Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls

January 1, 2022 to September 30, 2022

FORVIS

Mid America Computer Corporation

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls

January 1, 2022 to September 30, 2022

Contents

Section I
Independent Service Auditor's Report

FORVIS

1201 Walnut Street, Suite 1700 / Kansas City, MO 64106
P 816.221.6300 / **F** 816.221.6380
forvis.com

Independent Service Auditor's Report

Board of Directors and Shareholders
Mid America Computer Corporation
Blair, NE

Scope

We have examined Mid America Computer Corporation's (MACC or the Company) description of its Billing and Operations Support system (the System) entitled "Description of Mid America Computer Corporation's Billing and Operations Support System" for processing user entities' transactions throughout the period January 1, 2022 to September 30, 2022 (the description) and the suitability of the design and the operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in Mid America Computer Corporation's Assertion (the assertion). The controls and control objectives included in the description are those that management of the Company believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the System that are not likely to be relevant to user entities' internal control over financial reporting.

The information included in Section V of this report, Other Information Provided by Mid America Computer Corporation, is presented by management of the Company to provide additional information and is not a part of the Company's description of its System made available to user entities throughout the period January 1, 2022 to September 30, 2022. Information about the Company's disaster recovery plan has not been subjected to the procedures applied in the examination of the description of the System and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the System and, accordingly, we express no opinion on it.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of the Company's 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 II of this report, the Company 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. The Company 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 American Institute of Certified Public Accountants. Those standards require that we plan and perform the 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 January 1, 2022 to September 30, 2022. 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 controls involves the following:

- Performing procedures to obtain evidence 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, 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; and

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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 IV of this report.

Opinion

In our opinion, in all material respects, based on the criteria described in Mid America Computer Corporation's assertion:

A. The description fairly presents the System that was designed and implemented throughout the period January 1, 2022 to September 30, 2022.

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 January 1, 2022 to September 30, 2022 and user entities applied the complementary user entity controls assumed in the design of Mid America Computer Corporation's controls throughout the period January 1, 2022 to September 30, 2022.

C. The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period January 1, 2022 to September 30, 2022, if complementary user entity controls assumed in the design of Mid America Computer Corporation's controls operated effectively throughout the period January 1, 2022 to September 30, 2022.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV of this report, is intended solely for the information and use of the Company, user entities of the Company's System during some or all of the period January 1, 2022 to September 30, 2022, 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 user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

FORVIS, LLP

FORVIS, LLP

Kansas City, MO

November 15, 2022

Section II
Assertion and Description Provided by Mid America Computer Corporation

Mid America Computer Corporation
Assertion

We have prepared the description of Mid America Computer Corporation's (MACC or the Company) Billing and Operations Support system (the System) "Mid America Computer Corporation's Description of its Billing and Operations Support System for processing user entities' transactions throughout the period January 1, 2022 to September 30, 2022" (the description), for user entities of the System during some or all of period January 1, 2022 to September 30, 2022, 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 user entities of the System themselves, when assessing the risks of material misstatement of the user entities' financial statements.

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

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

A. The description fairly presents the System made available to user entities of the System during some or all of period January 1, 2022 to September 30, 2022, 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:

   1. 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:

      a. The types of services provided, including, as appropriate, the classes of transactions processed;

      b. 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;

      c. 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;

      d. How the System captures and addresses significant events and conditions other than transactions;

      e. The process used to prepare reports and other information for user entities;

      f. Services performed by a subservice organization, if any, including whether the inclusive method or carve-out method has been used in relation to them;

g. The specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls assumed in the design of the service organization's controls; and

h. 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.

2. Includes relevant details of changes to the service organization's system during the period covered by the description.

3. Does not omit or distort information relevant to the service organization's System, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the System and their user auditors and may not, therefore, include every aspect of the 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 January 1, 2022 to September 30, 2022 to achieve those control objectives if user entities applied the complementary controls assumed in the design of Mid America Computer Corporation's controls throughout the period January 1, 2022 to September 30, 2022. The criteria we used in making this assertion were that:

1. The risks that threaten the achievement of the control objectives stated in the description have been identified by management of the Company;

2. 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; and

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

Mid America Computer Corporation's Description of Its Billing and Operations Support System for Processing User Entities' Transactions Throughout the Period January 1, 2022 to September 30, 2022

Overview of Company & Services

Mid America Computer Corporation (MACC) is a full line service bureau that offers a wide range of computer processing, telecommunications, and professional services to user organizations (customers) in a number of industries. MACC performs processing for over 500 independent telephone, video, broadband, and wireless companies in over 45 states. MACC provides the ability to process billing transactions to accommodate the following offerings:

- Telephone billing
- Carrier access billing
- Video billing
- Wireless billing
- Broadband billing

The following description of controls provided by MACC only applies to operations of telephone billing and carrier access billing, as well as related computer operations. This description is focused on features that may be relevant to the controls of telephone billing and carrier access billing customers, and does not encompass all aspects of the services provided or procedures followed by MACC.

Telephone Billing

The telephone billing system is composed of four processes: polling, mediation, toll processing, and billing.

Polling

Polling is the collection of automated message accounting (AMA) records from the telephone central office switch. AMA records contain details for calls and carry the necessary information to support billing of long distance carrier access, as well as the end user of telephone services. AMA records usually are recorded on premise based equipment that supports electronic reading and remote dial up access and retrieval. The content or format of AMA is unaffected by the actual method employed to collect the data. This function is primarily concerned with the accurate and timely acquisition of the call data and verification that proper message volumes and date ranges are present for a billing cycle or run.

Mediation

Mediation processing takes switch data formats and reformats them into industry standard Electronic Message Interface (EMI) records for end user billing (Toll) or Access Usage Records (AUR) for the Carrier Access Billing System (CABS).

In order to provide the originating or terminating city, state, and other general information, mediation processing requires the use of a telephone industry standard data file referred to as the Terminating Point Master (TPM). This is sold and distributed by Telcordia on behalf of the entire U.S. telephone industry. The Telcordia information is received and updated monthly, generally the last week of the month. The Data Control group downloads the files that contain the information from the Telcordia FTP site. The files are processed by a Data Control staff member who runs a

production job that completely replaces the appropriate test and production, network versions of the TPM reference files.

Other miscellaneous outputs (*i.e.*, individual and unique traffic studies, reports, and summaries) generated by the mediation process support reporting and data requirements of the various states, regional bell operating company (RBOC) regions, and carriers.

Toll Processing

The input to Toll is EMI, which is generated from AMA switch records and call detail records (CDR) sources. EMI is also received from the Centralized Message Distribution System (CMDS) and other miscellaneous sources. The records are processed as they are received, and volumes are validated in accordance with expected norms. The batches are accumulated throughout the month and prepared for billing.

The toll processing determines the “type” of record recorded by the switch in order to find and apply the appropriate rate basis to the detail call. Rating is concerned with determining the originating location/number of the call; the terminating location/number; the date, time, and duration; and billing number in order to properly assign a charge to the call. These key elements are usually the guiding facts for the application of a tariff, provided by either the Local Exchange Carrier (LEC) or the Interexchange Carrier (IXC). Tariffs can be mileage sensitive and require the calculation of straight line distance between two points before the correct charge can be determined. Tariffs also may be applied on a flat rate basis, usually on a per minute or sub-minute basis.

After the company establishes a date for call records to be included on their billing or toll cut, the calls are screened for additional editing, have optional calling plans (OCPs) and/or default rates applied, are guided to a customer billing account, and are summarized for inclusion with the customer’s complete telephone billing statement. A part of the toll process involves the application of customized OCPs and requires client-requested maintenance to stay current with the rules or requirements of these plans. Messages that cannot be guided to a billing account are marked as unbillable and analyzed for “rebill” in a subsequent billing period. Summary totals of billable calls are used for accounting and Purchase of Accounts Receivable Statements (PARS) input and balancing purposes within CABS.

Billing

The billing system prepares and prints the actual customer statements and provides exchange level accounting, balancing procedures, and reports. The main components of the customer statement are the fixed monthly charges sometimes referred to as recurring charges, other charges and credits (OCCs), advertising, toll, and unpaid balances. MACC maintains a complete service order entry telephone business office support package that runs at the customer’s (telephone company) site, usually on a personal computer or network of personal computers. From this software platform, the customer service representatives of the telephone company maintain appropriate records and information related to their subscribers. This package provides for the major support items of service order entry, accounts receivable, OCCs, and a list of other support issues for running a typical telephone business office. In summary, the information under the control and authorization of the telephone company is transmitted to the corporate premises of MACC for inclusion into the final billing process. The toll processing, completely performed on the MACC system, is integrated with the customer data maintained by the telephone company, to produce the final monthly statement. From this process, complete customer statements are prepared and mailed, and accounting information is generated and distributed back to the telephone company along with updated copies of the customer account data files. The telephone business office then resumes normal operations for the next billing cycle.

Carrier Access Billing System (CABS)

An important aspect of telecommunications company operations is the process of billing long distance or IXCs for the cost of originating and terminating calls on their LEC networks. IXCs build and maintain an extensive infrastructure to support the carrying of calls across the entire United States, and the LEC provides the infrastructure for the subscriber to originate or terminate a call. For every call that originates within an LEC facility, there are tariff charges for the components of the local loop that are billable to the carrier of the call. The CABS system must take in all of the originating and terminating call traffic for each LEC; categorize it as to direct dialed, operator handled, 800, 900, directory assistance, etc.; accumulate the minutes of use for the calls originating on the LEC's facilities; and apply the appropriate charges per the tariff. This is done on a carrier by carrier basis, and each of the individual statements, or CABS bills, are remitted to the carriers for payment. When the amount to be billed to a carrier is extremely small, MACC provides a consolidated billing feature for efficiency. The small amounts to be billed by MACC's client companies are consolidated into one bill for presentation to the carrier. The consolidated bill process tracks the individual amounts owed to each LEC, and when the carrier remits payment, the revenue is divided and distributed back to each LEC. This system provides complete analysis of where charges are originating from and tracks payment from each carrier by invoice. There are also aging reports provided to each LEC and a complete procedure for LECs to initiate collection procedures. An additional requirement of the overall process of CABS is the preparation of the PARS. This is the process of reporting to the carrier the billed revenue of all calls. There are other access related processes within the CABS system that provide for billing of specialized services, facilities, shared facilities, and other industry related data preparation.

