All of the above production systems are homegrown applications (proprietary software platforms accessed via the web-based .NET framework) that process the data and transactions on behalf of ECI's clients.

To support their clients, ECI maintains a network of personal computers and servers and uses programs built for its data outsourcing system. The system consists of multiple components including servers, disk, a firewall (SonicWALL), and network switches. The servers are supported by a combination of Microsoft Windows Server 2012R2, 2016 and 2019. The workstations are running Windows 10.

OVERVIEW OF INTERNAL CONTROL

The following is a description of the five components of internal control, which include the control environment, risk assessment process, information and communication, monitoring, and control activities.

Control Environment

The control environment sets the tone at the top of an organization, fostering an awareness of internal control within its employees. It is the building block for all other components of internal control. ECI's control environment represents the collective effort of various elements in establishing the effectiveness of its operations. Such factors include the following items:

Integrity and Ethical Values: Organization values and behavioral standards have been established by senior executive management. These values and standards are communicated to all personnel through policy statements and manuals. All employees must acknowledge, in writing, that they have received any policy manuals distributed, and that they are expected to read and abide by the policies.

Commitment to Competence: The Human Resources ("HR") policies and processes of ECI are designed to: (1) identify and hire competent personnel, (2) provide employees with the training and information they need to perform their jobs, (3) evaluate the performance of employees to verify their ability to perform job assignments, and (4) through the performance evaluation process, identify opportunities for growth and job performance improvement. The HR function is responsible for the initial recruiting and evaluation of job applicants, which can include pre-screening interviews in accordance with ECI'S policies. The HR function then schedules interviews with supervisors and management of the departments, as appropriate, to perform final interviews and to make the final hiring decisions.

Management's Philosophy and Operating Style: ECI senior executives believe that ECI's clients, employees and the public are best served by a senior executive team that is highly involved in the day-to-day operations of the organization, while giving employees the authority they need to

properly serve their clients. Department managers are encouraged to address developing issues and risks proactively to minimize their impact on the organization and its clients.

Organizational Structure: The organizational structure of ECI, which provides the overall framework for planning, directing and controlling operations, uses an approach whereby personnel and business functions are segregated into departments according to job responsibilities. This approach allows the organization to clearly define responsibilities, lines of reporting and communications, and allows employees to focus on the specific business issues impacting their operations.

Authority and Responsibility: Lines of authority and responsibility are clearly established throughout the organization and are communicated through ECI: (1) management's philosophy and operating style, (2) organizational structure, (3) employee job descriptions, and (4) policy and procedure manuals.

Human Resources: In addition to the function described above, Human Resources is also responsible for (1) assisting senior executives in establishing human resource policies, (2) assisting employees with employment and benefit issues, (3) supporting the supervisors and managers of all ECI operating departments in their roles overseeing employees, and (4) supporting organization compliance with employment laws and regulations. The Human Resources function has developed an Employee Handbook that outlines many Human Resources policies. New hires must acknowledge, in writing, their understanding that they are expected to read and abide by the policies outlined in the manual. The manual is updated as needed and updated policy statements are distributed as appropriate. A comprehensive review of all policies and procedures is performed approximately once per year.

Reference validation is conducted for new hires and background checks are performed when needed. Training of personnel is accomplished through supervised on-the-job training, outside seminars, and in-house classes. Certain positions require the completion of specialized training. Management is responsible for ensuring that all personnel complete such training. Department managers are also responsible for encouraging the training and development of employees on an ongoing basis.

Risk Assessment Process

An entity's risk assessment process is its identification, analysis, and management of risks relevant to user organizations. ECI has placed into operation a risk assessment process to identify and manage risks that could affect its ability to provide reliable services to its clients. This process requires management to identify significant risks inherent in the EDI and Billing System Outsource Services processes outlined in this document and relied on by user organizations and to implement appropriate measures to monitor and manage these risks. This process has facilitated the

identification of various risks inherent in ECI's operating environment and ECI's management has developed and implemented reasonable measures for the ongoing management and mitigation of these risks. The risks considered by ECI management on an ongoing basis include:

- Operational and Cyber risk associated with computerized information systems; manual interface in the processes involved in transaction processing; and external systems for client system interfacing.
- Processing risk associated with, among other things, unresolved errors in the system that are then reflected in users billing.
- New legislation and the regulatory environment
- Competitive landscape
- Management conducts an assessment of risk of material misstatement as it relates to achieving control objectives for user entities. Management has implemented various measures to manage risks identified through the risk assessment process.

Information and Communication

Information and communication systems support the identification, capture, and exchange of information in a form and timeframe that enable people to carry out their responsibilities. The information system consists of procedures, whether automated or manual, and records established to initiate, record, process, and report entity transactions (as well as events and conditions) and to maintain accountability. The quality of system-generated information affects management's ability to make appropriate decisions in controlling the entity's activities.

To help align ECI's strategic and tactical decision making with operating performance, management is committed to maintaining effective communication with all personnel. Information comes from both inside and outside the organization and is used to guide ECI strategic and tactical decision making as well as to measure performance. External communications originate from a number of sources, take many forms such as e-mail and website postings, and are distributed to a number of destinations. ECI management has focused on establishing multiple channels of external communications to facilitate timely and appropriate communications in an ongoing manner. ECI management monitors internal and external communications on an ongoing basis to assess the effectiveness of these communications.

Monitoring

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changes in conditions. The management and supervisory personnel of ECI monitor performance quality and control operations as a normal part of their activities. ECI has implemented a series of "key indicator" management reports that measure the results of various processes involved in providing transaction processing to customers. Key indicator reports identify the causes of differences noted in the reconciliation process and

provide for investigation of any deviations of the computerized information system relative to the EDI and Billing System. Daily processing tickets processed through the system are highlighted in the system and are notated by users. The tickets are summarized in real time on screens that are reviewed by staff, investigated and resolved promptly using a three-level application.

Exception reports are proactively and regularly reviewed depending on the nature of the item being reported on by appropriate levels of personnel, and actions are taken as necessary. Major exceptions, if any, are referred to higher levels of systems' personnel for review. Users are informed of the disposition of any problems and the system keeps track of the investigation process.

Adherence to EDI and Billing System controls is monitored through a self-assessment program that is overseen by three levels of personnel and the Executive Management team to ensure compliance of policies and procedures. The assessment program has been designed to periodically evaluate administration and support operations for compliance within ECI's controls. The assessments also include conducting a Change Control Meeting process and performing daily and weekly reporting to ECI management. Management has established measures to prevent unauthorized access to or destruction of documents and records. Management exercises reasonable control over operations so that there is an absence of crisis and critical conditions. ECI has employed the services of programmers that have effectuated a high degree of centralized transaction processing and controls.

ECI IT management monitors their subservice organization through performing an annual review of the subservice organization's SOC reports and performing periodic site visits to the subservice organization facility. Refer to the "Physical Access" section below for additional details on ECI's subservice organization.

ECI IT monitors network performance and resources via SolarWinds and other monitoring tools; reports are produced for appropriate levels of personnel and actions are taken as necessary. In addition, the ECI IT and security team use Manages Security Services from ArticWolf to prevent and respond to cyber security and in house security threats quickly.

Monitoring of the Subservice Organization

ECI uses Webair, a subservice organization, to provide colocation data center hosting services. On an annual basis the subservice organization provides a SOC 2 report which ECI personnel review. In addition, during the year, ECI personnel make several visits to Webair to observe that procedures are being followed and determine if there are any issues to be discussed. If issues over physical security, environmental controls or backup storage is identified by Webair, an Exception report is communicated to ECI.

Control Activities

Control activities are the policies and procedures that help ensure that management directives are carried out. They help ensure that necessary actions are taken to address risks to the achievement of the entity's objectives. Control activities, whether automated or manual, have various objectives and are applied at various organizational and functional levels.

All departments are required to implement control activities that help assure the achievement of business objectives associated with: (1) the reliability of financial reporting, (2) the effectiveness and efficiency of operations, and (3) compliance with applicable laws and regulations. These control activities are designed to address the specific risks associated with the operations and are reviewed annually as part of the risk assessment process. ECI has developed formal policies and procedures covering various financial and operational matters to document the requirements for performing many of these control activities.

Specific control activities are provided under the *Control Environment* section, the *Information Technology Processes and General Controls* section, the *Transaction Processing and Controls* section, and in *Section IV—Description of EC Infosystems Inc.'s Control Objectives and Related Controls, and Independent Service Auditors Tests of Controls and Results of Tests*.

The next section of this report contains the following descriptions of ECI's control procedures. These control procedures are the responsibility of ECI and ECI's management. ECI's management is responsible for the design and implementation of the control procedures necessary to achieve these objectives.

INFORMATION TECHNOLOGY PROCESSES AND GENERAL CONTROLS

Application Development

ECI uses a formal system development process in development/maintenance projects to guide programming personnel in the design, coding, testing and implementation of changes. The policy describes the process through the following development phases:

1. Initiation
2. Feasibility Analysis
3. Requirements Definition
4. Design
5. Development
6. Testing
7. Release to Production
8. Ongoing Maintenance

Requests for changes are documented and approved by ECI management prior to commencing work on the project/change. Requests can come from a variety of sources including clients and from internal ECI initiatives. Potential requests are recorded in the custom-developed AcuTrack ticketing system which is used to document the request and includes the following information:

1. Origination of the request
2. Purpose of the request (definition of the problem and how it originated)
3. Time frame for completing the request
4. Priority level (i.e., Critical (Billing or Invoice), Compliance, Nice to Have)

Once a project is approved, it enters the requirements definition, design and development phases to move the project through the system development process. Microsoft Project tool is used for tracking the project through these phases.

Testing is performed in a separate QA/test environment by ECI prior to releasing into the client production environment. The testing phase is designed to demonstrate that the production system conforms to the requirements as specified in the functional requirements document. The code will be tested by QA staff producing to verify that the proper level of testing was performed. The level of testing depends on the complexity of the change and includes, but is not limited to, system testing, integration testing, regression testing, performance testing, automation testing, and user acceptance testing.

System documentation is provided by and is maintained by ECI. This documentation is updated on a periodic basis or whenever a major change is implemented that supersedes the information on the old documentation.

Change Management

All changes to the ECI client production environment are recorded and tracked. ECI uses Microsoft Project and Accutrack system to track the status and progress of each change request.

ECI rolls out changes to the client production environment upon approval of the appropriate IT management personnel. Changes are discussed and approved during a weekly change control and management meeting that is attended by IT personnel, Client Service personnel, and Project Management personnel. Each change control meeting reviews any changes from the prior week, discusses any changes approved but not implemented from the prior week, and approves new changes for the current week. The results of these meetings are documented in a change management spreadsheet containing a history log of the updates and maintained on ECI's SharePoint portal.

Segregation of duties exists such that the person approving the change to the client production environment is not the same person who is responsible for implementing the change to the client production environment.

Rollback procedures exist to allow the removal of changes, if necessary.

Physical Access

ECI uses Webair (“subservice organization”), a co-location data center facility to host ECI’s production servers and provide backup storage services. The subservice organization is located in Garden City, NY. The subservice organization provides physical security, rack space, power (including battery and generator power), internal/external communication connections and cooling.

There is an access control system at the subservice organization that controls access to the IT equipment. ECI identifies and authorizes appropriate personnel having access to the subservice organization facility.

Logical Access

An overall Information Security Policy is maintained by ECI. This policy details ECI’s security framework and the expectations of its employees in relation to maintaining a proper information security program.

Access to administer the network and production systems is restricted to authorized personnel. In the ECI environment, this role is limited to the Systems Administrators (SA), who are members of the Information Systems Department, and work as network, systems, and database engineers/administrators.

There is a process for assigning, modifying, and removing user access to the network and production systems. Once a new employee is hired, HR is notified of hiring including role and start date. HR will notify the Information Systems Department who will setup the new user on the production system(s) that they require to perform their job function. The process for terminating or modifying user access follows a similar process.

ECI uses an authentication access system to promote only authorized users. ECI and client users require a user ID and password in order to gain access to the production systems. In addition, users must connect via an authorized IP address so as to prevent unauthorized users from accessing the network and production systems from non-client locations. This is controlled by a combination of the user ID and password and the use of Secure Socket Layer (SSL) certificates to encrypt the user sessions via the web. ECI has implemented authentication controls to prevent ECI clients from accessing records they are not authorized to view.