Customer Master

Customer Master (CM) is a PC based account management application used by the telecommunication user organizations. The primary purpose of CM is to provide monthly billing information based upon initial installations, upgrade of existing services, or the addition of new services for each account on the client's database. Information is transmitted monthly from the telecommunication user organization's remote location or from MACC's hosted application (MSaaS) environment for internal processing at MACC. Transmitted customer data is merged with individual call records to prepare the final monthly bill. As a post-billing operation, the CM data is transmitted back to the telecommunication user organization to reflect final billing information and reporting.

Description of Technical Environment

MACC uses a network production environment consisting of multiple Windows servers with security controlled by Windows active directory. MACC's application systems are supported by offline (batch) data processing activities. The majority of offline computer processing consists of periodic runs to process transaction files, update master files, perform file maintenance functions, and prepare bills and reports. Bills and reports are printed at the data center and mailed to the user organization's location unless the user elects an alternative delivery method.

MACC's network processing environment is supported by the time scheduled execution of script files containing a series of commands to be executed. MACC's production processing environment is controlled by the MACC Scheduler Control (Windows Task Scheduler – Network) which is an automated system used to accurately control production processing.

The CM application resides at the user organization and is run from the user's personal computer (PC). Data for the CM application resides on a Windows® SQL server, also maintained by the user organization. Utilizing the CM application, user organizations transmit and receive data files over data lines from the user's PC to MACC's dedicated Windows based Enhanced File Transfer (EFT) server.

MACC offers a hosted environment for customers to access the applications via the Internet. The application and database are hosted at the MACC facility utilizing the Citrix platform. Customers access the application via a secure Citrix interface.

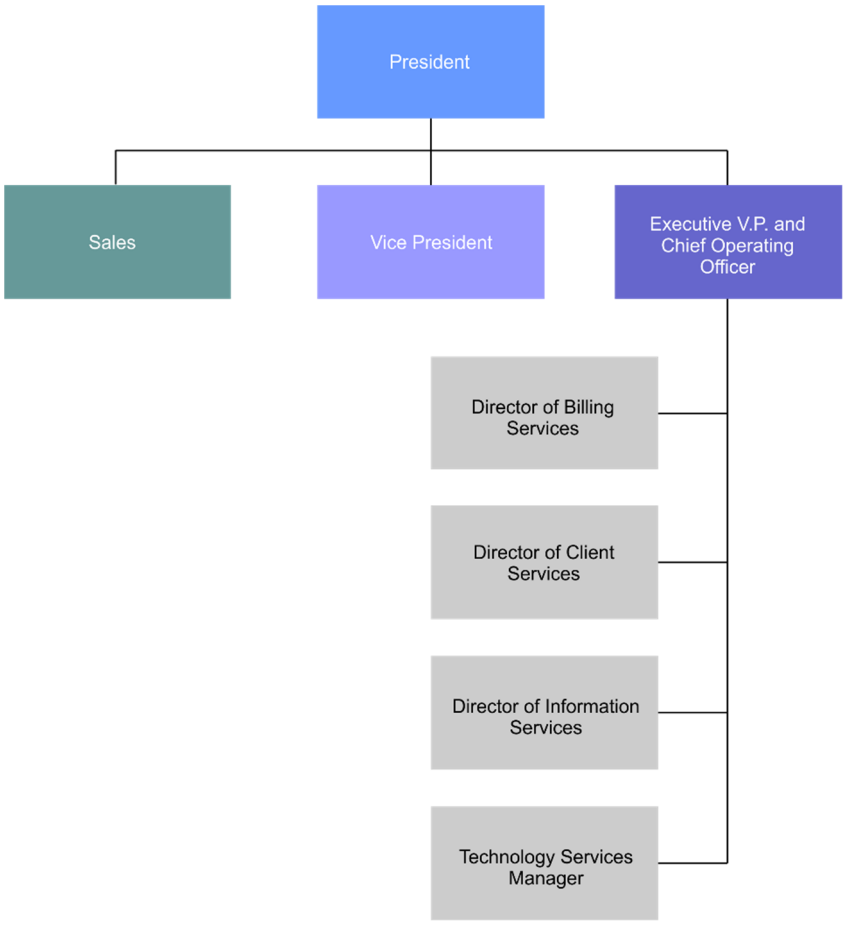
Relevant Aspects of the Control Environment, Risk Assessment Process, Monitoring, & Information & Communication

Control Environment

MACC's control environment reflects the overall attitude, awareness, and actions of the board of directors, management, and others concerning the importance of controls and their emphasis within the organization. The effectiveness of specific controls is established, enhanced, or mitigated by various factors, including:

Organizational Structure

MACC's organizational structure, its management's responsibilities, and its diligence, help to control MACC's activities. Changes to the organizational structure are made periodically to enhance the control environment structure. The assignment of responsibility and delegation of authority to deal with MACC's goals and objectives, operating functions, and regulatory requirements has been completed by MACC's management. The following organization chart identifies individuals with responsibilities for telephone and carrier access billing:



Each area is functionally separate and managed independently, thereby facilitating the separation of duties. MACC has established specific duties and responsibilities for the following areas:

- *Billing Services*: The Billing Services department is involved in the production, support, and fulfillment work for MACC's primary products, including Telecommunications Subscriber Billing and Carrier Access Billing. Billing Services schedules all non-automated production jobs and aids in the correction of day-to-day operational issues that may occur at user organization and MACC. The department is comprised of four divisions: Billing Operations, CABS, Data Control/Management, and Production Programming.
    - *Billing Operations*: This team is responsible for the production of MACC's clients' end user bills. Members of the Billing Operations team print, separate, insert, and mail the statements. During the inserting process, team members also insert target marketing materials into statements as requested by clients. Billing Operations is also responsible for a variety of quality control functions for MACC's clients during bill production. The distribution of billing reports is another responsibility of Billing Operations.
    - *CABS*: MACC's CABS team meets the needs of MACC's CABS clients. The CABS team schedules the production activities to create the CABS bills and reports, and also performs quality assurance on the results of these processes. The CABS team conducts extensive trending and balancing activities for the CABS billing process, and performs analytical review and research related to customer and carrier inquiries. They maintain the tariff, transport, and other tables, which provide key factors for the CABS billing process. The team also coordinates the billing of special access circuits and the Operating Company Number (OCN) billing processes. Team members create Data Master Reports and CD's as needed for MACC clients.
    - *Data Control/Management:* This team controls and maintains the database tables, which control the rating and toll processing of phone calls placed on MACC's clients' networks. The team also manages the company tariffs of MACC's clients which contain the rules and rates for processing calls. These tariffs contain information on rates, holidays, rate periods, and increments for BOC, AT&T, and toll resale carriers. Additionally, the team manages OCP rules, which are applied to calculate special rates for qualifying calls. The Data Control personnel process and validate the accuracy of incoming data using various edit reports. The Data Control team conducts extensive trending and balancing activities for the CABS and End-User billing processes, and performs analytical review and research related to customer and carrier inquiries. The Data Control team is responsible for monitoring and executing all production jobs to ensure all production deadlines are met. When issues are encountered in production jobs, the Data Control team is responsible to ensure issues are resolved.
    - *Production Programming*: Production Programmers provide development and support of computer application systems that are housed at MACC. Production Programmers provide system design, documentation, programming, and other resources necessary to satisfy information processing software requirements from the product specifications. Production Programming also maintains the integrity of production software by controlling migration of software modules and managing MACC's application systems.
- *Client Services*: The Client Services department consists of employees dedicated to servicing user organizations. The primary responsibility of the entire department is customer satisfaction, and Client Services is made up of five distinct areas in order to meet MACC customer needs. The first "hub" consists of the Software Support team, which is responsible for customer telephone consultation and support for MACC software. The second hub is made up of MACC's Training/Conversion Analysts, who are responsible for gathering pre-conversion information, working with customers throughout the entire

conversion process, and then training clients on MACC software post-conversion. Third, the Client Relations Managers and Account Managers are responsible for the day-to-day service to our customers, for all non-software related issues. The fourth hub is the Creative Services team, which handles all marketing, advertising, Web development, and graphics design not only for MACC but also for MACC's customers. Creative Services also manages all MACC events. The fifth hub is Project Management, which is responsible for the management of new company conversions, as well as special projects of existing customers.

- *Software Support:* The primary responsibility of the Software Support team's Software Support Representatives (SSR) is to be readily available for MACC's customers, in order to answer any questions they may have related to the day-to-day use of the Customer Master or Accounting Master programs (and all related modules). The SSR teams provide support Monday through Thursday from 7:00 a.m. through 7:00 p.m. Friday support is available from 7:00 a.m. through 5:00 p.m. The SSR teams also provide software upgrades and upgrade support to MACC's customers, for the two annual releases. Special projects (*i.e.*, hand-keying data, conversion assistance, and new FCC requirements) are also generally assigned to the SSR teams.

- *Training Support*: The Training/Conversion Analysts (TCA) are responsible for collecting client preferences regarding software installations. This includes working with the Sales team and the Project Management team to ensure all pertinent data is collected and verified prior to the conversion. During the conversion, the TCA works with the Project Manager and the Conversion Programmer to ensure data is accurately represented within the database. Post-conversion, TCAs are responsible for training clients on the use of MACC's Customer Master and Accounting Master software. The TCAs also provide Web based and on-site training to existing clients on new releases and other MACC products and services. The TCAs also present and train at MACC events.

- *Client Support*: The staff members of the Client Support team are the Client Relations Managers (CRM) and the Account Managers (AM). The primary representative/liaison between user organizations and MACC are the CRM/AM teams, who provide the daily communication link. The CRM/AM teams maintain contact with the user organizations in order to discuss problems, answer questions, and provide advance notice of upcoming changes. User organizations are encouraged to provide MACC's representative with specific plans and upcoming business needs. The CRM/AM teams assist user organizations by gathering system development requests for enhancements, as well as communicating these requests to the Product Development team. CRMs also make on-site visits to customers, as well as represent MACC at industry meetings. Lastly, the CRM/AM teams present at MACC events and industry meetings (when requested).

- *Creative Services*: The Creative Services team is responsible for all of MACC's marketing and advertising. Advertisements for trade magazines, tracking MACC attendance at state and national conferences, stocking promotional items, managing user group meetings, managing road shows, and managing user conferences are all also handled by the Creative Services team. Additionally, the Creative Services team has been expanded to include customer assistance, when requested, for marketing and advertising materials. Creative Services is responsible for MACC's internal and external websites, and for building websites for customers (when contracted to do so).

- *Project Management*: The primary function of the Project Management team at MACC is to manage new company conversions by serving as the single point of contact to communicate and manage expectations between the customer and our cross departmental project team. For existing MACC clients, the Project Management team

coordinates purchase of exchanges, database merges, carrier changes, wireless implementations, and special projects, etc.

- *Information Services (IS)*: The IS department consists of major areas responsible for the completion of the Product Life Cycle (PLC) efforts to implement MACC supported application enhancements. Below is a description of the teams involved in the IS department and their roles.
    - *Product Development*: MACC must constantly seek to add new functionality and capabilities that enable the products to solve business needs to compete in the area of telecommunications operational support systems and services. Input for enhancements comes from many sources, including MACC's customers, marketing and sales channels, industry and regulatory requirements, and senior management strategic direction. Deliverables from the Product Development team are the preparation of functional specifications to be utilized by programming to develop the supporting code.
    - *Programming*: Programmers provide new development and ongoing maintenance for the various applications supported. Programmers provide technical design, programming, testing, and supporting documentation necessary to satisfy the functional specifications business requirements from the product specifications. Programming also maintains the integrity of production software by controlling migration of software modules and managing MACC's application systems.
    - *Quality Assurance*: Quality Assurance (QA) analysts are responsible for developing, analyzing, and executing test cases on our various software products. Manual and automated test case development supports both new development and regression testing of the applications to ensure quality release distribution. The QA team tracks, documents, and reports uncovered defects from their testing and returns them to the programming team for resolution.
- *Technology Services*: The Technology Services department consists of two teams and is responsible for the technical operations at MACC. Below is a description of these teams and their roles.
    - *Network Services*: The Network Services team is responsible for setup, maintenance, and security of MACC's internal systems that house the production environment. These systems include the virtual infrastructure, centralized storage, backup systems, networking, and firewalls. Within the virtual infrastructure resides multiple servers including Domain Controllers, file servers, exchange servers, database servers, programming production servers, file transfer servers, helpdesk servers, IIS servers, hosted environment servers, and various other components utilized for development, testing, and production. In addition, this team provides installation and support of all internal computers and peripherals for MACC associates. Team members also maintain polling equipment.
    - *Tech Support*: The Tech Support team provides installation and ongoing support of computer hardware utilized by clients in the day-to-day operation of MACC's Customer Master and Accounting Master software. Support is available for clients on an on-site basis and remotely via telephone, email, and remote access applications. Technical Support Specialists also conduct assessments on client environments to inventory hardware and software, then provide recommendations for upgrades if needed. Remote support is available from Monday through Thursday from 7:00 a.m. to 7:00 p.m. and Friday from 7:00 a.m. to 5:00 p.m.
    - *MSaaS Support:* Both of the above teams work together to support MACC's hosted application solution. Support for this environment includes setup of users, files, and databases needed to run MACC's application as well as installation of client

connectivity software for clients, and maintenance and troubleshooting of the environment to keep it operating.

MACC has assigned responsibility and delegated authority to key management personnel to address organizational goals and objectives, operating functions, and regulatory requirements. MACC's employees have no duties, responsibilities, or authority at the user organization.

Human Resources Policies & Practices

Human Resources (HR) policies and practices are documented in MACC's Policies and Procedures Manual. HR controls exist to ensure that qualified competent people are recruited, developed, and retained to achieve MACC's business goals and achieve control objectives. These include controls for hiring, training, evaluating, promoting, and remunerating employees. Prospective employees complete an employment application. Employment is contingent on successful background checks. Employee retention is a high priority, and promotion criteria are clearly established and communicated. Management works with employees to develop their skills and abilities.

Risk Assessment Process

MACC has set clear business objectives and has implemented procedures to assess the key risks affecting achievement of those objectives. MACC recognizes that meeting its business objectives is largely dependent upon how its core software is maintained and perceived within the telecommunications industry.

Monitoring

Monitoring of the internal control systems assesses the quality of the internal control system's performance over time. Ongoing monitoring occurs in the course of operations and includes regular management and supervisory activities, and other actions personnel perform as their duties. Reporting of any deficiencies noted from the ongoing monitoring procedures is communicated to appropriate management representatives. Additionally, management is responsive to external auditor recommendations on means to strengthen internal controls. Other activities (such as those used to evaluate MACC's operations on a financial basis) are monitored by management through the use of strategic plans and budgets.

Management's control methods for monitoring key activities as they relate to the purpose of this report are grouped by control objectives, and are included in Section III, "Mid America Computer Corporation's Control Objectives and Related Controls, and FORVIS, LLP's Tests of Controls and Results of Tests."

Information & Communication

Pertinent control information is critical to maintaining an effective internal control system. Information is identified, captured, and communicated in a form and timetable that enables personnel to carry out their responsibilities in an efficient and effective manner. Reports are produced containing operational, financial, and compliance related information that make it possible to monitor and control the company. MACC utilizes not only internally generated data, but also information about external events, activities, and conditions necessary for business decision making and external reporting. Management stresses the importance of control responsibilities to personnel. This is accomplished through management supervision, as well as through the MACC Policies and Procedures Manual. Personnel understand their duties and roles in the internal control system, as well as how their individual activities relate to the work of others. In most cases, these duties and roles are outlined in their job descriptions. There are also effective means of communication and timely follow-up with external parties, such as customers, media, and governmental entities such as banking regulators. MACC provides to their customers a monthly

newsletter to identify changes that may affect their organization. MACC management is receptive to employee suggestions of ways to enhance productivity, quality, or other improvements to the current products offered by MACC.

Control Activities

MACC's control activities are the policies and procedures in place that help ensure management's directives are carried out. They ensure that necessary actions are taken to address risks to the achievement of MACC's objectives. Control activities occur throughout MACC at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties. Key MACC control activities, as they relate to the purpose of this report, are grouped by control objectives and are included in Section III, "Mid America Computer Corporation's Control Objectives and Related Controls, and FORVIS, LLP's Tests of Controls and Results of Tests."

Description of Transaction Processing

Telephone Billing

Polling

Toll messages are collected for processing at MACC from several sources. The majority of AMA (automated message accounting) message data is electronically collected (polled) via modem or FTP/SFTP connections between MACC and the user organizations' switches. A schedule of daily, weekly, and toll cut polling jobs to be executed, is maintained by the Billing Services Support Manager. Toll messages can also be collected by the user organization and sent to MACC by posting a file of the messages to MACC's Web based EFT server.

Mediation

During mediation, the AMA files from the switch or network are formatted by Mediation for further downstream processing in billing. MACC Billing Data Control personnel are responsible for monitoring activity by tracking transactions throughout Mediation system processing. The team reviews exception-based reports produced by Mediation that identify missing data files, anomalies in daily trend data, gaps in data for selected time frames within a day, and invalid data. In addition, MACC personnel can research anomalies by reviewing reports such as the Batch Analysis (list of files by switch), Trend Analysis (trending by specific time period), GAP Analysis (data gap within a selected time frame for a specific day), as well as the Invalid Data (list of invalid exchanges, 800's, cellular, and recycled data). The exceptions are tracked through the Mediation application for MACC personnel to review and determine if further analysis is appropriate prior to proceeding. Data errors identified during the review are noted within the Exception Tracking user interface (UI) of the application, investigated with the user organizations, and resolved based on the user's verbal or written instructions to MACC personnel.

Toll

Prior to initiating the toll application, the Toll Detail Edit by Exchange/Source (EMED) are systematically compared to defined control totals noted on the company detail (EMEDIT) using a six-month history verification for trending gaps on a daily basis. Exceptions are researched and resolved by Billing Data Control prior to processing.

The EMI detail report (PTED) is generated post-mediation and prior to initiating the toll application. It contains an edit of all third-party CDR toll calls for a customer broken down by source. It is reviewed by an automated process to determine if all polled data has been captured, no gaps exist, and trending of each data source compared to the previous month. If any discrepancy is detected,

an automated email process is initiated to a control group that will investigate the discrepancy and the process is halted. In addition, the MX0120 daily toll counts report is generated out of the toll setup procedure, which details the totals of messages and identifies all carriers received for each day of the period. The remaining toll process, such as message editing, directory assistance, and OCP applications, are executed. Rated calls are collected for inclusion in billing data files, revenue analysis, and customer invoicing.

At the completion of the toll process, an automated process is executed to review the EM0701 Toll report. Exchange information, usage volumes, and revenues are analyzed and trended in the automated process. If variances outside of defined thresholds are encountered in the automated process, an email is sent to a control group, and research is done to verify if the change in data volume is valid.

Billing

User organizations utilizing the CM system are responsible for validating customer information and balancing to prior month's billings. Clients are required to follow a predefined keying sequence when entering customer information. In addition, edit checks (*e.g.*, verifying numeric data, verifying the number of digits, calculating a check digit) are performed on data entered by clients to validate the information prior to processing.

The Customer posts the data files to the EFT server. MACC retrieves the file from the EFT server during the next update process. An automated process runs to check that the exact amount of data posted by the customer is received accurately and completely. If a discrepancy is detected, an automated email process is initiated to a control group that will investigate the discrepancy and the billing process is halted. Another automated process is run immediately following the first verification to compare drop insert information from the customer to a spreadsheet containing drop insert information maintained at MACC. If any discrepancy is detected, an automated email process is initiated to a control group that will investigate the discrepancy and the billing process is halted. During the billing process, an automated process is executed to review the BL5001, BL5002, BL5004, and the BL51A reports to investigate any discrepancies or changes in trends, comparing them to prior months' recurring charges, toll, OCC, taxes, and advertising totals. If variances outside of defined thresholds are encountered in the automated process, an email is sent to a control group, and research is done to verify if the change in data volume is valid.

Special Access Circuit Billing

MACC provides special access circuit billing for Carrier Access Billing System (CABS) customers. Special access circuits provide end-user customers with dedicated lines for their sole use at fixed costs. The billing for this service can be included on the CABS bill, or a direct invoice can be sent to the carrier or end-user. The CABS customer supplies MACC with an Access Service Request (ASR), Work Order Request Document (WORD), or the MACC internal Special Access Reporting Form (SPA000) form. The document(s) are decoded to determine billing information. Information is compared to third-party sources such as NECA Tariff Number 4, LERG, etc., for accuracy and completeness prior to setting up the special access billing information. The circuits are billed based on rates from the company's current access tariff and are updated with each rate change. The CABS customer is notified if any discrepancies are found, and MACC updates the request document accordingly. A SPAC12 report, which summarizes the special circuit billing, is provided monthly to the CABS customer for review. Billing information is reviewed by a second team member before it is released for billing.