ECI has developed defined username and password standards for access to the ECI network domain (“network” or “domain”). Each network user has a unique user ID. The domain password standards enforce the following (but are not limited to): unique user name, a minimum password length of 10 alpha/numeric characters with password complexity enforced; a limit of 5 unsuccessful access requests (keyed to valid user name) before the ID is suspended for 30 minutes, and a password change interval of 52 days.

Network infrastructure includes firewall protection and is monitored for unauthorized access attempts. The firewall also performs real-time intrusion prevention and detection at all different locations in the network.

Anti-virus protection is in use throughout the ECI environment and systems are kept up-to-date with recent signature files. Windows-based computers (clients and servers) connected to the ECI computer network use the AVAST anti-virus protection software and Carbon Black.

The network and production systems are configured with patches and upgrades applied. Available updates are evaluated for compatibility in the ECI environment by testing them in the staging environment to ensure they are compatible and reliable prior to installing them into the production environment. For workstations, Windows Update Server, third-party tool and group policy facility are used to centrally download and distribute patches.

Computer Operations

ECI performs incremental, differential and full backups of each of its production systems. Access to administer and schedule backup jobs is restricted to authorized ECI personnel. Restoration testing of backup data is performed on a quarterly basis.

ECI utilizes reputable and reliable backup solutions to perform backups. Currently it is utilizing Veeam Backup & Replication software. Through its respective management console and/or dashboard, ECI personnel schedules, tracks and monitors production system backups.

Access to production (job scheduling) processing control language and executable programs is defined to restrict the ability to execute, modify, delete or create to appropriate individuals. This function is limited to the NOC personnel. Business significant and critical job processing is monitored by ECI to ensure successful and timely completion, including a review and resolution of any exceptions. Processing problems are recorded and resolved by the technical support personnel.

TRANSACTION PROCESSING AND CONTROLS

Data Transmissions

Data transmissions are monitored by ECI to ensure that the transmissions are complete, accurate, received on a timely basis, and sent from authorized sources. The NOC is responsible for monitoring the data transmissions sent in from ECI clients. The NOC is staffed from 7am to 7pm Monday through Friday. The NOC uses automated tools to check data transmission files for accuracy, completeness, and conformity with prescribed data file layouts. Any errors are identified, and follow-up actions are taken to correct the noted issues.

Recording of Transactions

Client files are received, processed, and sent back out during the processing day. The NOC is responsible for monitoring the processing environment. The TrueTrack tracking system is designed to achieve complete and timely processing based on the executed agreement in place.

At the completion of the day, the NOC performs the end-of-day process to close out the processing day. At the completion of this process, the NOC sends an end-of-day e-mail to the ECI President and the Associate Director of Information Systems, containing the Operations Task List that summarizes the days processing and includes the following information:

1. Results of Inbound Daily Processing
2. Results of Outbound Daily Processing
3. Summary of Ad-hoc Processes
4. TrueTrack File Issues (if any)
5. Any other processing problems during the day

The results of this e-mail are reviewed by the ECI President and the Associate Director of Information Systems and any processing instructions for the following day are communicated to the NOC to resolve any issues.

Client Issue Tracking

Processing actions are monitored, and problems highlighted by the system are identified on a timely basis and assigned to operations for effective disposition. Any client related issues are recorded in AcuTrack and include the client name, a description of the issue, the severity of the issue, and who was assigned to resolve the issue. Any actions taken by ECI are also recorded on the ticket. Once the issue is resolved, the ticket is closed, and the date of the closure is noted on the ticket.

Any critical issues are discussed during a weekly management meeting to review the issue, the cause of the issue, and any steps taken to resolve the issue.

Client Data Integrity

Complete and accurate electronic data is maintained on file for each user with the proper version of the data files. Client files are sent via a File Transfer Protocol (“FTP”) tool, a standard network protocol used for the transfer of computer files between the client and ECI servers, at various times during the day. Once the files are received, they are downloaded approximately every 15 minutes and deposited in a staging directory to await processing by the system.

As each file is processed, the system checks for any errors in the file. If any errors are found, there is a notification of the error on the NOC console as well as any e-mail that is also sent to the NOC operations staff. The error is researched by the NOC personnel and any corrective action, such as calling the client or resubmitting the data file, is undertaken.

Once the file has been successfully processed, it is automatically moved to an archive directory so that 1) the staging area can be “cleaned” for the next batch of files, and 2) ECI can maintain a history of file submissions. In addition, the file processing activity can also be viewed on TrueTrack once the file is processed.

Client Output Documents

Client documents are distributed to clients in an electronic format and only authorized recipients may obtain the information. Client output is available via several electronic formats using FTP and EC Central, TrueTrack, UtiliBill and UtiliPort (“production systems”). The location of the output information is dependent on the nature of the transaction and the level of service that the client has subscribed to from ECI. Users must execute a Customer Agreement that outlines specific processing needs. The client output file process is documented by the completion of the Operations Task List.

For each output service, ECI has provided security mechanisms that can be used by clients to control access to the output information. For FTP, this can be an ID and password that controls access to the FTP site. For production systems, this includes an ID, a password and detailed function and screen level security parameters that can be configured by the client.

CONTROL OBJECTIVES AND RELATED CONTROLS

ECI has specified the control objectives and identified the controls that are designed to achieve the related control objective. The specified control objectives, related controls, and complementary user entity controls are presented in Section IV, *EC Infosystems’ Control Objectives and Related Controls, and Independent Service Auditors Tests of Controls and Results of Tests*, are an integral component of ECI’s description of its EDI and Billing System Outsource Services.

COMPLEMENTARY USER ENTITY CONTROLS

The processing of transactions performed by ECI for user entities (“clients”) and the controls at ECI cover only a portion of the overall internal control related to the EDI and Billing System Outsource Services. It is not feasible for the control objectives relating to the processing of transactions to be solely achieved by ECI. Therefore, each user entities’ internal control must be evaluated in conjunction with the controls of ECI and the testing summarized in the *Section IV—Description of EC Infosystems’ Control Objective and Related Controls, and Independent Service Auditors Tests of Controls and Results of Tests* section of this report.

The following complementary user entity controls should not be regarded as a comprehensive list of all controls that should be deployed by user entities, because there may be additional controls that would be appropriate for the user entities that are not identified in this report. In addition, specific user entity and ECI responsibilities may be set forth in formal agreements between ECI and each user entity. User entities should understand the distribution of the responsibilities and implement appropriate controls to ensure all responsibilities are effectively performed. Accordingly, the list of Complementary User Entity Controls does not purport to be, and is not, a complete listing of the controls that provide a basis for the assertions underlying the financial statements of clients.

User entities are responsible for ensuring that the following complementary user entity controls are properly addressed:

Complementary User Entity Controls

- 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. (Control Objective 14)
- Timely written notification of changes in the designation of user individuals authorized to instruct ECI regarding activities is adequately communicated to ECI. (Control Objectives 9, 10, 11, 12)
- 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 timely. (Control Objectives 9, 10, 11, 12)

Complementary User Entity Controls

- Timely written notification of changes in related parties for purposes of identifying parties-in-interest transactions is adequately communicated to ECI. (Control Objectives 9, 10, 11, 12)
- User entities are responsible for establishing physical security protections over all workstations, servers, and communication hardware that connect to the ECI systems, which are housed in their facilities or other locations under their control or supervision. Physical access should be limited to only those individuals that require such access to perform their jobs. (Control Objective 3)
- User entities 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.). (Control Objective 4)
- User entities are responsible for developing appropriate system security within their applications and systems that connect to the ECI systems. This responsibility applies to all user entities facilities or other locations including third-party locations that connect to the ECI production systems and are under the user entity's control or supervision. (Control Objective 6)
- An Information Security Policy approved by user entities' management is implemented across any user entity third-party that connects to the ECI production systems. (Control Objective 4)
- Security awareness training is provided to all personnel with access to Confidential Utility Information. (Control Objectives 4, 5)
- User entities 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. (Control Objective 7)

Complementary User Entity Controls

- Confidential Utility Information is encrypted in transit utilizing industry best practice encryption methods. (Control Objective 10)
- User entities are responsible for developing their own Business Continuity Plans. (Control Objective 7)

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

As stated in the description, ECI uses Webair, a co-location data center facility that hosts ECI's production servers and provides backup storage services.

The description indicates that certain control objectives and control specified in the description can only be met, if complementary subservice controls, assumed in the design of ECI's controls, are suitably designed and operating effectively, along with related controls at ECI.

ECI has identified the following subservice organization controls:

Related Control Objectives	Webair Controls
Control Objective 3: Controls provide reasonable assurance that physical access to ECI's production systems is restricted to properly authorized and appropriate individuals.	Physical security of the data center
Control Objective 7: Controls provide reasonable assurance that programs, files and datasets related to network and production systems that have been identified as requiring periodic backup, either for availability or data integrity purposes, are appropriately backed up and restorable.	Physical security of the data center Environmental controls of the data center

**Section 4: EC Infosystems Inc.'s Control Objectives and Related Controls and Independent Service
Auditors' Tests of Controls and Results Thereof**

Introduction

This report on the internal controls placed in operations and tests of operating effectiveness is intended to provide interested parties with sufficient information to obtain an understanding of those aspects of EC Infosystems' controls that may be relevant to a user organization's internal control structure. This report, when combined with an understanding of the policies and procedures at user organizations, is intended to assist user auditors in planning the audit of the user organization and in assessing control risk for assertions of the user organizations' financial statements that may be affected by policies and procedures of EC Infosystems' Electronic Data Interchange (EDI) and Billing System Outsource Services system.

The system description, control objectives and related controls are the responsibility of EC Infosystems management. Marcum's responsibility is to express an opinion that the system description was fairly presented and controls were suitably designed to achieve the control objectives specified in the Testing Matrices and were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives, specified by EC Infosystems' management, were achieved during the period of October 1, 2020 to September 30, 2021.

Control Environment

The control environment represents the collective effect of various components in establishing and enhancing the effectiveness of specific controls and mitigating identified risks. In addition to testing the design and operating effectiveness of the control activities in Section 4 of this report. Our examination also included tests of and consideration of the relevant components of EC Infosystems' control environment over the operations that support the Electronic Data Interchange (EDI) and Billing System Outsource Services system.

Our tests of the control environment included the following procedures to the extent we considered necessary to address management's relevant control environment and included the following:

- Obtaining and understanding of EC Infosystems' organizational structure, including the segregation of duties, policy statements and personnel policies.
- Discuss with management, operations, administrative and other personnel who were responsible for developing and enforcing daily activities and requirements.
- Testing of oversight and company level controls on a sample basis to ensure key control environment activities were operating as described

Testing Approach

The objective of our testing is to determine the operating effectiveness of the controls specified by EC Infosystems' Electronic Data Interchange (EDI) and Billing System Outsource Services system throughout the period of October 1, 2020 to September 30, 2021. Testing was designed with the intent to perform procedures reasonable but not absolute assurance that the specified controls were achieved during 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:

Nature of Control and Frequency of Performance	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

Testing Matrices

Change Development (Change Management)

Control Objective 1: Controls provide reasonable assurance that request to develop production system/application changes are authorized, tested, documented, and approved.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.1	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.
1.2	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 within the examination 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.
1.3	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 within the examination 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.
1.4	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.

Change Migration (Change Management)

Control Objective 2: Controls provide reasonable assurance that changes to the production systems are tracked and authorized prior to implementation and change migration duties are segregated.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.1	Changes to the ECI client production environment are recorded and tracked.	For a sample of changes to the production environment within the examination period, inspected the corresponding IT support ticket and determined that each change was recorded and tracked in a ticket.	No exceptions noted.
2.2	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 within the examination 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.
2.3	Segregation of duties exists such that the person approving the change to the client production environment is not the same person who is responsible for implementing the change to the client production environment.	<p>For a sample of changes to the production environment within the examination 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.</p> <p>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 approve changes or develop code.</p>	No exceptions noted.
2.4	Rollback procedures exist allowing the removal of changes, if necessary.	For a sample of changes to the production environment within the examination period, inspected the related documentation and determined that rollback procedures were included, if necessary.	No exceptions noted.

Physical Access

Control Objective 3: Controls provide reasonable assurance that physical access to ECI's production systems is restricted to authorized individuals.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.1	ECI identifies and authorizes appropriate personnel having access to the subservice organization facility that hosts ECI's production servers.	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.
3.2	On an annual basis, ECI management obtains and performs a documented review over the subservice organization's SOC report to ensure any issues identified by external auditors are monitored and resolved.	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.

Logical Access (ECI Network)

Control Objective 4: Controls provide reasonable assurance that logical access to ECI's network and production systems is restricted to authorized individuals.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.1	A written Enterprise Information Security Policy is maintained by ECI. This policy details ECI's security framework and the expectations of its employees in relation to maintaining a proper information security program.	Inspected the Enterprise Information Security Policy and determined that the policy establishes a framework and expectations for employees to follow.	No exceptions noted.
4.2	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.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.3	A process is in place for assigning and removing user access to the network and production systems.	<p>Inspected the Password and Access Control Management procedure and noted that a process is in-place for assigning, modifying, and removing user access to the production system, and that the procedure was recently reviewed.</p> <p>For a sample of new hires within the examination 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.</p> <p>For a sample of terminated employees during the examination period, inspected email chains and access lists and determined that access to the network domain and all production systems was revoked timely.</p>	No exceptions noted.
4.4	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.
4.5	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.	<p>Observed the Single Sign On (SSO) Portal settings and determined that SSO is used to authenticate into production systems.</p> <p>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.</p>	No exceptions noted.

Logical Access (Client Access)

Control Objective 5: Controls provide reasonable assurance that personnel are prevented from gaining access to unauthorized data.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.1	Authentication controls prevent ECI clients from accessing records they are not authorized to view.	For one ECI client within the examination period, observed the SFTP and production systems authentication controls and verified that SFTP and production systems have authentication controls in place to prevent client users from accessing records they are not authorized to view, such as other client records.	No exceptions noted.
5.2	Client users require a user ID and password in order to gain access to the production systems.	For each production system, observed an ECI employee log into the system as a client with a unique user name and password.	No exceptions noted.

Logical Access (Network Security)

Control Objective 6: Controls provide reasonable assurance that network security is implemented and functioning.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.1	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.
6.2	Anti-virus protection is active on all workstations and servers in the ECI network. Virus definitions are set to update at least daily.	Inspected the configuration of the anti-virus software and determined that it is installed on servers and workstations and configured to receive virus updates at least daily.	No exceptions noted.
6.3	The ECI Network is configured with necessary patches and upgrades as recommended by Microsoft.	Inspected a list of Windows patches applied during the examination period and determined that the necessary updates were installed.	No exceptions noted.



Computer Operations (Backup and Recovery)

Control Objective 7: Controls provide reasonable assurance that programs, files, and datasets related to network and production systems that have been identified as requiring periodic backup, either for availability or data integrity purposes, are backed up and restorable.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.1	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.
7.2	ECI performs a nightly backup of the production data and backups are logged.	For a sample of days within the examination 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.
7.3	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.
7.4	Restoration testing of backup data is performed on a quarterly basis.	For a sample of quarters within the examination period, inspected data restoration log and determined that data restoration test was performed successfully by management.	No exceptions noted.

Computer Operations (Batch and Online Processing)

Control Objective 8: Controls provide reasonable assurance that production systems used to process batch and online transactions and prepare related reports are restricted to authorized individuals, executed in a timely manner and processed to completion.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.1	Access to modify, delete, or create production processing control language and executable programs (job scheduling) is restricted to select authorized individuals.	Inspected the system generated list of individuals with access to production (job scheduling) processing control language and executable programs within the examination period and determined through comparison of the Company organizational chart that such access was restricted to ECI IT personnel according to job functions.	No exceptions noted.
8.2	Business significant and critical job processing is monitored by ECI to ensure successful and timely completion, including a review and resolution of any exceptions.	<p>Observed the ECI Network Operating Center (“NOC”) Team monitor business significant and critical job processing to completion within the examination period.</p> <p>For a sample of processing problems that occurred during the examination 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.</p>	No exceptions noted.

Computer Operations (Process Activity Monitoring)

Control Objective 9: Controls provide reasonable assurance that ECI has defined and implemented a problem management system to ensure that operational incidents, problems and errors are recorded, analyzed and resolved in a timely manner.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
9.1	ECI monitors system activity, and processing problems are recorded and appropriately resolved by an ECI technical support personnel.	<p>Observed the ECI Network Operating Center (“NOC”) Team use the AcuTrack system to track processing errors.</p> <p>For a sample of processing problems that occurred during the examination 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.</p>	No exceptions noted.

Data Transmissions

Control Objective 10: Controls provide reasonable assurance that data transmission between ECI, its users and other entities are complete, accurate, and sent from authorized sources.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
10.1	Data transmissions are monitored by ECI to ensure that transmissions are complete, accurate, and sent from authorized sources.	<p>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.</p> <p>For a sample of days within the examination 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.</p>	No exceptions noted.

Recording of Transactions

Control Objective 11: Controls provide reasonable assurance that data transmission between ECI, its users and other entities are complete, accurate, and sent from authorized sources.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
11.1	ECI utilizes the TrueTrack system to process transactions in accordance with its user entity agreements.	<p>Observed ECI personnel utilize the TrueTrack system and determined that all Electronic Data Interchange transactions are actively monitored.</p> <p>For a sample of days within the examination 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.</p> <p>For a sample of inbound and outbound processing exceptions identified during the monitoring process within the examination 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.</p>	No exceptions noted.
11.2	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 examination 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.

Client Issues Tracking

Control Objective 12: Controls provide reasonable assurance that highlighted errors or issues are assigned numbers, logged with dates, and researched and corrected or resolved and communicated to users.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
12.1	Processing actions are monitored, and problems highlighted by the TrueTrack tracking system are identified and assigned to operations for disposition.	<p>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.</p> <p>Observed the use of the UtiliPort system and determined that ECI can summarize processing results.</p> <p>For a sample of processing problems, 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.</p>	No exceptions noted.

Client Data Integrity

Control Objective 13: Controls provide reasonable assurance that client data and file versions are complete and accurate.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
13.1	Electronic data is monitored to ensure complete and accurate client data is stored on the production systems.	<p>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.</p> <p>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.</p> <p>For a sample of days within the examination 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.</p>	No exceptions noted.

Client Output Documents

Control Objective 14: Controls provide reasonable assurance that output data is complete and accurate based on processing needs defined in the Customer Agreements and are made available to authorized recipients on a timely basis.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
14.1	Documents are distributed to ECI clients in an electronic format using SFTP and production systems, and only authorized recipients may obtain the information.	Observed an ECI employee log into the SFTP system with a unique user name and password and validated that they only have access to the data of one client. Observed an ECI employee use SFTP and determined that ECI clients have a system to securely transmit files to ECI.	No exceptions noted.
14.2	Users must execute a Customer Agreement that outlines processing requirements. The client output file process is documented by the completion of the Operations Task List.	For a sample of clients, inspected the executed customer agreement and determined that it outlines processing requirements. For a sample of days within the examination period, inspected the Operations Task Lists 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.

Section 5: Other Information Provided by EC Infosystems, Inc.

Overview of ECI's Disaster Recovery Plan

EC Infosystems Inc. is committed to providing uninterrupted 24/7 service to its customers. There are, however, unforeseen events and natural disasters that may cause a disruption in service.

In the event of a disaster the primary goal is to bring the core EDI services back online within the shortest available time frame. Once activated, the disaster recovery systems are fully capable of immediately handling all core services needed to process the EDI files for all of ECI's customers. After the core services are restored, ECI will complete the recovery process by installing additional hardware and restoring ancillary databases and services such as the online tracking and billing systems.

ECI contracts with WebAir for its managed Disaster Recovery as a Service (DRaaS) with a 15-minute replication SLA. The hosting facility is located in Chicago, IL. The replicated systems are maintained and tested on a regular basis. Customers and staff members will have immediate access to the DRaaS systems as soon as they are required.

Reliable database and file system backups are also key to restoring service after a system outage. Key databases are backed up directly to the disaster recovery servers at various times throughout the day and are available for immediate use should the need arise. EC Infosystems also performs full system backups using high speed disk-to-disk storage devices. Daily incremental and weekly full images are maintained at a secured offsite location. The retention cycle for the daily backups are daily from the primary backup system. Files and databases can be restored directly to the disaster recovery systems using the same type of high quality, high speed tape devices that are in use at the primary datacenter.

ECI reviews and updates the disaster recovery plans on a regular basis and works closely with their partners and suppliers to ensure that equipment and services are in place and operational in the event of a disaster. Every staff member is trained and tested on the recovery procedures and is ready to do their part should the need arise. Whether during normal operating conditions or a natural disaster, ECI always remains committed to providing superior service and support.

The first step to disaster recovery is preparing for the disaster. Data must be backed up, hardware and software must be maintained, and staff must be trained. The following outlines the procedures that ECI performs to prepare for the recovery.

- **Hardware Maintenance** - Backup hardware is thoroughly tested to ensure that all systems are operational when needed. Hardware is also upgraded on a regular basis to match the configuration of our primary datacenter.

- **System Software Maintenance** - Operating system and third-party software system upgrades are applied to both the primary and backup servers.
- **EC Infosystems Software Maintenance** - ECI customer information system software upgrades are applied weekly to both the primary and backup servers ensuring that all systems function correctly in the event of a disaster.
- **Database System Backup** - All system and customer database backups are replicated nightly and stored to disk at a secure off-site facility. Certain mission critical databases are also replicated in real time directly to the backup server. This allows for the fastest possible restoration of critical database systems.
- **File System Backup** - Full file system backups of EDI files, flat files, and other supporting file system objects are performed weekly. Incremental backups are performed nightly. All backups are replicated to disk at a secure offsite facility.
- **Data Communication Testing** - Live internet connections are maintained at all times and are an integral part of the backup process. Voice communication facilities are also maintained and tested on a regular basis.
- **Staff Training** - All new staff members are fully trained in backup and recovery procedures. All staff members also participate in periodic reviews and training drills ensuring that everyone is up to date on emergency operating procedures.

Each emergency situation presents its own unique set of challenges and must be handled in different ways. It is beyond the scope of this document to describe every contingency plan in full detail that ECI has in place. Outlined below are the general procedures that would be taken in the event of a disaster of any nature.

- **Staff Notification** - All essential EC Infosystems staff members are contacted and briefed on the situation.
- **Recovery Assessment** - The recovery team meets to assess the situation and determine the level of recovery needed. The recovery plan is adjusted to address any special needs or situations.
- **Backup System Activation** - The backup system is maintained in an online and ready state 24/7. A recovery team member need only log on to the system. Core EDI systems, databases and files are immediately available from hot backups that were performed directly from our datacenter to the backup server.
- **Service Provider Notification** - Key vendors and service providers are notified of the situation. Internet addresses are rerouted to the backup facility, additional hardware is ordered, and any other critical supplies and services are requisitioned.

- **Customer Notification** - Utilities and Retail Marketers are notified of the situation. Any changes in voice and data communication procedures are identified. Customers will continue to receive status updates throughout the entire recovery process.
- **Activate Primary Systems** - The core EDI systems and services are activated, and processing is resumed. ECI staff closely monitors all system activity during this time to ensure that acceptable service levels are maintained at all times.
- **Restore Secondary Databases** - Secondary databases and files are restored from available replicated disk backups. Customers are notified to retransmit any additional data files that may have been lost due to the emergency situation.
- **Activate Secondary Systems** - Secondary systems that were not absolutely critical such as online tracking and billing systems are activated and made available for customer use.
- **Restore Full Capacity** - Additional hardware is added to the backup servers to return the system to full operating capacity.