Carrier Access Billing

CABS Pre-Loading Process & Review

The CABS process utilizes information received from various sources, including input tapes, from the RBOC and output files generated in the Mediation application. When a file has been received, a preloading process is initiated that verifies the header and trailer, or NPA/NXX, based on specific

tape sort. Records are sorted by Operating Company Number (OCN) identified in the tape. The append (CAAP) and the split (CASP) process are run when the preloading process is complete. If the CAAP/CASP produces a return code due to an NPA/NXX, an error message is sent to CABS Verification for review. If the counts of the calls do not match with the header and trailer information, then Data Control will receive an error message to review and correct.

Prior to initiating the Carrier Access application, the CABS Selection Summary Report (CAPE) is systematically compared to defined control totals noted on the company summary (CA5000) verification for trending gaps. Exceptions are researched and resolved by the Data Control Team prior to processing.

CABS Process & Review

After the CABS pre-load process successfully completes the CABS process, it is run in one combined job called the CASU. If no discrepancies are detected through the automated checks that are in place during this process, it will continue all the way through to the CABS bill (CABL). Each step has automated checks that stop processing if discrepancies are encountered. The first process is the Edit (CAED). An automated email is generated for any discrepancies and sent to a control group who in turn researches and reviews to determine any changes or corrections that are needed. On completion of the CAED process, the data is loaded into an automated load (CALD) trending process to compare current data volumes to previous months' data volumes. If variances outside of the defined thresholds are encountered, an email is generated and sent to a control group for research and review to verify if the volume change is valid.

After completion of the CALD process, the calculation process (CALC) is initiated. An automated verification process detects any calculation error, which generates an error report (CALC100) that is sent to a control group for investigation and correction. Upon correction, a rerun from the beginning of the process is necessary.

After completion of the CALC process, the CABS bills process (CABL) is initiated. An Audit Trail Report and report packet is generated. The final Audit Trail report is reviewed through an automated verification process to verify that billed or dropped data is correct. If discrepancies are detected, an email is sent to a control group for research. This process also generates the bill for the appropriate carrier and generates the following reports: CAB130R (Access Minutes of Use Report), EQ110B- 03 (Equal Access CABS Netting Report), CAPR180 and the CAPR190 summary reports, consolidated billing reports (CAIC0100/CAIC0110 and the CAIC0112) and the EM53 Toll Statement. An automated verification process balances the messages and minutes of use from these reports, and if out of balance errors are detected, will stop processing and auto generate an email to a control group, who would then research and correct any out of balance findings. When all balancing is completed, the post process (CAPS) is initiated and bills are distributed to the carrier for payment.

Consolidated Billing Process & Review

Consolidated billing consists of billing for carriers with lower generated access revenue as requested by the company. At the conclusion of all MACC CABS client billings, the CABS consolidated carrier billing process combines the companies' data that is selected to be billed on a consolidated bill for each carrier. An automated process verifies that the records selected for the consolidated billing process were complete and accurate. If any error is detected, a control group is notified for investigation and correction.

The carrier consolidated bills are then produced, which generates the CAIC1010, CAIC1050-2, CAIC0150, CAIC0170, and CAIC0117 reports. The consolidated carrier billing must balance to the CAIC0117 report before the consolidated carrier bills are printed. The accounting file is also balanced against the reports. All of these reports are also saved online for a minimum of 24 months.

Upon printed completion, the bills are sorted and verified, CD's burned and distributed to carriers. An email is sent notifying MACC personnel that consolidated billing for the month is completed.

Carrier Payments

MACC provides collection and remittance services for CABS customers. This process allows MACC to send one consolidated bill to an IXC on behalf of multiple LECs. MACC receives and collects payments as an authorized representative of the LEC. Once MACC receives payment from the IXC, MACC will promptly remit to the LEC the appropriate portion of the carrier access revenues less any compensation due to MACC as stated in the LEC's general service agreement.

At the completion of the CABS billing process, the CABS Revenue Assurance group receives a download of the CABS accounting file. This file is interfaced into the consolidated billing database, a Paradox database residing on the LAN server. This program tracks the invoice, receipt, payment, adjustment, and dispute information. The collection, accounts receivable, and payment information originate from this database. Access to the consolidated bill database is limited to members of the Revenue Assurance group. After the file is uploaded, the CABS Revenue Assurance group balances the consolidated bill database to the CABS CAIC1050-1 (Summary of Charges by Carrier) and CAIC0170-1 (Summary of Carrier Access Charges by ACNA) reports generated from the consolidated billing process to verify the accuracy and completeness of the interface.

Several monthly reports are generated from the consolidated billing database and forwarded to the customer to assist in reconciling information to MACC's records. These include the accounts receivable cover letter and report, delinquent IXC address list, adjustment letter, and ad hoc reports as requested.

The IXCs receive the bill containing the current month's access charges by company. In addition, the LEC will receive a monthly statement identifying all invoices with outstanding amounts. The outstanding items are identified by invoice number, invoice date, billed amount, credit/adjustments, receipts, balance due, and reference to a dispute number, if appropriate. The statement also contains an aging of the amount indicating current charges, over 30 days, over 60 days, or over 90 days old.

As CABS revenue is received by MACC, it is collected by the accounting department and deposited. The deposit slip and check stubs are forwarded to the CABS Revenue Assurance group, who post the receipts within the consolidated bill database against the appropriate carrier invoice. Bimonthly, MACC generates ACH payments for the user organizations' portion of the collected revenue. Prior to sending the ACH payment, the accounting department verifies the company and correct amount and that each payment is accounted for. With each ACH payment, the user organization receives an email notification with the account receivables aging report and remittance advice along with any reports needed for ACH payment.

In the event a carrier disputes some or all of the charges on the consolidated access bill, a formal dispute process is utilized by MACC to track and resolve dispute issues. Carrier disputes must be in writing and contain the following information: the carrier contact, dispute description, disputed amount by ACNA by invoice and by company, and a total disputed amount. MACC assigns a dispute number and tracks disputes within the consolidated bill database. A help desk issue is created for each dispute and forwarded to CABS personnel for verification and resolution. Upon resolution, the collection database is updated, CABS personnel notify the carrier and the customer of the resolution results with their monthly reports.

Reference File Maintenance

Within the primary telephone billing application, MACC personnel perform updates to the extended area service (EAS) file, tariff master file, and OCP file. EAS changes are initiated by the user organizations for purposes of promotional study, surveys, or rating/toll services. The user organizations call, email, or fax requests to the client service manager, Data Management, or other appropriate personnel. Each change is assigned a Helpdesk work order and forwarded to the Data Management group for review and approval. The Data Management team member working the request puts production processes on hold for the company, if necessary; creates a copy of the production files; and enters the required changes. When the changes have been completed, results are reviewed by another Data Management team member to verify the accuracy and completeness of the changes. Programming is then notified that the updated table can be loaded into Mediation. Once Data Management has been notified of Mediation being updated, the production processes are then taken off of hold. If the EAS change is for a new customer or a new service for an existing customer, it will generally require some coding effort. The help desk issue is then forwarded to the Production Programming Manager for review, approval, and assignment to a developer.

The Data Management group receives and tracks tariff and OCP changes. MACC receives tariff or OCP changes from the RBOCs, IXCs, or their customers. Changes are subject to the same procedures noted above for EAS changes, except the changes are quality checked by the Data Management group after the next production toll run. If errors are noted during the quality check, the customer is placed on hold while the error is corrected, then the Data Management group makes the necessary corrections, and requests a process rerun.

Within the CABS application, MACC personnel will perform updates to the tariff, transport, interexchange, and equal access files as requested by the user organizations. When CABS personnel receive requests for changes, they are logged, and personnel perform the updates to the appropriate tables. Changes are verified by a second member of the CABS group prior to placing the changes into production.

Output Data & Documents

MACC's system generates various reports and other output data reviewed by MACC's personnel. These reports are sent on to the user organizations for their review. The number and type of reports sent to the users varies based on the particular user organization's needs. The user organization has the option to receive through hardcopy, compact disk (CD), digital versatile disk (DVD), or through the EFT server.

For user organizations that choose to receive output in hardcopy, MACC maintains a master checklist of reports to be delivered to each customer. Updates to the master list are informally generated from the customer through the Billing Operations team. These reports are accumulated throughout the billing process and marked off the checklist before mailing to the customer. The checklist is initialed and dated when complete. The customer usually specifies the timing and delivery method of the reports.

For user organizations that choose to receive output on electronic format, MACC utilizes a proprietary application called Data Master. The Data Master application maintains an inventory of output documents and creates disks for distribution to user organizations. The application maintains a list of required reports by user organization, and all reports must be present in the Data Master application before the disk image is extracted from the database. Once the disk image is extracted, MACC can create a CD for a user organization.

If the outside organization chooses to receive its output from the MACC EFT server, it can access the server through HTTPS or Secure FTP. Organizations that utilize an HTTP connection to the EFT server will be automatically redirected to a secure HTTPS connection. Organizations that utilize the FTP method must connect via secure FTP. All users are required to log in with a unique

user ID and password prior to accessing the system. In addition, each organization's data files are maintained in a separate directory structure that is only accessible by that specific user. Sensitive data files are protected with an encrypted password unique to that customer.

Description of General Computer Controls

Application Development & Change Control

MACC has developed a formal system development methodology for use in development and maintenance projects to guide personnel in the design, testing, and implementation of system modifications. While procedures may vary slightly for small projects, the same general approach is utilized to help ensure all programming activity is properly designed, tested, and implemented.

Requests for application program development and maintenance are submitted by users, carriers, companies, or internal departments. MACC has implemented Helpdesk, a help desk/system request tracking application that automates the request process and tracks the request from inception through completion. Each request details the application involved, customer affected, request number, issue, date requested, and date to be implemented. Helpdesk automatically assigns a sequential work order number for each associated task to be completed related to this request. Requests are approved and prioritized during regularly scheduled enhancement and production support meetings. Work efforts on approved projects are then completed by staff members.