REPORT ON

EC INFOSYSTEMS, INC.'S

DESCRIPTION OF ITS ELECTRONIC DATA INTERCHANGE (EDI) AND
BILLING SYSTEM OUTSOURCE SERVICES SYSTEM AND ON THE
SUITABILITY OF ITS CONTROLS RELEVANT TO SECURITY,
PROCESSING INTEGRITY, AND CONFIDENTIALITY THROUGHOUT
THE PERIOD

APRIL 1, 2021 TO SEPTEMBER 30, 2021



EC Infosystems, Inc. – SOC 2 TYPE II TABLE OF CONTENTS

Acronym Table	i
Section 1: Assertion of the Management of EC Infosystems, Inc.	1
Section 2: Independent Service Auditors' Report	5
Section 3: EC Infosystems, Inc.'s Description of its Electronic Data Interchange (EDI) and Billing System Outsource Services System	10
Scope and Purpose	10
Services Provided	10
Principal Service Commitments and System Requirements.....	11
Components of the System Used Provide the Services	13
Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring Controls.....	22
Disclosure of Security Incidents	37
Complementary Subservice Organization Controls	37
Complementary User Entity Controls.....	38
Significant Changes to the System throughout the Review Period	39
Applicable Trust Services Categories.....	39
Section 4: EC Infosystems, Inc.'s Trust Services Categories, Criteria, Related Controls, and Test of Controls	40
Testing Approach.....	41
Sampling Approach	41
Trust Services Security, Processing Integrity, and Confidentiality Categories, Criteria, Related Controls, and Tests of Controls	42

Acronym Table

➤ AICPA	American Institute of Certified Public Accountants
➤ AES	Advanced Encryption Standard
➤ AMI	Advanced Metering Infrastructure
➤ API	Application Programming Interface
➤ CEO	Chief Executive Officer
➤ CSV	Comma-Separated Values
➤ EDC	Electric Distribution Company
➤ EDI	Electronic Data Interchange
➤ ERCOT	Electric Reliability Council of Texas
➤ ES	Energy Supplier
➤ EST	Eastern Standard Time
➤ FTP	File Transfer Protocol
➤ FTPS	File Transfer Protocol Secure
➤ GISB	Gas Industry Standards Board
➤ GIS	Geographic Information Systems
➤ HR	Human Resources
➤ IDS	Intrusion Detection System
➤ IPS	Intrusion Prevention System
➤ IT	Information Technology
➤ IS	Information Security
➤ KPI	Key Performance Indicator
➤ MFA	Multi Factor Authentication
➤ NAESB	North American Energy Standards Board
➤ NAS	Network Attached Storage
➤ NOC	Network Operations Center
➤ PGP	Pretty Good Privacy
➤ RAID	Redundant Array of Independent Disks
➤ QA	Quality Assurance
➤ SAN	Storage Area Network
➤ SFTP	SSH File Transfer Protocol
➤ SIEM	Security Information and Event Management
➤ SLA	Service Level Agreement
➤ SOC	System and Organizational Controls
➤ SSL	Secure Socket Layer
➤ SSO	Single Sign-on
➤ TSC	Trust Service Criteria
➤ UB	UtiliBill
➤ USPS	United States Postal Services
➤ VAN	Value Added Network
➤ VPN	Virtual Private Network



Section 1: Assertion of the Management of EC Infosystems, Inc.



333 Earle Ovington Blvd, Suite 102
Uniondale, NY 11553

Tel : 516-874-8000
Fax: 516-739-4724

www.ecinfosystems.com

Assertion of the Management of EC Infosystems, Inc.

We have prepared the description of EC Infosystems Inc.'s ("EC Infosystems" or "ECI") Electronic Data Interchange (EDI) and Billing System Outsource Services system entitled "EC Infosystems Inc.'s Description of its Electronic Data Interchange (EDI) and Billing System Outsource Services System" for processing user entities' transactions throughout the period April 1, 2021 to September 30, 2021 (description) for user entities of the system during some or all of the period April 1, 2021 to September 30, 2021, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

EC Infosystems uses a subservice organization for colocation data center hosting services. The description includes only the control objectives and related controls of EC Infosystems and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by EC Infosystems can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls at EC Infosystems. The description does not disclose the actual controls at the subservice organizations.

The description also indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of EC Infosystems' controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

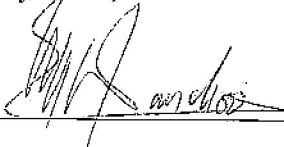
We confirm, to the best of our knowledge and belief, that:

- a. The description fairly presents the EC Infosystems' Electronic Data Interchange (EDI) and Billing System Outsource Services system made available to user entities of the system during some or all of the period April 1, 2021 to September 30, 2021, for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:
 - i. Presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable:
 - (1) The types of services provided, including, as appropriate, the classes of transactions processed.

- (2) The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.
 - (3) The information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
 - (4) How the system captures and addresses significant events and conditions other than transactions.
 - (5) The process used to prepare reports and other information for user entities.
 - (6) Services performed by a subservice organization, if any, including whether the inclusive method or the carve-out method has been used in relation to them.
 - (7) The specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the controls.
 - (8) Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.
- ii. Includes relevant details of changes to the Electronic Data Interchange (EDI) and Billing System Outsource Services system during the period covered by the description.
 - iii. Does not omit or distort information relevant to the system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors and may not, therefore, include every aspect of the Electronic Data Interchange (EDI) and Billing System Outsource Services system that each individual user entity of the system and its auditor may consider important in its own particular environment.
- b. The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period April 1, 2021 to September 30, 2021, to achieve those control objectives if the subservice organizations and user entities applied the complementary controls assumed in the design of EC Infosystems' controls throughout the period April 1, 2021 to September 30, 2021. The criteria we used in making this assertion were that:
 - i. The risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization.
 - ii. The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

- iii. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

EC Infosystems, Inc.

A handwritten signature in black ink, appearing to read 'Mohan Wanchoo', is written over a horizontal line.

Mohan Wanchoo, President & CEO

12/23/2021

DATE

Section 2: Independent Service Auditors' Report

Independent Service Auditors' Report

To: EC Infosystems, Inc.

Scope

We have examined EC Infosystems Inc.'s ("EC Infosystems" or "ECI") accompanying description of its Electronic Data Interchange (EDI) and Billing System Outsource Services system found in Section 3 titled "EC Infosystems, Inc.'s Description of its Electronic Data Interchange (EDI) and Billing System Outsource Services System" throughout the period April 1, 2021 to September 30, 2021, (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 1, 2021 to September 30, 2021, to provide reasonable assurance that EC Infosystems' service commitments and system requirements were achieved based on the trust services criteria relevant to security, processing integrity, and confidentiality (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

EC Infosystems uses a subservice organization for colocation data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at EC Infosystems, to achieve EC Infosystems' service commitments and system requirements based on the applicable trust services criteria. The description presents EC Infosystems' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of EC Infosystems' controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

Service Organization's Responsibilities

EC Infosystems is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that EC Infosystems' service commitments and system requirements were achieved. In Section 1, EC Infosystems has provided the accompanying assertion titled "Assertion of the Management of EC Infosystems" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. EC Infosystems is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

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

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.

- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

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

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

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4.

Opinion

In our opinion, in all material respects:

- a. the description presents EC Infosystems' Electronic Data Interchange (EDI) and Billing System Outsource Services system that was designed and implemented throughout the period April 1, 2021 to September 30, 2021 in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period April 1, 2021 to September 30, 2021, to provide reasonable assurance that EC Infosystems' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of EC Infosystems' controls throughout that period.

- c. the controls stated in the description operated effectively throughout the period April 1, 2021 to September 30, 2021, to provide reasonable assurance that EC Infosystems' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of EC Infosystems's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of EC Infosystems, user entities of EC Infosystems' Electronic Data Interchange (EDI) and Billing System Outsource Services system during some or all of the period April 1, 2021 to September 30, 2021, business partners of EC Infosystems subject to risks arising from interactions with the Electronic Data Interchange (EDI) and Billing System Outsource Services system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

Marcum LLP

Marcum LLP

December 23, 2021
New Haven, CT 06511

Section 3: EC Infosystems, Inc.'s Description of its Electronic Data Interchange (EDI) and Billing System Outsource Services System

Scope and Purpose

EC Infosystems, Inc. (ECI) is a technology services vendor that provides an Electronic Data Interchange (EDI) and billing services to its clients. The scope of this report covers ECI's direct marketing platform system at ECI's facility located in Uniondale, New York. This report applies only to services covered within the company's electronic data interchange (EDI) and billing system outsource services system provided by ECI to user entities.

ECI's system is designed with the assumption that certain controls will be implemented by user entities. In certain situations, the application of specific controls at user entities is necessary to achieve the service commitments and system requirements included in this report. There may be control activities that are not identified in this report that would be appropriate for user entities.

Services Provided

ECI provides Electronic Data Interchange (EDI) and Billing System Outsourced Services for the deregulated gas and electric marketplace. In this deregulated energy industry, ECI's system enables the processing of transactions through its UtiliBill, EC Central, TrueTrack and UtiliPort proprietary applications for users to acquire and support gas and electric customer activity and billing services. The processes that support user activity for their customer base include:

- Providing users an operational platform to create rate/pricing data.
- Enrolling users' new customer application data.
- Providing users with bulk uploads via secure electronic FTP (file transfer protocol) exchange.
- Transmitting users' customer data to/from respective utilities via EDI.
- Receiving meter reading details from the utilities.
- Receiving invoice details from Utility Rate Ready utilities.
- Providing users with the ability to calculate billing invoices on Utility Bill Ready, Dual and Marketer Bill Ready utilities.
- Transmitting billing invoices to Utility Bill Ready utilities.
- Providing users with the ability to create and send invoices for Dual and Marketer Bill Ready accounts.
- Providing users with the ability to manage accounts receivable activity via reports.
- Receiving remittances of payment notification from utilities.
- Providing users the ability of manual or automated logging of payment activity from their customers.
- Providing users with the ability to send notifications to customers in the form of emails or letters generated from the system for activities related to rate changes and payment activity.
- Providing users with transactional tracking, operational, management and ad hoc reports.

- Providing users data reporting in a variety of formats.

The users are securely connected to ECI's proprietary software platform via secured web access. The system applications enable user's access to the system in real time while allowing ECI operating personnel to manage and monitor the EDI transaction processing functions.

Principal Service Commitments and System Requirements

The principal service commitments are:

- To meet the specific terms in Service Level Agreements with each client.
- To process client transactions completely and accurately, including identifying and designating confidential information when it is received/created and to determine the period over which the confidential information is to be retained.
- To ensure all transactions, including confidential information is protected during the system design, development, testing, implementation, and change processes.
- Technical safeguards for data transmissions exist, using 256-bit AES encryption and are stored in encrypted format using software supporting the 256-bit AES encryption. Use of removable media is prohibited by policy except when authorized by management.
- ECI and client users require a user ID and password in order to gain access to its systems.
 - System security is configured to require internal and external users to change their passwords upon their initial system sign-on and thereafter every 52 days after their initial sign-on.
 - ECI and client users require a user ID and password in order to gain access to its systems. External access by personnel is permitted only through a two-factor encrypted VPN connection.
- Protect confidential information from erasure or destruction during the specified retention period of the information;
- Identify confidential information requiring destruction when the end of the retention period is reached and to;
- Erase or otherwise destroy confidential information that has been identified for destruction.
- A NOC reviews transactions to ensure that the transmissions are complete, accurate, received on a timely basis, and sent from authorized sources. Any errors are identified and follow-up actions are taken to correct the noted issues.

The system requirements are:

- ECI has a formal change management system development process in the development/maintenance of projects to guide programming personnel in the design, coding, testing and implementation of change procedures for all system application changes.
 - Controls exist, including a segregation of duties, such that the person approving the change to the client production environment is not the same person who is responsible for implementing the change to the client production environment.
 - That testing is performed in a separate QA/test environment by ECI prior to releasing into the client production environment.
 - Access to the shadow test environment utilized to reproduce and test production data is restricted to authorized users; and access to nonproduction environments is granted based on job roles and duties.
- Logical access controls exist; including the handling of confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition.
 - A network infrastructure with firewall protection and an active directory management to monitor and control unauthorized access attempts.
 - Access to administer the systems is restricted to authorized personnel and access to confidential information is granted based on job roles and duties.
 - A process is in place for assigning, modifying, and removing user access to the production system(s).
 - Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties.
 - Awareness training is provided to personnel around the policy and usage of confidential and personal information.
- ECI and client users require a user ID and password in order to gain access to its systems.
 - System security is configured to require internal and external users to change their passwords upon their initial system sign-on and thereafter every 52 days after their initial sign-on.
 - ECI and client users require a user ID and password in order to gain access to its systems. External access by personnel is permitted only through a two-factor encrypted VPN connection.
- ECI's subservice organization SOC reports are reviewed, documented and assessed for impact to ECI's control environment. Periodic site visits to the data center are performed by ECI's IT department. Site visits are documented accordingly.