Customer Master

For the Customer Master (CM) application, MACC accumulates program fixes and changes into product releases, which are distributed to user organizations twice per year. MACC will receive enhancement and defect management requests from user organizations, Quality Assurance (QA), and other MACC personnel. Each request is logged into the Helpdesk system for tracking. Priorities for each release are identified based upon a business case and presented to senior management by the Product team. Once approved as release content, projects are managed through the Agile SDLC to completion for the release.

Programming for the CM application is performed in combination with Delphi, SQL, and/or Report Builder. Source file revision control for the CM application is performed using the TortoiseSVN automated version control tool. This tool allows team development of software applications to track and store changes to a file allowing programmers to see a file's history and return to earlier versions of a file, if necessary. During the design and development stage, programmers check out programs from the TortoiseSVN tool, and place them into their work directories.

The programmers complete the technical coding requirements of the request and perform appropriate unit and system testing before checking the revised code into the CM build stage of TortoiseSVN. When all requirements for the next build of the CM product are checked in, an updated version of the product is generated, and a document is prepared outlining all help desk issues and work orders included. The new CM product is then sent to the QA team, located in the Information Services area, for extensive testing.

QA analysts review program changes and test results against the help desk issue and/or requirement documentation. If satisfied, the QA analysts approve the coding changes and close the work order. If coding fails validation, a new work order is opened reflecting the outstanding issues and assigned back to the programmer for resolution. This process is repeated for each help desk issue in the CM build until consensus is reached by the MACC management team that the product is ready for client distribution. The Customer Service Representatives (CSR) coordinate with user organizations to arrange uploading of the new CM product release database and executable. A CM

update letter is prepared and distributed to every company reflecting the new functionality included in the product and tips on how to properly utilize the features.

If a problem surfaces with the CM product in production, the company contacts their CSR at MACC, and the problem is verified with a QA representative. If the problem can be replicated, a new help desk work order is opened and assigned to IS for programming and, if required, a new build of the CM product will be generated and distributed following the same process identified above.

Production Applications

Production applications are modified and enhanced by production programmers in the Billing Services department. The programmers update the maintenance log identifying the date, description of work, and work order number. The maintenance log is maintained within the program's source code.

Development is performed in combination with Micro Focus, UltraEdit, and/or Visual Studio. Source file revision control for the Network application is performed using the TortoiseSVN automated version control tool. This tool allows team development of software applications to track and store changes to a file allowing programmers to see a file's history and return to earlier versions of a file, if necessary. During the design and development stage, programmers check out programs from the TortoiseSVN toll, and place them into their work directories.

The code is compiled, and testing is performed in a test environment until all tests are passed. Testing is performed under the direction of the project leader at both the unit and system level. Test data is obtained from prior cycle runs or is generated by program and includes both valid and invalid data in order to test normal processing routines and error handling.

Project leaders review program changes and test results and authorize the code to be moved to the staging folder. Code changes are then automatically copied to the Verification folder only accessible by the Data Control team. Code in the verification folder is then moved to the appropriate Production folder by the Data Control team. When the new code is moved to the Production folder, a backup is made of the previous version of the code.

Once changes are completed, the initiator is notified of implementation. If the initiator is internal to MACC, the notification is made through the automated processes of Helpdesk when the issue is closed. Issue resolution is a required part of the process of closing an issue in Helpdesk. If the initiator of the issue was external to MACC, the single point of contact for the issue would be the MACC staff member that sponsored the issue internally on behalf of the external client. Closure notification is provided via Helpdesk as outlined above, and the single point of contact would complete appropriate follow-up for closure of the issue with the external client.

If a problem surfaces with a program in production after business hours, the operations personnel identifying the problem will notify the appropriate programming team for corrective action. Additionally, they will identify a point of contact who will be responsible for coordinating the movement of the modified code into our production environment.

Logical Access

Security Administration

Addition of new users and updates to existing users is controlled through a standardized form in Helpdesk. The form is completed by the incoming user's manager. The request automatically generates an email message to the Technology Services team. The user's job function, in combination with restrictions provided by the employee's manager, is used to determine the extent of privileges granted. Once the appropriate access has been established, the new user is created, and the request form is filed by Technology Services.

The removal of existing users is controlled through a similar process. The outgoing user's manager submits a form specifying the name of the user and date of termination. The request automatically generates an email to the Technology Services team. Appropriate personnel will revoke the user's access at the end of their regular scheduled shift on their last day unless otherwise specified in the request. Under certain circumstances, network administrators may receive an urgent request from HR or the user's manager and access will be revoked immediately. An email is automatically generated when the user's access has been revoked. The email and request form are filed by Technology Services.

When a user changes positions from within the company, the user's new manager submits a form specifying the change information and permissions required for the new position. The user's access is modified appropriately. The form is then filed by Technology Services.

Local Area Network

Access to the LAN domain is controlled through Active Directory domain security functions. Unique user IDs and passwords are required for all users and administrators. Password parameters are enforced through domain account policies, including password complexity requirements.

Domain auditing settings are in place to log user and system events on the Domain Controllers. Automatic email notifications are sent to network administrators when a user account has been enabled, disabled, locked, or unlocked. Domain activity is tracked through a Security Information and Event Management system (SIEM). Activity details are delivered automatically via daily email reports. The Technology Services team utilizes PRTG software to monitor internal server and service visibility. Failure and return to service notifications are sent via email and text to network administrators.

Technology Services maintains a firewall to restrict traffic access to MACC's DMZ and internal LAN network. The firewall has multiple zones for added layers of security. The WAN zone faces all outside traffic on the Internet with routable public IP addresses. The DMZ zone is for internal servers that need to be accessed from the Internet regularly and is isolated from other internal zones to keep them more secure. The LAN zone is for MACC's internal corporate network. All Internet traffic must pass through the WAN zone prior to entering/leaving any MACC network. All incoming traffic is managed via security rules on the WAN zone that only allow the necessary IP addresses and ports for inbound traffic, such as FTP and Web.

MACC utilizes a third-party security company to perform quarterly external vulnerability scans. The scan results are compiled into a report and delivered to Technology Services for review.

Enhanced File Transfer (EFT) Server

The EFT Server is utilized to transmit and receive data files and output reports between MACC and outside organizations via the Internet. The EFT Server runs on a dedicated Windows based server, which resides in MACC's DMZ. Internal access to the EFT Server is controlled through standard local and domain security functions. External access is controlled through unique login/password authentication from within the EFT interface.

Job Scheduling

The Data Control team is responsible for monitoring and executing all production jobs. The MACC Scheduling Control tool controls the automated scheduling of applications. MACC Scheduling Control features include the ability to identify conditional start times, such as the completion of a review or the existence of a data file. These items are identified, updated, and monitored by Data Control personnel.

Requests for adding jobs to the processing schedule are initiated using electronic mail. Data Control personnel obtain run instructions, modify any XML required, and add the job to the current schedule in the MACC Scheduling Control. Initial service and rerun requests are communicated through email notification. The xmlClient will inform Data Control personnel of processing problems with an abnormal-end notice through email. In the event of an abnormal end, personnel will follow the job restart instructions, if there are any.

Data Control personnel monitor the xmlClient and abends daily to determine if all jobs were completed. If processing problems occur, team members will follow up using email sent to the appropriate personnel identifying projects or issues needing attention for resolution.

Data Backup

Weekly full backups are performed on the production environment every weekend. Full backups begin on Friday night and are staged throughout the weekend for optimal performance. All full backups are finished by Tuesday afternoon and are rotated to a secure off-site facility. Weekly full backups are kept off site in rotation for five weeks. Every fifth backup is then retained for an additional 10 weeks before being rotated back into the queue.

Daily incremental backups are performed on a nightly basis. Incremental backups are performed Monday through Thursday evenings and are taken off site on Friday afternoon. The incremental backups are stored with the corresponding full backups and kept off site during the full rotation schedule.

The off-site location is within a separate, physically secured building located two miles from the data center. The location is monitored closely during business hours. Access to the building is restricted to authorized personnel via key card access. Tapes are stored in a locked cabinet within the facility.

Storage Media

MACC utilizes a Backup-to-Disk-to-Tape (B2D2T) method for backups. Systems are first backed up to disk and verified for data consistency. They are then duplicated to tape and verified to ensure the duplicate copy is consistent with the disk copy. Both virtual and non-virtual servers are backed up to disk, then duplicated to tape using Veeam Backup software. SQL servers are backed up to disk using SQL Native Backup tools. The disk backups are then duplicated to tape using Veeam Backup software.

Physical Security & Environmental Controls

Entrances to MACC's building are restricted to employees through key card access. Various categories of secured areas have been established to restrict personnel to those areas that correspond to their job responsibilities. An employee must scan a key card when both entering and exiting the building. The front entrance to the building is unlocked and monitored by a receptionist during business hours. Visitors, vendors, and any other outside parties must sign in with the receptionist at the front desk prior to being provided with a visitor pass and are escorted by MACC personnel within the building.

Within the building, a secured area has been established for the computer room. This area contains servers, telecommunication equipment, high-speed printers, and storage media, and is situated on the ground floor away from external walls and windows. Access to the computer room is limited to appropriate personnel by key card access. Servers, routers, and other key elements of the Network infrastructure are maintained within the computer room. Visitors within this area must be escorted by authorized personnel.

To gain access to the building and/or the computer room, the employee's supervisor must submit a request form to Human Resources. Human Resources will update the security system to activate the appropriate employee's card to gain access. Upon termination/resignation, the card is retrieved and deactivated immediately. In the event the card cannot be obtained from the employee, the access is deactivated manually. Invalid access attempts are recorded on an access violation report and reviewed after the end of each month for unusual access attempts.

The building is equipped with multiple features to prevent and detect failures that could result in the loss of the computer center's ability to continue processing. These include an uninterruptible power supply (UPS) system, backup diesel generator, environmental temperature and humidity conditioning equipment, and a main power switch to shut down the computer system. The computer center is equipped with separate fire zones, smoke detectors, a sprinkler system, handheld fire extinguisher, and raised flooring. Emergency procedures outline the actions to be taken when damage or loss occurs or becomes an imminent possibility.

Critical pieces of equipment in the computer room are on a maintenance agreement with a specified vendor. Preventive maintenance is performed on a scheduled basis by the original vendor, MACC personnel, or subcontractor. Prescribed preventive maintenance procedures on printers are in place and followed using the vendor's prescribed maintenance and trouble reporting procedures.

MACC utilizes a NAID (National Association of Information Destruction) certified vendor to destroy waste paper. Waste paper is disposed of in locked containers located throughout the building. Each month, the vendor comes on site to MACC to shred the waste paper.

Subsequent Events

Effective October 1, 2022, MACC was acquired by N. Harris Computer Corporation, a provider of mission-critical software for the public sector, healthcare, utilities, and telecom verticals. The sale closed after the reporting period and there were no material changes to MACC's processes prior to the sale date.

Summary

The description presented above is designed to provide the reader a brief description of the activities performed by Mid America Computer Corporation. Mid America Computer Corporation's management believes the activities are appropriate for the services provided.

Mid America Computer Corporation's specific control objectives and related control activities are included in Section III of this report, "Information Provided by Service Auditor, FORVIS, LLP" and captioned as "Provided by Mid America Computer Corporation." Although the specific control objectives and control activities are included in Section III, they are nonetheless an integral part of Mid America Computer Corporation's description of its system and controls.

Complementary User Entity Control Considerations

In designing its system, Mid America Computer Corporation has contemplated that certain complementary controls would be implemented by user organizations to achieve certain control objectives included in this report. This report is restricted to services provided to user entities of Mid America Computer Corporation and, accordingly, does not extend to controls in effect at user entity locations. It is not feasible for all of the control objectives relating to the processing of transactions to be completely achieved through Mid America Computer Corporation's implemented controls. While Mid America Computer Corporation fully achieves some objectives, procedures performed by user entities contribute significantly to the overall achievement of control objectives. This section highlights procedures that should be considered by user entities in order to fully achieve desired control objectives. Other control objectives may be defined by the user entities and must be achieved solely by the user entity.

Complementary User Entity Controls

Telephone Billing (Control Objectives 1 & 2)

- Controls should be in place at the user entity to ensure that all data (*i.e.*, transactions) related to MACC have been input completely and accurately.
- Controls should be in place at the user entity to ensure that all message data is recorded by the switch and is retained for at least 45 days.
- Controls should be in place at the user entity to ensure that all message data and toll transactions are completely and accurately rated.
- Controls should be in place at the user entity to ensure that the subscriber summary balance report (BL51), which identifies the balance due, recurring, toll, and other charges processed in the billing application, is reviewed to ensure all amounts are appropriate.
- Controls should be in place at the user entity to ensure that reviews and investigation of all unbillable or dropped calls are performed by reviewing the BL41U unbillable toll report.
- Controls should be in place at the user entity to ensure that reviews and investigation of all unbillable or dropped calls are performed by reviewing the MX5001 Unselected Current Toll Data report.
- Controls should be in place at the user entity to ensure that monitoring and trending information related to toll amounts and message counts are performed.
- Controls should be in place at the user entity to ensure that service order, cash receipt, and adjustment transactions are authorized, and input completely and accurately.
- Controls should be in place at the user entity to ensure that correction to service order, cash receipt, or adjustment transactions are authorized and input completely and accurately.
- Controls should be in place at the user entity to ensure that all discrepancies in customer-controlled variables are resolved in a timely manner.
- Controls should be in place at the user entity to ensure that access to the Customer Master application is limited to authorized personnel.
- Controls should be in place at the user entity to ensure that Customer Master users validate and balance their data files prior to posting the files to the EFT server.

Carrier Access Billing (Control Objectives 3, 4, & 7)

- Controls should be in place at the user entity for reviewing and ensuring that all carrier access messages are rated completely and accurately and recorded in the proper period. User entities should review the CAB130, EQ110, and CA241 reports to ensure completeness and accuracy of the feature group D billing processes. User entities should be reviewing the CAIC0100 report detailing the billed messages for each carrier to ensure completeness and accuracy.
- Controls should be in place at the user entity for reviewing and ensuring that charges are processed completely and accurately. User entity should perform a review and reconciliation of the monthly reports received by the user entity, including the accounts receivable report, delinquent IXC address list, adjustment letter, remittance advice, and special access circuit billing summary (SPAC12 report).
- Controls should be in place at the user entity for reviewing and ensuring that receipts are processed completely and accurately. User entity should perform a review of the remittance advice and timely notifications to MACC of any disputed items or adjustments.

Reference File Maintenance (Control Objective 5)

- Controls should be in place at the user entity to ensure that changes to externally controlled data performed by MACC personnel are authorized and recorded completely and accurately.
- Controls should be in place at the user entity to ensure that changes to user controlled hardware/software modifications are authorized and input completely and accurately including, but not limited to, changes in the composition of the data such as software changes and maintenance to the switch.
- Controls should be in place at the user entity to ensure that schedules of all tariffs, tables, and service charges for the telephone and carrier access billing applications are provided to the service organization on a timely basis including, but not limited to:
    - Access rates
    - Customer information
    - Unit sensitive pricing table
    - Intra-LATA OCP tables
    - Information related to the rebilling of any intra-LATA or inter-LATA toll messages
    - Changes in existing billing formats, rating, and OCP

Output Data & Documents (Control Objective 6)

- Controls should be in place at the user entity to ensure that output documents received are reviewed by appropriate personnel at the user entity in a timely manner.
- Controls should be in place at the user entity to ensure that knowledge of sensitive passwords to MACC EFT server and encrypted files are limited to appropriate personnel.

System Development & Application Changes (Control Objective 8)

- Controls should be in place at the user entity to ensure that appropriate management personnel authorize system enhancement requests.

Logical Access (Control Objective 9)

- Controls should be in place at the user entity for granting application software, system software, and data files access to authorized user entity users and removing access as necessary.
- Controls should be in place at the user entity to ensure that data files are transmitted to MACC using a secure method.

Data Backup (Control Objective 11)

- Controls should be in place at the user entity to ensure that all message data transferred to the service organization via magnetic tape be retained for at least 60 days.

Section III
Information Provided by Service Auditor, FORVIS, LLP

Information Provided by Service Auditor, FORVIS, LLP

Mid America Computer Corporation provided an assertion and description of the system included in Section II of this report, "Assertion and Description Provided by Mid America Computer Corporation."

This section presents the following information provided by Mid America Computer Corporation.

- The control objectives specified by management of Mid America Computer Corporation.
- The controls established and specified by Mid America Computer Corporation to achieve the specified control objectives.

Also included in this section is the following information provided by FORVIS.

- A description of the procedures performed by FORVIS to determine whether Mid America Computer Corporation's controls were properly designed, placed in operation and operated effectively to achieve the specified control objectives throughout the period.
- The results of FORVIS' procedures.

Types & Descriptions of the Tests of Operating Effectiveness

Type	Description
Inquiry	Inquired of appropriate personnel regarding, among other things: • Knowledge of and additional information regarding the control policy or procedure; and • Corroborating evidence of the control policy or procedure.
Inspection	Inspected documents and records indicating performance of the controls. These procedures may include, among other things: • Inspection of reconciliations, including supporting source file information, and management reports; • Examinations of source documentation and authorizations to verify validity of information; • Examination of documents or records for evidence of control performance; and • Inspection of system documentation.
Observation	Observed the application or existence of specific controls as represented.
Re-performance	Re-performed the control, or processing of the application control, to confirm the accuracy of its operation. These procedures may include, among other things: • Obtaining evidence of the accuracy and correct processing of transactions by performing independent calculations; and

Type	Description
	• Re-performing the matching of various system records by independently matching the same records to the Client's prepared reconciliations, if applicable.

Control Objective Matrices

Figure 1 – Toll Messages			
Control Objective – Provided by Mid America Computer Corporation			
Controls provide reasonable assurance that toll messages are input and processed completely and accurately.			
Provided by Mid America Computer Corporation		***Provided by FORVIS***	
Control Activity		***Testing Procedures***	***Test Results***
1.	A schedule of the weekly polling jobs is maintained and executed by the scheduling department.	Inquired of the Billing Services Support Manager regarding toll-cut polling job sheets. Inspected sign off sheets for a sample of weeks noting that a schedule of polling jobs is maintained and executed.	No exceptions noted
2.	Systematic gap and trending analysis is performed over the AMA, EMI, and AUR files. Significant variances are researched and resolved.	Inquired of the Billing Services Support Manager regarding gap and trending analysis. Inspected the gap analysis performed within the Exception Tracker for a sample of exceptions noting variances are researched and resolved.	No exceptions noted
3.	Access to modify the gap and trending thresholds is restricted to authorized personnel.	Inquired of the Billing Services Support Manager regarding individuals with access to modify gap and trending thresholds, noting they are authorized. Inspected a list of users with access to Data Mediation and traced users to the company organizational chart for reasonableness.	No exceptions noted
4.	Mediation systematically prevents transmitting of AUR and EMI files without a manual review in the event of open file exceptions identified during the monthly transmitting process. The system logs the user, date, and response for transmitting the files with unaddressed exceptions.	Inquired of the Billing Services Support Manager regarding gap and trending analysis. Inspected the gap analysis performed within the Exception Tracker for a sample of exceptions, noting that exceptions are reviewed. Inspected Data Mediation noting that the system requires manual review of exceptions and logs the user, date, and response.	No exceptions noted

Figure 1 – Toll Messages			
Control Objective – Provided by Mid America Computer Corporation			
Controls provide reasonable assurance that toll messages are input and processed completely and accurately.			
Provided by Mid America Computer Corporation		***Provided by FORVIS***	
Control Activity		***Testing Procedures***	***Test Results***
5.	Prior to initiating the toll application, the Toll Detail Edit by Exchange/Source (EMED) is systematically compared to defined control totals noted on the company detail (EMEDIT) using a six-month history verification for trending gaps. Exceptions are researched and resolved by Billing Data Control prior to processing.	Inquired of the Billing Services Support Manager regarding EMED reports. Inspected the EMED reports and evidence of resolution for a sample of exceptions.	No exceptions noted
6.	Prior to initiating the toll application, the Toll Detail Edit by Exchange/Source (PTED) are systematically compared to defined control totals noted on the company detail report (MX0110) using a previous month history verification for trending and six-month history verification for gap trending, exceptions are researched and resolved by Billing Data Control prior to processing and/or initiating a rerun.	Inquired of the Billing Services Support Manager regarding PTED reports. Inspected the PTED report and evidence of resolution for a sample of PTED exceptions identified.	No exceptions noted
7.	At the completion of the toll processing, the Toll Processing Counts (EMTL) are systematically compared to defined control totals noted on the company summary report (EM0701) using a six-month history verification for trending. Exceptions are researched and resolved by Billing Data Control prior to processing and/or initiating a rerun.	Inquired of the Billing Services Support Manager regarding EMTL reports. Inspected the EMTL reports and evidence of resolution for a sample of EMTL exceptions identified.	No exceptions noted
8.	Access to update production for TOLL trending sign offs is restricted to the authorized personnel based on job responsibilities.	Inquired of the Billing Services Support Manager regarding individuals with update rights to the production environment, noting individuals are authorized. Inspected a list of individuals with access to update production and traced to the organization chart for reasonableness.	No exceptions noted