Components of the System Used Provide the Services

Infrastructure

ECI physical structures reside at the following:

- Home Office: EC Infosystems, Inc., 333 Earle Ovington Blvd, Suite 102, Uniondale NY 11553
- Satellite Offices:
 - PA: 1275 Glenlivet Drive, Suite 132, Allentown, PA 18106
 - TX: 2617 Bissonnet Street, Houston TX 77006
- Hardware – Servers
 - Webair, a collocation facility which includes, rack space, power (including battery and generator power), internal/external communication connections and cooling.

All of the systems detailed in the Software section are home grown applications, (proprietary software platforms accessed via the web based .NET framework), that process the data and transactions on behalf of ECI's clients.

To support their clients, ECI maintains a network of personal computers and servers and uses programs built for its data outsourcing system. The system consists of multiple components including servers (Dell R710, R720, R920 and 2950 models HPE ProLiant DL360 Gen9, Gen 10); disk storage, (EMC Unity, EqualLogic and Dell PS 6100s), a firewall (Sonicwall), and network switch (Dell 6428). The servers are supported by a combination of Microsoft Windows 2012R2, 2016 and 2019. The workstations are running Windows 10.

Software

The Electronic Data Interchange (EDI) and Billing System Outsource Services are processed through the following proprietary applications.

UtiliBill

The UtiliBill application is the customer information system used by clients (marketers, retailers), to manage customers, generate bills, and manage accounts receivable (A/R) and accounts payable (A/P) functions. UtiliBill is a scalable system that allows the setup of residential customers as well as large commercial and industrial (C&I) national accounts. This system is designed to accommodate clients operating in multiple states and different billing scenarios for both residential and large C&I customers.

UtiliBill makes information readily available to clients and provides a wide range of reports that help the client manage their business operations. Clients can choose to personalize their reports to give them the look and feel they desire.

This UtiliBill application provides the following capabilities, among others:

Billing – Process meter reads and rates to generate bills based on the customer's billing cycle. Retain bill images on-line for customer service access. Establish budget billing for certain customers.

E-Billing – Process bills the same as Billing above, but sends electronic bills. Customers can enroll with a customer service representative.

Payments – Marketers receive payments through lock boxes, electronic funds transfer, cash, and check and can post these items via upload transactions to UtiliBill. Establish payment plans for certain customers.

Adjustments – Marketers can manage adjustments to customer billing and receivables.

Credit and Collections – Marketers can maintain accounts receivable information by customer and account, process collections criteria, send notices to delinquent payers and initiate severance process.

Rates Management – Marketers maintain and apply rates based on numerous factors.

Premise Information – Marketers maintain accurate premise address information validated by USPS and the local tax office. Integrate premise information with GIS.

Service Point Information – Marketers maintain accurate location information for service points for the customer.

Meter Reads – Upload data into UtiliBill via interface by EDI system or user input.

Customers – Marketers can manage customer information.

Customer Contacts – Marketers can capture every contact with a customer whether by phone or numerous types of letters.

Utility Specific Data – Marketers can set utility specific data per utility.

System API for UB system – Provides many APIs for the business function and data management for system to system communication between UB and clients/ third party.

Reports – Provides numerous reports and queries are used by the marketers for daily management by functional area.

Security – Configure the application to allow/restrict specific users visibility and update capability at multiple levels – from data field to division levels.

EC Central

EC Central Website: This is one of the client transaction submission applications available for ECI clients to submit transactions to the trading partner as needed.

Transactions and Translations

EDI system receives files in the form of ECI formatted flat files, X12, fixed length and Excel formats. EDI systems are capable of processing all the transaction received in the energy industry. Following are few core frequently transacted data set.

814 Transaction Set : The primary process addressed by this transaction set 814 are the customer requests for the enrollment with the third party supplier, the maintenance of customer account information, disenrollment or dropping out from the service provider and for the changing the customer information.

Meter Reading (867 Transaction Set): -This communicates the usage data the customer consumed each service period along with historical usage. This transaction mostly flows from the trading partner EDC to the client ES.

Payments / Remittance (820 Transaction Set): - The payment or remittance advice transaction is primarily used to communicate with the client about the amount deposited to the client's bank account.

Invoice (810 Transaction Set):- This transaction set flows bidirectional between the EDC and ES depends on the billing method type. This contains the information about the amount the ES or EDC going to bill to the end consumer.

Application Advice (824 Transaction Set): – This transaction set is used to acknowledge or reject 810 transactions received from the billing party.

SMT (Smart Meter Texas) Data: – ECIs process SMT data files for the clients who are enrolled for receiving the daily electricity usage data for AMI meters in the ERCOT territory. ECI pulls data from SMT using an automated system.

Translations (XML, FF, Excel, Fixed length): - EDI system supports different file formats to exchange transactions between utilities and energy marketers. EDI system translates the data files based on recipient need in X12 format, Fixed Length format, CSV/ EXECL or ECI defined standard flat files.

Communication with partners (GISB/ NAESB / VAN/ FTP):– To exchange the files between partners, ECI follows industry standard electronic delivery mechanism protocol GISB and NAESB. ECI ensures the files are encrypted thru PGP encryption. ECI also supports the trading partners who use the industry standard protocols like VAN, FTPS and SFTP.

Communication with Intra-System and Clients: - The communication protocol used by the marketers to exchange the files with ECI are FTPS and SFTP protocol. The automated file watcher service checks for the incoming files and transports the files to the processing server.

Tracking Systems: - EC Central data processing systems are integrated with TrueTrack, which is a real time tracking system. This system updates statuses at various processing stages and monitors system processing integrity in real time. The data collected used in the TrueTrack application to visualize the data file processing progress in real time.

TrueTrack

This is a dynamic transaction tracking system that provides for the tracking of all inbound and outbound transactions processed on the various EDI systems. This system provides for verification of successful transmission and receipt of transactions.

Transactions- Provides the ability to view inbound and outbound EDI transactions.

Reports – System provides inbound and outbound reporting displaying successfully processed transactions as well as exceptions which require immediate attention.

Security – Configure the application to allow/restrict specific users visibility and update capability.

UtiliPort

UtiliPort provides enhanced functionality of the TrueTrack application and allows ECI clients to monitor all transactions flowing through the EDI transaction management system and see customer activity information in an easy to track web portal. It helps clients to view their transactions at an overall level and enables them to drill down to the individual transaction level.

UtiliPort allows clients to monitor events that need immediate attention and track a customer's enrollment process with a utility in detail.

As part of this system, clients are provided with various types of information that enable them to manage their day to day business functions. The system lists certain time sensitive action items that need to be performed on an immediate basis. It also gives the clients various exception reports and standard reports.

Transactions- Provides the ability to view inbound and outbound EDI transactions.

Reports – System provides inbound and outbound reporting displaying successfully processed transactions as well as exceptions which require immediate attention.

Security – Configure the application to allow/restrict specific users visibility and update capability.

Supporting Software

The following software supports ECI application software of UtiliBill, EC Central, TrueTrack and UtiliPort applications:

VPN - for some users

The interfaces used with UtiliBill, EC Central, TrueTrack and UtiliPort are ECI custom web API's and batch files submitted via FTP.

People

ECI personnel involved in the governance, operation and use of UtiliBill, EC Central, TrueTrack and UtiliPort applications include ECI developers, operators, users, managers, clients, consultants and vendor personnel. These users can be organized into the following functional areas:

Executive Department - Serves as management of the processing operations. This department has the ultimate responsibility for administration of the operations. The department interacts with customer managers and is responsible for performance measurement, and compliance with the policies and procedures, government rules and regulations, legal governance, and user agreements. It ensures that the operation is ethical and promotes integrity; transparency and accountability with all transactions and establishes operation controls to monitor the system through various levels of management.

ECI's Organizational Chart is reviewed annually by the CEO and discussed with management, updated as needed. Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors. Those job descriptions are reviewed by ECI management on an annual basis for needed changes and descriptions are updated as needed.

Management consider the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner. The Governance Board – IT supplements its expertise relevant to security, processing integrity, and confidentiality when defining authorities and responsibilities, and as needed, through the use of a subcommittee or consultants. ECI also considers the need to interact with and monitor the activities of external parties when establishing structures, reporting lines, authorities, and responsibilities. Management considers requirements relevant to security, processing integrity and confidentiality when defining authorities and responsibilities.

ECI considers the background of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals. ECI also considers the technical competency of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.

Operations Department – Operations staff performs transaction processing of operations twenty-four hours a day, three hundred and sixty five days a year. EDI transaction processing is performed through ECI's processing facility to ensure transactions are processed accurately from data input online by user entities. This department monitors and interacts with the Executive Department and the Computer Information Systems Department and responds to user requests and investigations during business hours.

The supervising personnel are supported by staff personnel and are responsible for ensuring that the processing protocols are effectively carried out in the processing of users' data including the monitoring of all transaction processing activities. Each employee upon hire signs an employee handbook signifying responsibility and accountability for data protection.

The NOC is part of the Operations Department and provides assurance that the network infrastructure and activities are authorized and that the application-processing services provided by ECI are both timely and accurate.

Information Systems Department - This department provides the required support to maintain and operate the systems environment. It includes the computer operations, systems and programming, system software support and infrastructure functions. This department interacts with the Operations Department to provide any required client support services. The Information Systems Department is also responsible for providing application development services related to ECI production applications.

All Employees, Contractors and Vendors – Personnel are required to read and accept the code of conduct upon their hire and to formally reaffirm them annually. ECI's employee handbook includes a disciplinary policy for personnel who violate the code of conduct. Employee training over ECI's code of conduct compliance is performed at least annually. Hiring procedures include a comprehensive screening of candidates for key positions and consideration of whether the verified credentials commensurate with the proposed position. New personnel are offered employment subject to background checks and reference validation.

ECI considers the background of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals. ECI considers the technical competency of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals. In addition, ECI provides training programs, including continuing education and training, to ensure skill sets and technical competency of existing personnel, contractors, and vendor employees are developed and maintained.

System descriptions are made available to authorized external users that delineate the boundaries of the system and describe relevant system components as well as the purpose and design of the system. Documentation of the system description is made available to authorized external users via ECI's customer-facing website. ECI's external system users are subjected to training prior to use of the system.

Internal and external system users receive a technical broadcast in the event of application changes.

Policy and procedures documents for significant processes are made available on ECI's intranet. Employee training over ECI's code of conduct compliance is performed at least annually. Personnel are required to read and accept the code of conduct upon their hire and to formally reaffirm them annually. Customer requirements are documented in service agreements.

ECI has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security, processing integrity, and confidentiality and provides resources necessary for personnel to fulfill their responsibilities. Job requirements are documented in the job descriptions, and candidates' abilities to meet these requirements are evaluated as part of the orientation, onboarding, performance review, and transfer evaluation processes. During the annual performance review process, training goals, as required, for each personnel are established and documented.

ECI Personnel

ECI personnel with responsibility for designing, developing, implementing, operating, maintaining, or monitoring system controls receive communications about their responsibilities, including changes in their responsibilities, and are provided with the information necessary to carry out those responsibilities. ECI communicates its objectives and changes to those objectives to personnel in a timely manner to improve security knowledge and awareness and to model appropriate security behaviors to personnel through a security awareness training program.

ECI prepares and communicates information about the design and operation of the system and its boundaries to authorized personnel to enable them to understand their role in the system and the results of system operation. ECI personnel with responsibility for designing, developing, implementing, operating, maintaining, or monitoring system controls receive communications about their responsibilities, including changes in their responsibilities, and have the information necessary to carry out those responsibilities. ECI also communicates its objectives to personnel to enable them to carry out their responsibilities. System changes that affect responsibilities or the achievement of ECI's objectives are communicated in a timely manner.

Procedures

ECI has developed and implemented various procedures and controls to support the Trust Service Category requirements for security, confidentiality and processing integrity of the UtiliBill, EC Central, TrueTrack and UtiliPort applications. An overview of these procedures is described below.

ECI has placed into operation a risk assessment process with procedures such as assessing the business impact of loss of confidentiality, and processing integrity, threat and vulnerability assessment of the application to identify and manage risks that could affect its ability to provide reliable services to its clients. This process requires management to identify significant risks inherent in the Electronic Data Interchange (EDI) and Billing System Outsource Services processes outlined in this document and relied on by user organizations and to implement appropriate measures to monitor and manage these risks. This process has facilitated the identification of various risks inherent in ECI's operating environment and ECI's management has developed and implemented reasonable measures for the ongoing management and mitigation of these risks. The risks considered by ECI management on an ongoing basis include:

- Operational and Cyber risk associated with computerized information systems; manual interface in the processes involved in transaction processing; and external systems for client system interfacing.
- Processing risk associated with, among other things, unresolved errors in the system that are then reflected in users billing.
- New legislation and the regulatory environment.
- Competitive landscape.
- Management conducts an assessment of risk of material misstatement as it relates to achieving control objectives for user entities. Management has implemented various measures to manage risks identified through the risk assessment process.

Internal and external users have been provided with information on how to report security, processing integrity, and confidentiality failures, incidents, concerns, and other complaints to appropriate personnel. Incident response policy is documented and maintained for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints.

System changes that affect internal and external users' responsibilities or ECI's commitments and system requirements relevant to security, processing integrity, and confidentiality are communicated to those users in a timely manner. Internal and external system users receive a technical broadcast in the event of application changes.

Requests for changes are documented and approved by management prior to commencing work on the project/change. Internal and external system users receive a technical broadcast in the event of application changes. A change control process is formally documented, maintained and reviewed at least annually. Major changes to roles and responsibilities and changes to key personnel are communicated to affected internal and external users via email, as needed. If a notification is not sent, a valid business reason is documented.

Data

Data Transmissions

Data transmissions are monitored by ECI to ensure that the transmissions are complete, accurate, received on a timely basis, and sent from authorized sources. The NOC is responsible for monitoring the data transmissions sent in from ECI clients. The NOC is staffed from 7am to 7pm EST Monday through Friday. The NOC uses automated tools to check data transmission files for accuracy, completeness, and conformity with prescribed data file layouts. Any errors are identified and follow-up actions are taken to correct the noted issues.

Recording of Transactions

Client files are received, processed, and sent back out during the processing day. The NOC is responsible for monitoring the processing environment during the day.

At the completion of the day, the NOC performs the end-of-day process to close out the processing day. At the completion of this process, the NOC sends an end-of-day e-mail to the Director of Operational Excellence to summarize the days processing that includes the following information:

- Results of Inbound Daily Processing
- Results of Outbound Daily Processing
- Summary of ad hoc processes
- Integration testing status with utilities
- TrueTrack File Issues (if any)
- Any other processing problems during the day

The results of this e-mail are reviewed by the Director of Operational Excellence and any processing instructions for the following day are communicated to the NOC to resolve any issues.

System inputs are measured and recorded completely, accurately, and timely to meet ECI's processing integrity commitments and system requirements. Application edits limit input to acceptable value ranges.

EDI data processing is validated by ECI's TrueTrack system. The TrueTrack system portal automatically reports inconsistencies in the process to an ECI operator to correct the processing errors.

Monitoring of EDI data processing is performed on each business day by the ECI Operations team. UtiliBill maintains an event log file for data processing. Processing errors are scanned by the UtiliBill module 3 times a day, (initiated by the UtiliBill support staff), and a ticket is initiated by the support staff. The UtiliBill support staff compiles report of outstanding tickets and sends to management stakeholders daily in form of charts and KPI.

System edits require mandatory fields to be complete before a record entry is accepted. Electronic files received contain batch control totals. During the load processing data captured is reconciled to batch totals automatically by the applications. EDI data processing is validated by ECI's TrueTrack system. The TrueTrack system portal automatically reports inconsistencies in the process to an ECI operator to correct the processing errors. The characteristics of processing inputs that are necessary to meet requirements are defined. Processing inputs are evaluated for compliance with defined input requirements. Records of system input activities are created and maintained completely and accurately in a timely manner.

Data is processed completely, accurately, and timely as authorized to meet ECI's processing integrity commitments and system requirements. EDI data processing is validated by ECI's TrueTrack system. The TrueTrack system portal automatically reports inconsistencies in the process to an ECI operator to correct the processing errors. UtiliBill maintains an event log file for data processing. Processing errors are scanned by the UtiliBill module 3 times a day, (initiated by the UtiliBill support staff), and a ticket is initiated by ECI's UtiliBill support staff.

Application regression testing validates key processing for the application during the change management process. Application edits limit input to acceptable value ranges.

EDI data processing is validated by ECI's TrueTrack system. The TrueTrack system portal automatically reports inconsistencies in the process to an ECI operator to correct the processing errors.

Processing actions are monitored and problems highlighted by the system are identified on a timely basis and assigned to operations for effective disposition. The processing specifications that are necessary to meet product or service requirements are defined. Processing activities are defined to result in products or services that meet specifications. Errors in the production process are detected and corrected in a timely manner. System processing activities are recorded completely and accurately in a timely manner. Inputs are processed completely, accurately, and timely as authorized in accordance with defined processing activities.

Client Issue Tracking

Processing actions are monitored and problems highlighted by the system are identified on a timely basis and assigned to operations for effective disposition. Any client related issues are recorded in AcuTrack and include the client name, a description of the issue, the severity of the issue, and who was assigned to resolve the issue. Any actions taken by ECI are also recorded on the ticket. Once the issue is resolved, the ticket is closed and the date of the closure is noted on the ticket. Acutrack integrated automated process of escalation to monitor issue resolution progress.

Any critical issues are discussed during a weekly management meeting to review the issue, the cause of the issue, and any steps taken to resolve the issue.

Client Data Integrity

Complete and accurate electronic data is maintained on file for each user with the proper version of the data files. Client files are sent via FTP at various times during the day. Once the files are received, they are downloaded approximately every 15 minutes and deposited in a staging directory to wait processing by the system.

As each file is processed, the system checks for any errors in the file. If any errors are found, there is a notification of the error on the NOC console as well as any e-mail that is also sent to the NOC operations staff. The error is researched by the NOC personnel.

Once the file has been successfully processed, it is automatically moved to an archive directory so that the staging area can be “cleaned” for the next batch of files, and ECI can maintain a history of file submissions. In addition, the file processing activity can also be viewed on TrueTrack once the file is processed as well. The TrueTrack system logs the data file source and destination.

Client Output Documents

Client documents are distributed to clients in an electronic format and only authorized recipients may obtain the information. Client output is available via several electronic formats such as FTP, TrueTrack, and UtiliPort. The location of the output information is dependent on the nature of the transaction and the level of service that the client has subscribed to from ECI.

For each output service, ECI has provided security mechanisms that can be used by clients to control access to the output information. For FTP, this can be a simple ID and password that control access to the FTP site. For TrueTrack and UtiliPort, this not only includes an ID and password but also detailed function and screen level security parameters that can be configured by the client.

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring Controls

Control Environment

ECI has a robust control environment to ensure the security, processing integrity and confidentiality of ECI’s data and systems.

ECI has developed and implemented strong information systems policies for all relevant and applicable technologies. Control activities, whether automated or manual, have various objectives and are applied at various organizational and functional levels.

All departments are required to implement control activities that help assure the achievement of business objectives associated with the security, confidentiality, and processing integrity, the effectiveness and efficiency of operations, and compliance with applicable laws and regulations. These control activities are designed to address the specific risks associated with the operations and are reviewed annually as part of the risk assessment process. ECI has developed formal policies and procedures covering these various security, confidentiality, and processing integrity matters to document the requirements for performing many of these control activities.

ECI identifies potential threats that could impair system security, processing integrity, and confidentiality commitments and system requirements, including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system. ECI then analyzes the significance of risks associated with the identified threats and determines mitigation strategies for those risks, including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies. Finally, ECI identifies and assesses changes, (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls), that could significantly affect the system of internal control and then reassesses and revises as necessary, risk assessments and mitigation strategies based on the identified changes.

During the risk assessment and management process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives. In response to the identification of such risks, management updates its policies, procedures, processes, and controls, as needed.

In addition, management identifies sub-objectives related to security, processing integrity and confidentiality to support the achievement of ECI's objectives related to reporting, operations, and compliance.

Processes

ECI's control objectives and related controls are included in Section IV of this report, *EC Infosystems, Inc.'s Trust Services Categories, Criteria, Related Controls, and Test of Controls*, to eliminate the redundancy that would result from listing them in this section and repeating them in Section IV. Although the control objectives and related controls are included in Section IV, they are, nevertheless, an integral part of ECI's description of controls. ECI's management is responsible for the design and implementation of the control procedures.

Logging and monitoring software is used to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security threats and vulnerabilities, and resource utilization and to detect unusual system activity or service requests. This software sends a message to the operations center and security organization and automatically opens a priority incident or problem ticket and change management system record item. Incident response policy is documented and maintained for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints.

ECI's support center documents, records, and resolves or escalates requests received and notifies ECI personnel of potential breaches and incidents. Vulnerability monitoring scans are performed on a periodic basis. Management takes appropriate action based on the results of the scans. Resolution of events is reviewed at the bi-weekly operations and security group meetings.

ECI's employee handbook includes a disciplinary policy for personnel who violate the code of conduct.

Processes are in place to periodically review physical access to ensure consistency with job responsibilities. The appropriateness of access credentials is reviewed on a periodic basis for unnecessary and inappropriate individuals with credentials.

All data is backed up to RAID protected industry standard NAS / SAN devices with multiple levels of redundancy. Periodic audits are carried out to test the integrity of the infrastructure and applications of the provider. Data is hosted at data center with 24x7x365 SLA expectation.

Incident response policy is documented and maintained for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints.

Logical access to information assets, including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components is restricted through the use of access control software and rule sets. ECI identifies, inventories, classifies, and manages information assets.

Network segmentation permits unrelated portions of ECI's information system to be isolated from each other. Points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed. The types of individuals and systems using each point of access are identified, documented, and managed.

New internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required or the infrastructure and software are no longer in use.

Processes are in place to protect encryption keys during generation, storage, use, and destruction.

Application Development

ECI uses a formal system development process in development/maintenance projects to guide programming personnel in the design, coding, testing and implementation of changes. The policy describes the process through the following development phases:

- Initiation
- Feasibility Analysis
- Requirements Definition
- Design
- Development

- Testing
- Release to Production
- Ongoing Maintenance

Change Management

ECI implements a formal change management system development process in the development/maintenance of projects to guide programming personnel in the design, coding, testing and implementation of changes procedure for all system application changes. All changes must follow the documented change management policies and procedures to ensure that changes to the business applications and requests for changes are documented and approved by management prior to commencing work on the project/change and ensure that they are tested in a separate test environment and approved before the change is moved into the production environment. A change control process is formally documented, maintained and reviewed at least annually, wherein management has define configuration standards.

Requests can come from a variety of sources including clients and from internal ECI initiatives. Potential requests are recorded in the AcuTrack system which is used to document the request and includes the following information:

1. Origination of the request
2. Purpose of the request (definition of the problem and how it originated)
3. Time frame for completing the request
4. Priority level (i.e., Critical (Billing or Invoice), Compliance, Nice to Have)

Once a project is approved, it enters the requirements definition, design and development phases to move the project through the system development process. All changes to the ECI client production environment are recorded and tracked. ECI uses Microsoft Project to track the status and progress of each change request.

ECI uses a formal system development process in development/maintenance projects to guide programming personnel in the design, coding, testing and implementation of changes and identifies information specifications required to support the use of products and services.

Code review is required for high impact changes that meet established criteria that mandate code reviews and walkthroughs. These are performed by a peer programmer who does not have responsibility for the change.

Testing is performed in a separate QA/test environment by ECI prior to releasing into the client production environment. The testing phase is designed to demonstrate that the system conforms to the requirements as specified in the functional requirements document. The code will be tested by Quality Assurance staff producing Test Analysis reports to verify that the proper level of testing was performed. The level of testing depends on the complexity of the change and includes, but is not limited to, system testing, integration testing, regression testing, performance testing, automation testing, and user acceptance testing.