Figure 2 – Account Records			
Control Objective – Provided by Mid America Computer Corporation			
Controls provide reasonable assurance that billing records are guided to the respective customer's account completely and accurately.			
Provided by Mid America Computer Corporation		***Provided by FORVIS***	
	Control Activity	***Testing Procedures***	***Test Results***
1.	The Customer Master application has built in edit checks to prevent incomplete or inaccurate entry.	Inquired of the Software Support Manager regarding Customer Master edit checks. Observed a test transaction noting that various edit checks are in place to prevent incomplete or inaccurate entry.	No exceptions noted
2.	The billing system compares and validates the bill cut data prior to executing the pre-bill (verification job ran) job. Errors, if any, are corrected.	Inquired of the Billing Services Support Manager regarding bill cut verification jobs. Inspected the BMPT email configurations, noting that emails are sent upon error. Inspected the BMPT emails and evidence of resolution for a sample of abends.	No exceptions noted
3.	Prior to billing, customer data are systematically compared to defined control totals noted on the company summary (BL51A), six-month trending (BL5001), and 12-month bill master verification history (BL5002). Exceptions are researched and resolved by Billing Data Control prior to processing.	Inquired of the Billing Services Support Manager regarding BL reports. Inspected the BL reports showing the results of the systematic comparison of control totals and evidence of resolution for a sample of companies that resulted in BL errors.	No exceptions noted

Figure 3 – CABS Billing			
Control Objective – Provided by Mid America Computer Corporation			
Controls provide reasonable assurance that carrier access messages are input and processed completely and accurately.			
Provided by Mid America Computer Corporation		***Provided by FORVIS***	
	Control Activity	***Testing Procedures***	***Test Results***
1.	Prior to initiating the Carrier Access application, the CABS Selection Summary Report (CAPE) is systematically compared to defined control totals noted on the company summary (CA5000) verification for trending gaps. Exceptions are researched and resolved by Billing Data Control prior to processing.	Inquired of the Billing Services Support Manager regarding the automated CAPE reports. Inspected CAPE reports showing the results of the systematic comparison of control totals and evidence of resolution for a sample of CAPE exceptions identified.	No exceptions noted
2.	An automated CAED verification process is initiated to validate exchanges, data sources, and monthly modifications changes within the billing period. A control group is notified of any needed corrections.	Inquired of the Billing Services Support Manager regarding the automated CAED verification process. Inspected verification emails and CAED review reports for a sample of CAED errors.	No exceptions noted
3.	An automated trending report is initiated for the CALD process comparing carrier minutes of use (MOU) records from the prior three-month report data. Variances outside of defined thresholds are researched and resolved by the control group.	Inquired of the Billing Services Support Manager regarding automated trending reports. Inspected the trending reports and evidence of remediation for a sample of CALD errors.	No exceptions noted
4.	An automated CALC verification process is initiated that detects any calculation errors. An email is generated to the control group for correction. Any calculation correction would require reprocessing the data.	Inquired of the Billing Services Support Manager regarding the automated CALC verification process. Inspected the automated email and evidence of resolution for a sample of CALC errors.	No exceptions noted
5.	An automated verification process is initiated to balance messages and minutes from the CAPR180 and CAPR190 (Summary Reports), EQ110b-03 (CABS Netting Reports), EM53 (Toll Reports) validating the data and report accuracy. An auto-generated email for any balancing discrepancies is initiated to a control group for research and correction.	Inquired of the Billing Services Support Manager regarding the automatic CAPR verification process. Inspected the emails, reports, and evidence of remediation for a sample of CARV/CABL errors.	No exceptions noted

Figure 3 – CABS Billing			
Control Objective – Provided by Mid America Computer Corporation			
Controls provide reasonable assurance that carrier access messages are input and processed completely and accurately.			
Provided by Mid America Computer Corporation		***Provided by FORVIS***	
Control Activity		***Testing Procedures***	***Test Results***
6.	Access to update production for CABS trending sign offs is restricted to the authorized personnel based on job responsibilities.	Inquired of the Billing Services Support Manager regarding individuals with the ability to update production, noting individuals are authorized. Inspected a list of individuals with the ability to update production and traced to the organization chart for reasonableness.	No exceptions noted

Figure 4 – CABS Billing			
Control Objective – Provided by Mid America Computer Corporation			
Controls provide reasonable assurance that carrier payments are input and processed completely and accurately.			
Provided by Mid America Computer Corporation		***Provided by FORVIS***	
	Control Activity	***Testing Procedures***	***Test Results***
1.	Access to the Consolidated Billing Database is restricted to authorized personnel based on job responsibility.	Inquired of the Billing Services Support Manager regarding individuals with access to the Consolidated Billing Database, noting individuals are authorized. Inspected a list of Consolidated Billing Database users and traced users to the company organization charts for reasonableness.	No exceptions noted
2.	The Consolidated Billing Database is reconciled to the Summary of Carrier Access Charges report (CAIC0117-1) after the CABS accounting file upload.	Inquired of the Billing Services Support Manager regarding the consolidated CABS reconciliation. Inspected the Summary of Carrier Access Charges report and the CABS account files for a sample of months, noting that the totals have been reconciled.	No exceptions noted
3.	Prior to sending, payments are reviewed and balanced by a member of the CABS Revenue Assurance group and reconciled by the Accounting Group.	Inquired of the Accounting Manager regarding the payment review process. Inspected the paradox report balancing queries for a sample of months, noting that payments are balanced. Inspected the ACH payment listing and check listing for a sample of months and traced amounts to the Payment and Transfers sheets, noting that amounts have been reconciled.	No exceptions noted
4.	MACC utilizes a formalized dispute process for tracking and resolving CABS payment dispute issues for MACC collect companies.	Inquired of the Billing Services Support Manager regarding the formalized CABS payment dispute process. Inspected the dispute reporting tool noting that a formalized process is in place for tracking and resolving CABS payment dispute issues. Inspected the dispute reports for a sample of months, noting that disputes were tracked and resolved.	No exceptions noted

Figure 5 – Reference Files			
Control Objective – Provided by Mid America Computer Corporation			
Controls provide reasonable assurance that reference file transactions are processed completely and accurately.			
Provided by Mid America Computer Corporation		***Provided by FORVIS***	
	Control Activity	***Testing Procedures***	***Test Results***
1.	Access to change reference files is limited to authorized users based on job responsibility.	Inquired of the Billing Services Support Manager regarding users with access to change reference files, noting users are authorized. Inspected a list of Production Control Group members and traced to the company organization charts for reasonableness.	No exceptions noted
2.	CMS reference file changes and Tariff reference file changes are reviewed by a second team member before implementation.	Inquired of the Billing Services Supervisor regarding reference files changes. Inspected the review ticket created for a sample of reference file changes, noting that a second team member reviewed the change before implementation.	No exceptions noted
3.	A review of user access is performed annually by management to detect and remove unnecessary or unauthorized access.	Inquired of the Billing Services Support Manager regarding the user access review. Inspected the annual review performed on users with access to modify reference files.	No exceptions noted

Figure 6 – Output Data & Documents			
Control Objective – Provided by Mid America Computer Corporation			
Controls provide reasonable assurance that output data and documents are complete and distributed to the appropriate user entities.			
Provided by Mid America Computer Corporation		***Provided by FORVIS***	
Control Activity		***Testing Procedures***	***Test Results***
1.	A master checklist is maintained for each company each month for reports, output data, and documents in hard copy to control accuracy of the output data and documents.	Inquired of the Billing Services Support Manager regarding the monthly company checklists. Inspected completed company checklists for a sample of companies and a sample of months, noting the accuracy of output data and documents is controlled.	No exceptions noted
2.	A reconciliation of the CD Burn Log is performed between client requests for billing information on a CD and the CDs created.	Inquired of the Billing Services Support Manager regarding CD burn log reconciliations. Inspected the burn log reconciliation logs for a sample of months and a sample of companies noting, that a reconciliation is performed.	No exceptions noted
3.	EFT server and File Transfer Protocol (FTP) users are required to log on with a unique user ID and password prior to accessing the system.	Inquired of the Technology Services Manager regarding EFT and FTP sites. Inspected the client logon screens requiring a username and password. Inspected the password configurations.	No exceptions noted
4.	Each client organization's data files are maintained in a separate directory structure that is only accessible by that specific user.	Inquired of the Technology Services Manager regarding client data files. Inspected the directory structure, noting separate folders and permissions for each client.	No exceptions noted
5.	Sensitive data files are uniquely encrypted and password protected to each customer.	Inquired of the Technology Services Manager regarding data file encryption. Inspected the password requirement for decrypting files. Inspected the script command that is used to encrypt the files.	No exceptions noted

Figure 7 – Special Access Circuit Billing			
Control Objective – Provided by Mid America Computer Corporation			
Controls provide reasonable assurance that special access circuit billing information is entered completely and accurately.			
Provided by Mid America Computer Corporation		***Provided by FORVIS***	
Control Activity		***Testing Procedures***	***Test Results***
1.	A second Special Access member reviews billing information for circuits entered into the system.	Inquired of the Billing Services Support Manager regarding new circuits. Inspected the special access check off spreadsheet for a sample of new circuits, noting that a review was performed.	No exceptions noted
2.	A SPAC12 report, summarizing special access billing, is provided to the CABS customer each month for auditing purposes.	Inquired of the Billing Services Support Manager regarding SPAC12 reports. Inspected the SPAC12 reports delivered to clients for a sample of companies and a sample of months.	No exceptions noted
3.	Annually, the Special Access billing rates are changed based on the tariff rates.	Inquired of the Billing Services Support Manager regarding the annual changes to the Special Access billing rates. Inspected the SPAC12 reports and traced rates to the 2022 NECA reference guides or interstate rates for a sample of companies, noting that rates were updated.	No exceptions noted