An appropriate segregation of duties exists such that the person approving the change to the client production environment is not the same person who is responsible for implementing the change to the client production environment. Changes are discussed and approved during a weekly change control and management meeting that is attended by IT personnel, Client Service personnel, and Project Management personnel. Each change control meeting reviews any changes from the prior week, discusses any changes approved but not implemented from the prior week, and approves new changes for the current week. During the risk assessment and management process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives. In response to the identification of such risks, management updates its policies, procedures, processes, and controls, as needed.

The results of these meetings are documented in the change management meeting memo.

A process exists to manage emergency changes and documented in ECI's change control policy. The IT system includes a change-detection mechanism, (for example, file integrity monitoring tools), to alert personnel of unauthorized modifications to critical system files, configuration files or content files. Procedures are in place to filter, summarize, and analyze anomalies to identify security events. Management has also implemented processes to monitor the effectiveness of detection tools.

Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program and actions are taken, if necessary. Those security events are evaluated to determine whether they could or did result in the unauthorized disclosure or use of personal information and whether there has been a failure to comply with applicable laws or regulations. When an unauthorized use or disclosure of personal information has occurred, the affected information is identified.

Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are assigned, including the use of external resources when necessary.

ECI rolls out changes to the client production environment upon approval of the appropriate IT management personnel. Final go-live approval is required prior to the release update being applied to ECI's systems and applications. Rollback procedures exist to allow the removal of changes, if necessary and every change request includes a rollback procedures exist allowing the removal of changes. Changes to the ECI client production environment are recorded and tracked.

Security patches, determined to be applicable to ECI's environment, are tested and approved prior to being deployed into production. Vulnerability monitoring scans are performed on a periodic basis. Management takes appropriate action based on the results of the scans.

System documentation is provided by and is maintained by ECI. This documentation is updated on a periodic basis or whenever a major change is implemented that supersedes the information on the old documentation. ECI and client users require a user ID and password in order to gain access to its systems.

Physical Security Access

ECI uses a collocation facility which includes physical security, rack space, power (including battery and generator power), internal/external communication connections and cooling.

The independent subservice organization provides a SOC1 report to its clients. As noted above, ECI receives and reviews the SOC report for their procedures and to ensure that there are no noted exceptions. During the course of the year ECI personnel make several visits to our subservice provider to observe that procedures are being followed and determine if there are any issues to be discussed. Any exception reports are sent from the service provider to ECI staff.

There is an access control system at ECI's office to control access to the IT equipment and sensitive data. Access to the data center can only be authorized by ECI's CEO.

Visitors are required to sign-in at the main reception desk and must be escorted in the facility by appropriate personnel. ECI maintains an authorized list of personnel who may have access to the organization's hosting facility.

Procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable. Procedures are also in place to remove data and software stored on equipment to be removed from the physical control of ECI and to render such data and software unreadable.

The types of activities that can occur through a communication channel (for example, FTP site) are restricted. Processes are in place to protect mobile devices (such as laptops, smart phones and tablets) that serve as information assets. Technologies are used to restrict ability to authorize and execute transmission, movement and removal of information.

Procedures are in place to scan information assets that have been transferred or returned to ECI's custody for malware and other unauthorized software and to remove any items detected prior to its implementation on the network.

Logical Security Access Controls

An overall Information Security Policy is maintained by ECI. This policy details ECI's security framework and the expectations of its employees in relation to maintaining a proper information security program. Logical access to information assets, including hardware, data, (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components are restricted through the use of access control software and rule sets.

Access to administer the systems is restricted to authorized personnel. In the ECI environment, this role is limited to the Systems Administrators (SA's), who are members of the Information Systems Department, and work as network, systems, and database engineers/administrators.

There is a process for assigning, modifying, and removing user access to the production system(s). Once a new employee is hired, HR is notified of hiring including role and start date. HR will notify the Information Systems Department who will set the new user up on the various systems that they require to perform their job function. The process for terminating or modifying user access follows a similar process. Authentication controls prevent users from accessing information they are not authorized to view.

ECI uses a complex authentication access system to promote only authorized users. All ECI and client users require a user ID and password in order to gain access to the system. In addition, users must connect via an authorized IP address so as to prevent unauthorized users from accessing the systems from non-client locations. The system also prevents users from accessing records that they are not authorized to view. This is controlled by a combination of the user ID and password and the use of SSL certificates to encrypt the user sessions via the web. External access by personnel is permitted only through a two-factor encrypted VPN connection.

ECI has developed defined username and password standards for access to the ECI domain. The domain password standards enforce the following, but are not limited to: unique user name, a minimum password length of 10 alpha/numeric characters with password complexity enforced; a limit of 5 unsuccessful access requests (keyed to valid user name) before the ID is suspended for 30 minutes, and a password change interval of 52 days. On receiving an exit document, the System Administrator disables access of the terminated personnel within 24 hours.

Network infrastructure includes appropriate firewall protection and is monitored for unauthorized access attempts. The firewall also performs real-time intrusion detection at two different locations in the network. Firewall hardening standards are based on relevant applicable technical specifications that are compared against product and industry recommended practices and updated periodically. Security Incident and Event Management, (IPS, IDS from SonicWALL), software continually collects firewall logs and parses the entries using business rules and known threat signatures. Articiwolf creates alerts the security and network operations teams when anomalous traffic or packets are identified so that firewall rules can be immediately updated to reduce security threat risks in the network, systems, and data stores.

Anti-virus protection is in use throughout the ECI environment and systems are kept up-to-date with recent signature files. All Windows-based computers (clients and servers) connected to the ECI computer network use the AVAST and Carbon Black anti-virus protection software.

Systems are configured appropriately with only necessary patches and upgrades applied. All available updates are evaluated for compatibility in the ECI environment by testing them in the staging environment to ensure they are compatible and reliable prior to installing them into the production environment. For all workstations, a third party tool and group policy facility are used to centrally download and distribute patches.

Security Policies

ECI has developed and implemented information systems policies for all relevant and applicable technologies. The Governance-IT demonstrates independence from management and exercises oversight of the development and performance of internal control. The Governance-IT supplements its expertise relevant to security, processing integrity, and confidentiality, as needed, through the use of a subcommittee or consultants. Management and the Governance-IT consider the need for ECI to interact with and monitor the activities of external parties when establishing structures, reporting lines, authorities, and responsibilities. Therefore, the Governance-IT supplements its expertise relevant to security, processing integrity, and confidentiality, as needed, through the use of a subcommittee or consultants.

The main security policy for ECI is the “Information Security Policy”, which dictates that applicable security principles of security, processing integrity, and confidentiality are defined and designed to support and steer all the measures intended to identify and deal with IS risks. In addition, the thematic security policies are defined for each of the themes such as identity and access management, passwords, remote access, internet access, partner access, networks and telecoms, endpoint security, vulnerability and patch management, third party hosting, usage policy, and printer security. These policies are reviewed once a year by the ECI IT Security Group and are updated. If any changes are made, ECI would be informed during the IS Security Officers meeting.

Procedures are in place to contain security incidents that actively threaten ECI objectives, enabling ECI to analyze security incidents and determine system impact. ECI deploys control activities through policies that establish what is expected and in procedures that put policies into action. Those procedures are in place to mitigate the effects of ongoing security incidents and end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized access, and other remediation actions. Additionally, procedures are in place to restore data and business operations to an interim state that permits the achievement of ECI objectives.

ECI identifies and assesses changes that could significantly impact the system of internal control. To meet its objectives, ECI uses detection and monitoring procedures to identify changes to configurations that result in the introduction of new vulnerabilities, and susceptibilities to newly discovered vulnerabilities. ECI obtains or generates and uses relevant, quality information to support the functioning of internal control and prepares and communicates information about the design and operation of the system and its boundaries to authorized personnel to enable them to understand their role in the system and the results of system operation.

ECI communicates information to improve security knowledge and awareness and models appropriate security behaviors to personnel through a security awareness training program. In doing so, ECI specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

ECI identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. ECI has protocols for communicating security incidents and actions taken to affected parties are developed and implemented. Identified vulnerabilities are remediated through the development and execution of remediation activities. The design of incident response activities is evaluated for effectiveness on a periodic basis.

The conduct of individuals and organizations operating under the authority of ECI and involved in the unauthorized use or disclosure of personal information is evaluated and, if appropriate, sanctioned in accordance with ECI policies and legal and regulatory requirements.

An understanding of the nature, (for example, the method by which the incident occurred and the affected system resources), and severity of the security incident is obtained to determine the appropriate containment strategy, including a determination of the appropriate response time frame, and the determination and execution of the containment approach.

Periodically, management reviews incidents related to security, processing integrity, and confidentiality and identifies the need for system changes based on incident patterns and root causes. Events that resulted in unauthorized use or disclosure of personal information are communicated to the data subjects, legal and regulatory authorities and others as required.

Communications about the nature of the incident, recovery actions taken, and activities required for the prevention of future security events are made to management and others as appropriate, (internal and external). The root cause of the event is determined and additional architecture or changes to preventive and detective controls, or both, are implemented to prevent and detect recurrences on a timely basis.

Lessons learned are analyzed, and the incident response plan and recovery procedures are improved.

Incident recovery plan testing is performed on a periodic basis. The testing includes the development of testing scenarios based on threat likelihood and magnitude; the consideration of relevant system components from across ECI that can impair security, confidentiality and processing integrity; the scenarios that consider the potential for the lack of availability of key personnel; and the revision of continuity plans and systems based on test results.

Personnel Security

ECI has a team of security experts as part of its IT department. As part of the hiring process, ECI performs background checks before the hiring of all its employees to ensure that they are in compliance with ECI ethics policies.

Physical Security and Environmental Controls

ECI is assisted by a subservice organization – Webair - a co-location Data Center residing in Garden City NY that hosts UtiliBill, EC Central, TrueTrack and UtiliPort application production systems and data. In addition, Webair Uniondale, NY a, co-location Data Center residing in Webair Chicago, IL serves as ECI Disaster Recovery site. ECI employees are complying with Webair procedures and controls as it relates to Physical Security and Environmental Controls.

Case Management

ECI has implemented a formal case management procedure to ensure that all issues and incidents are resolved systematically in a consistent and timely manner. ECI uses the AccuTrack ticketing system for its case management solution. Every incident or issue reported by users is logged into the AccuTrack system as a ticket and assigned to the appropriate IT resource. The tickets are assigned a priority, based on which, the internal SLA for resolution is determined. All unresolved tickets are escalated after internal SLA expiration and followed up to ensure timely resolution. IT management regularly tracks ticket resolution performance and takes appropriate actions to ensure smooth functioning of IT systems.

System Account Management

ECI's security policies mandate that, to the extent possible, all user accounts must be unique and named accounts. System accounts are permitted with proper justification. In addition, all default account names and passwords are changed to ensure security of the applications and databases.

Data Backup and Recovery

ECI has documented data backup and recovery procedures to ensure that the critical data and systems are backed up in case of errors and disasters. Critical data is identified and backed up on appropriate recovery points based on data classification using the Veeam, data backup solution. Backup data is replicated to redundant storage at the disaster recovery data center on a continuous basis. The backup job status is monitored on daily basis by the backup administrator and any processing problems are recorded, escalated and appropriately resolved by the technical support personnel.

Access to production (job scheduling) processing control language and executable programs are defined to restrict the ability to execute, modify, delete or create to appropriate individuals. This function is limited to the NOC personnel. Business significant and critical job processing is monitored by ECI to ensure successful and timely completion, including a review and resolution of any exceptions.

Procedures exist to prevent, or detect and correct, processing errors to meet ECI's processing integrity commitments and system requirements. All data is backed up to RAID protected industry standard NAS / SAN devices with multiple levels of redundancy. Periodic audits are carried out to test the integrity of the infrastructure and applications of the provider. Data is hosted at data center with 24x7x365 SLA expectation. Backup and recovery policy is documented, maintained and reviewed quarterly.

The review of ECI's subservice organization SOC reports are reviewed documented and assessed for impact to ECI's control environment. Periodic site visits to the data center are performed by ECI's IT department. Site visits are documented accordingly.

Processing capacity is monitored through weekly inspection of backup device space capacity, system space capacity, and database strength capacity. Critical infrastructure components have a defined level of redundancy based on risk assessment.

The definition of the data is available to the users of the data. The description of the data identifies any information that is necessary to understand each data element and the population in a manner consistent with its definition and intended purpose (meta-data) that has not been included within the data. The population of events or instances included in the data, the nature of each element (for example, field) of the data (that is, the event or instance to which the data element relates); source(s) of the data; the unit(s) of measurement of data elements (for example, fields); the accuracy/correctness/precision of measurement; the uncertainty or confidence interval inherent in each data element and in the population of those elements; the date the data was observed or the period of time during which the events relevant to the data occurred; and the factors in addition to the date; the period of time used to determine the inclusion and exclusion of items in the data elements and population; and the definition is complete and accurate.

Data is stored and maintained completely, accurately, and in a timely manner for its specified life span to meet ECI's processing integrity commitments and system requirements. Backup and recovery policy is documented, maintained and reviewed quarterly. Restoration testing of backup data is performed on a quarterly basis. Backup logs are reviewed by the designated ECI IT and Application team. ECI performs a backup of the production data in accordance with its backup policies. Access to administering and scheduling backup jobs is restricted to authorized personnel. Output is protected when stored or delivered, or both, to prevent theft, destruction, corruption, or deterioration that would prevent output from meeting

specifications. Output is distributed or made available only to intended parties. Procedures are in place to provide for the completeness, accuracy, and timeliness of distributed output. Records of system output activities are created and maintained completely and accurately in a timely manner.

Encryption Controls

Encryption controls protect authentication information and application sessions. ECI protects confidential information during system design, development, testing, implementation, and change processes to meet ECI's objectives related to confidentiality. ECI protects personal information during system design, development, testing, implementation, and change processes to meet ECI's objectives related to privacy. A process is in place to select and implement the configuration parameters used to control the functionality of software and to protect encryption keys during generation, storage, use, and destruction. Objectives affected by system changes are identified, and the ability of the modified system to meet the objectives is evaluated throughout the system development life cycle. Changes in infrastructure, data, software, and procedures required to remediate incidents to continue to meet objectives are identified, and the change process is initiated upon identification.

Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet ECI's objectives during response, mitigation, and recovery efforts. The risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of ECI to meet its objectives.

ECI has established procedures regarding confidential information and backup recovery. Procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained. Procedures are in place to protect confidential information from erasure or destruction during the specified retention period of the information. Procedures are in place to identify confidential information requiring destruction when the end of the retention period is reached. Procedures are in place to erase or otherwise destroy confidential information that has been identified for destruction.

Automated UtiliBill, EC Central, TrueTrack and UtiliPort Application Controls

System output is complete, accurate, and distributed to meet ECI's processing integrity commitments and system requirements. Application regression testing validates key processing for the application during the change management process. EDI data processing is validated by ECI's TrueTrack system. TrueTrack system portal automatically reports inconsistencies in the process to an ECI operator to correct the processing errors. Monitoring of EDI data processing is performed on each business day by the ECI Operations team.

UtiliBill maintains an event log file for data processing. Processing errors are scanned by the UtiliBill module 3 times a day (initiated by the UtiliBill support staff) and a ticket is initiated by ECI's UtiliBill support staff. ECI and client users require a user ID and password in order to gain access to its systems. ECI has developed defined username and password standards for access to the ECI domain. The domain

password standards enforce the following (but are not limited to): unique user name, a minimum password length with password complexity enforced; a limit on the number of unsuccessful access requests (keyed to valid user name) before the ID is suspended, and a password change is required. Processing actions are monitored and problems highlighted by the system are identified on a timely basis and assigned to operations for effective disposition.

Stored items are protected to prevent theft, corruption, destruction, or deterioration that would prevent output from meeting specifications. System records are archived, and archives are protected against theft, corruption, destruction, or deterioration that would prevent them from being used. Procedures are in place to provide for the complete, accurate, and timely storage of data. Records of system storage activities are created and maintained completely and accurately in a timely manner.

Modification of data, other than routine transaction processing, must be authorized and processed to meet ECI's processing integrity commitments and system requirements. Application regression testing validates key processing for the application during the change management process. Access to administer the systems is restricted to authorized personnel. Application installation rights are restricted based on privileged security roles. Authentication controls prevent users from accessing information they are not authorized to view. Access to administering and scheduling backup jobs is restricted to authorized personnel. Backup and recovery policy is documented, maintained and reviewed quarterly. Restoration testing of backup data is performed on a quarterly basis.

Risk Assessment Process

ECI conducts an annual risk assessment of all UtiliBill, EC Central, TrueTrack and UtiliPort applications, which identifies threats which could impact Security, Confidentiality and Processing Integrity requirements. ECI has placed into operation a risk assessment process to identify and manage risks that could affect its ability to provide reliable services to its clients. This process requires management to identify significant risks inherent in the Electronic Data Interchange (EDI) and Billing System Outsource Services processes outlined in this document and relied on by user organizations and to implement appropriate measures to monitor and manage these risks. This process has facilitated the identification of various risks inherent in ECI's operating environment and ECI's management has developed and implemented reasonable measures for the ongoing management and mitigation of these risks. The risks considered by ECI management on an ongoing basis include:

1. Operational and Cyber risk associated with computerized information systems; manual interface in the processes involved in transaction processing; and external systems for client system interfacing.
2. Processing risk associated with, among other things, unresolved errors in the system that are then reflected in users billing.
3. New legislation and the regulatory environment.
4. Competitive landscape.

5. Management conducts an assessment of risk of material misstatement as it relates to achieving control objectives for user entities. Management has implemented various measures to manage risks identified through the risk assessment process.

ECI's risk identification and assessment process includes:

1. Identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles;
2. Assessing the criticality of those information assets;
3. Identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and
4. Identifying the vulnerabilities of the identified assets.

ECI's risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to ECI's information systems.

ECI's consideration of the potential significance of the identified risks includes:

1. Determining the criticality of identified assets in meeting objectives;
2. Assessing the impact of identified threats and vulnerabilities in meeting objectives;
3. Assessing the likelihood of identified threats; and
4. Determining the risk associated with assets based on asset criticality, threat impact, and likelihood.

The assessment of fraud risks includes consideration of threats and vulnerabilities that arise specifically from the use of IT and access to information. The risk identification process considers changes arising from changes in ECI's systems and changes in the technology environment. It also considers changes in vendor and business partner relationships.

Information and Communication Systems

Information and communication systems support the identification, capture, and exchange of information in a form and timeframe that enable people to carry out their responsibilities. The information system consists of procedures, whether automated or manual, and records established to initiate, record, process, and report ECI transactions, as well as events and conditions, and to maintain accountability. The quality of system-generated information affects management's ability to make appropriate decisions in controlling ECI's activities. A high-level description of the information system is provided in the *Overview of Operations* section.

To help align ECI's strategic and tactical decision making with operating performance, management is committed to maintaining effective communication with all personnel. Information comes from both inside and outside the organization and is used to guide ECI strategic and tactical decision making, as well as to measure performance. External communications originate from a number of sources, take many forms

such as e-mail and website postings, and are distributed to a number of destinations. ECI management has focused on establishing multiple channels of external communications to facilitate timely and appropriate communications in an ongoing manner. ECI management monitors internal and external communications on an ongoing basis to assess the effectiveness of these communications.

ECI performs a variety of activities that cover the role of information and communication systems, which ensure that all the users understand the controls that are related to each of the principles and their individual responsibilities in implementing, monitoring and execution of these controls. These include the following activities:

1. The information security staff will perform annual self-assessment walk-throughs of controls with the controls owners prior to audits.
2. ECIIT and Information Security staffs send out email alerts to the users on an as needed basis.
3. All new employees undergo an employee orientation, which includes a review of the HR Manual. A section of the HR Manual covers the roles and responsibilities, acceptable use policies and related IT security and controls information.
4. EC Infosystems has a documented Incident Management Policy, which explains how to identify IT security breaches and the escalation procedures that are communicated to all ECI employees.

Control Activities

Control activities are the policies and procedures that help ensure that management directives are carried out. They help ensure that necessary actions are taken to address risks to the achievement of ECI's objectives. Control activities, whether automated or manual, have various objectives and are applied at various organizational and functional levels. ECI 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.

All departments are required to implement control activities that help assure the achievement of business objectives associated with security, processing integrity and confidentiality. These control activities are designed to address the specific risks associated with the operations and are reviewed annually as part of the risk assessment process. ECI has developed formal policies and procedures covering various matters related to security, processing integrity and confidentiality to document the requirements for performing many of these control activities.

Specific control activities are provided under the *Section IV*.

Monitoring Controls

ECI implements various controls to monitor the security, processing integrity and confidentiality of all UtiliBill, EC Central, TrueTrack and UtiliPort applications. At a high level, ECI management performs annual assessment of the overall IT control environment. For all the critical systems, which include all UtiliBill, EC Central, TrueTrack and UtiliPort applications, an annual risk assessment is performed to monitor and review the impacts, threats and vulnerabilities. ECI also generates and reviews the Key

Performance Indicators of the UtiliBill, EC Central, TrueTrack and UtiliPort applications on a monthly basis with senior management.

ECI IT systems and applications are monitored on a continuous basis using a variety of tools. To ensure the security of the ECI environment, a network based Sonicwall Intrusion Detection/Prevention Systems are deployed, which monitors and blocks the network traffic in case of security breaches. ECI utilizes services from the SISA Information Security for quarterly external and internal vulnerability scanning, including website scanning to monitor for new vulnerabilities. In addition, Articywolf is deployed for log management and security event alerting and reporting to monitor the UtiliBill, EC Central, TrueTrack and UtiliPort applications. ECI has also installed Stealthbit tool to monitor file and folder access permissions and Solarwinds tool to monitor system performance.

Additionally, ECI protects their networks and systems with firewalls, IDS, IPS, SIEM, secure VPN connections, anti-virus software, access control, internet filtering, centralized proactive network monitoring, physical and environmental security controls.

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changes in conditions. The management and supervisory personnel of ECI monitor performance quality and control operations as a normal part of their activities. ECI has implemented a series of "key indicator" management reports that measure the results of various processes involved in providing transaction processing to customers. Key indicator reports identify the causes of differences noted in the reconciliation process and provide for investigation of any deviations of the computerized information system relative to the EDI and Billing Systems.

Daily processing tickets processed through the system are highlighted in the system and are notated by users. The tickets are summarized in real time on screens that are reviewed by staff, investigated and resolved promptly using a three level application review.

Exception reports are proactively and regularly reviewed by the applicable manager and/or supervisor depending on the nature of the item being reported on, and actions, including escalation is taken as necessary. Major exceptions, if any, are referred to higher levels of systems' personnel for review. Users are informed of the disposition of any problems and the system keeps track of the investigation process. Management uses a variety of different types of ongoing and separate evaluations, including penetration testing, independent certification made against established specifications (for example, ISO certifications), and internal audit assessments.

Management exercises reasonable control over operations so that there is an absence of crisis and critical conditions. ECI has employed the services of programmers that have effectuated a high degree of centralized transaction processing and controls. ECI has also strengthened the control environment, promoted segregation of duties and established physical controls among the different levels of personnel.

Management also monitors their subservice organizations through review of applicable SOC reports and periodic site visits.

Disclosure of Security Incidents

There have been no significant security incidents that affected the achievement of the services commitments and systems requirements of the electronic data interchange and billing systems.

Complementary Subservice Organization Controls

ECI uses Webair to provide data center facility services and backup services locations. The accompanying description includes only those controls and related control objectives of ECI, and does not include controls and related control objectives of Webair. This report did not extend to controls of Webair. The below table outlines control activities that are expected to be implemented by our subservice organizations and their applicable trust services criteria.

Control Activity Expected to be Implemented by the Subservice Organizations	Applicable Trust Services Criteria
Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, approved, maintained, and monitored to meet ECI's service commitments and system requirements.	CC 6.8, CC 7.2, CC 7.5, CC 8.1
Recovery plan procedures supporting system recovery are tested to help meet ECI's service commitments and system requirements.	CC 7.5
Logical access security software, infrastructure, and architecture have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, out, and offline elements; and (3) prevention and detection of unauthorized access to meet ECI's commitments and system requirements as they relate to security processing integrity and confidentiality.	CC 6.2, CC 6.3, C1.1
Physical access to facilities housing the system (for Example, data centers, backup media storage and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet ECI's commitments and system requirements as they relate to security, processing integrity and confidentiality.	CC 6.4, C1.1