Figure 8 – Application Development & Maintenance			
Control Objective – Provided by Mid America Computer Corporation			
Controls provide reasonable assurance that changes to existing applications and the development of new applications are authorized, documented, tested, moved into the appropriate operating libraries, and communicated to relevant client personnel.			
Provided by Mid America Computer Corporation		***Provided by FORVIS***	
Control Activity		***Testing Procedures***	***Test Results***
1.	The source code library is configured to prevent duplicate checkout and record program version.	Inquired of the Director of Information Services regarding source code library. Observed an attempt to check out a code that is locked by another user, noting the prevention of duplicate code check out. Inspected the version history log, noting that program version is recorded in the source code library.	No exceptions noted
2.	Unit, system, and QA testing are performed with documented test plans and manual or automated test scripts.	Inquired of the Director of Information Services regarding test plans. Inspected the tickets showing testing performed and associated test plans and test scripts for a sample of version releases and a sample of enhancements.	No exceptions noted
3.	Product Managers and MACC Management approve releases prior to being implemented to production.	Inquired of the Director of Information Services regarding implementing releases into production. Inspected approvals for a sample of releases.	No exceptions noted
4.	With each release, a Customer Master (CM) update letter is prepared and distributed to user organizations via the customer portal, reflecting the new functionality included in the product, and tips on how to properly utilize the features.	Inquired of the Director of Information Services regarding CM update letters. Inspected the CM update letter and evidence of distribution on the MACC website for a sample of releases.	No exceptions noted
5.	Application development and testing occurs in an environment separate from production.	Inquired of the Billing Services Support Manager regarding application development. Observed separate environments for development, test, and production.	No exceptions noted

Figure 8 – Application Development & Maintenance			
Control Objective – Provided by Mid America Computer Corporation			
Controls provide reasonable assurance that changes to existing applications and the development of new applications are authorized, documented, tested, moved into the appropriate operating libraries, and communicated to relevant client personnel.			
Provided by Mid America Computer Corporation		***Provided by FORVIS***	
Control Activity		***Testing Procedures***	***Test Results***
6.	Project leaders review program changes and test results prior to authorizing the migration of the change to production.	Inquired of the Billing Services Support Manager regarding program changes. Inspected evidence of review of test results for a sample of program changes.	No exceptions noted
7.	Access to promote changes into production environments is restricted to authorized personnel.	Inquired of the Billing Services Support Manager regarding individuals with access to promote changes to production, noting individuals are authorized. Inspected a list of individuals with access to promote changes to production and traced to the organization chart for reasonableness.	No exceptions noted

Figure 9 – Logical Access			
Control Objective – Provided by Mid America Computer Corporation			
Controls provide reasonable assurance that logical access to application software, system software, and data files are protected from unauthorized access or change.			
Provided by Mid America Computer Corporation		***Provided by FORVIS***	
	Control Activity	***Testing Procedures***	***Test Results***
1.	The organization has established an authentication mechanism for information systems that provides for individual accountability.	Inquired of the Technology Services Manager regarding the authentication mechanism for information systems. Inspected the Active Directory user report, noting no shared accounts.	No exceptions noted
2.	Management has defined and implemented Domain password standards with expiration requirements and a 16-character minimum length.	Inquired of the Technology Services Manager regarding password requirements. Inspected the Default Domain Policy and MACC password policy, noting expiration and minimum length requirements.	No exceptions noted
3.	Access to administrator privileges and functions is restricted to personnel with responsibility for performing system administrative functions.	Inquired of the Technology Services Manager regarding personnel with administrator privileges. Inspected the list of administrators and traced to the organization chart for reasonableness based on job functions.	No exceptions noted
4.	New hires and role changes are formally documented and authorized by management.	Inquired of the Technology Services Manager regarding new hires and role changes. Inspected the tickets created for a sample of new hires and role changes, noting that they are formally documented and authorized by management.	No exceptions noted
5.	System and application level access granted to an individual is revoked in a timely manner when the individual is terminated.	Inquired of the Technology Services Manager regarding system and application-level access termination. Inspected the automated email noting that the account has been disabled for a sample of terminated employees.	No exceptions noted
6.	Account creation and lockout events are defined within the Windows Task Scheduler and email alerts are sent to domain administrators when security events are identified.	Inquired of the Technology Services Manager regarding security events. Inspected the Windows Task Scheduler configurations showing definition of security events and notification configurations. Inspected email notification alerts.	No exceptions noted

Figure 9 – Logical Access			
Control Objective – Provided by Mid America Computer Corporation			
Controls provide reasonable assurance that logical access to application software, system software, and data files are protected from unauthorized access or change.			
Provided by Mid America Computer Corporation		***Provided by FORVIS***	
Control Activity		***Testing Procedures***	***Test Results***
7.	A review of user access is performed annually by management to detect and remove unnecessary or unauthorized access.	Inquired of the Technology Services Manager regarding periodic user access reviews. Inspected the most recent annual user access review performed by management.	No exceptions noted
8.	Security events are monitored by the SIEM and alerts are reviewed and verified by the Technology Services team when received. Automated monthly summary reports are also reviewed for additional validation.	Inquired of the Technology Services Manager regarding the SIEM tool. Inspected the SIEM tool notification configurations noting that daily emails are sent. Inspected the monthly emails along with evidence of review for a sample of months.	No exceptions noted

Figure 10 – Job Scheduling			
Control Objective – Provided by Mid America Computer Corporation			
Controls provide reasonable assurance that job schedules are prepared, executed, and deviations are tracked through to resolution.			
Provided by Mid America Computer Corporation		***Provided by FORVIS***	
Control Activity		***Testing Procedures***	***Test Results***
1.	Job schedules are monitored through the automated MACC Production scheduler. Deviations from scheduled processing are researched and resolved by Data Control personnel.	Inquired of the Billing Services Support Manager regarding job scheduling. Observed the XML Automated job scheduler folders. Inspected resolution for a sample of deviations noting that they are researched and resolved.	No exceptions noted
2.	Administrator access to the MACC Production Scheduler is appropriate and restricted to limited personnel.	Inquired of the Billing Services Support Manager regarding administrator access to the job scheduler, noting individuals are authorized. Inspected list of job scheduler administrators and traced to the organization charts for reasonableness.	No exceptions noted
3.	Production incidents, problems, and errors are monitored for status by Data Control personnel on a daily basis. Timely follow-up is performed on unresolved issues.	Inquired of the Billing Services Support Manager regarding job scheduling. Inspected email communication regarding resolution for a sample of job schedule deviations, noting that follow-up is performed timely.	No exceptions noted

Figure 11 – Storage Media & Backup			
Control Objective – Provided by Mid America Computer Corporation			
Controls provide reasonable assurance that production data is backed up on a periodic basis and tested for recoverability.			
Provided by Mid America Computer Corporation		***Provided by FORVIS***	
Control Activity		***Testing Procedures***	***Test Results***
1.	Backups for the Windows servers are performed on a weekly basis.	Inquired of the Technology Services Manager regarding weekly server backups. Inspected backup schedules, noting weekly backups are in place. Inspected backup logs for a sample of weeks. Inspected a list of individuals who have the ability to change backup schedules, noting access is restricted.	No exceptions noted
2.	Weekly backup jobs are monitored to determine if any issues identified are tracked and resolved.	Inquired of the Technology Services Manager regarding weekly backups. Inspected resolution for a sample of failed backups. Inspected alert notification configurations for failed backups.	Nonoperating activities: the circumstances that warrant the operation of this control activity did not occur during the period covered by the report, and therefore, no testing was performed.
3.	Restoration tests of backup data are performed at least annually as part of Disaster Recovery procedures.	Inquired of the Technology Services Manager regarding restoration tests. Inspected the 2022 annual restoration test procedures and results. Inspected a screenshot of evidence that the disaster recovery procedures occurred.	No exceptions noted

Figure 12 – Environmental Controls			
Control Objective – Provided by Mid America Computer Corporation			
Controls provide reasonable assurance that physical access to computer network equipment and storage media is restricted to authorized personnel and stored in a secure and environmentally controlled facility.			
Provided by Mid America Computer Corporation		***Provided by FORVIS***	
Control Activity		***Testing Procedures***	***Test Results***
1.	Access to the computer room is limited by a key card access system at the entrance. Access is limited to personnel with appropriate card access clearance.	Inquired of the Director of Billing Services regarding individuals with access to the computer room, noting individuals are appropriate. Inspected a list of individuals with access to the computer room and traced to the organization chart for reasonableness, noting access is restricted to individuals with a key card.	No exceptions noted
2.	Director of Billing Services must approve access to the computer room.	Inquired of the Director of Billing Services regarding access to the computer room. Inspected evidence of approval for a sample of computer room badges issued during the period.	No exceptions noted
3.	Physical access to the data center is removed for terminated users.	Inquired of the Director of Billing Services regarding access to the data center. Inspected the computer room access expiration date for a sample of terminated employees, noting that physical access was removed.	No exceptions noted
4.	The computer room is environmentally controlled by the use of redundant air conditioners, fire suppression equipment, uninterruptible power supply (UPS), and diesel generator.	Inquired of the Director of Billing Services regarding computer room environmental controls. Inspected the maintenance reports noting that redundant air conditioners, fire suppression, UPS, and generators are in place. Observed the computer room, noting the appropriate environmental controls are in place.	No exceptions noted

Section IV
Additional Information Provided by Mid America Computer Corporation

Additional Information Provided by Mid America Computer Corporation

Business Interruption Plan

MACC has developed and implemented a Business Interruption Plan (BIP). The management team at MACC strongly believes that contingency planning is not a luxury, but an essential element for protecting the safety of all employees and providing uninterrupted quality service to customers. The BIP outlines the procedures that must take place to sustain critical business processes in the interim following a business interruption and during the recovery process to restore to normal business operations. The plan includes the Technology Services recovery priorities and focuses on business processes, communications recovery, alternate work sites, and data application requirements. The MACC Management Team is committed to updating the plan quarterly and testing the plan annually. All appropriate changes will be made in accordance with the plan maintenance procedures.

IBM/Kyndryl Business Continuity and Resiliency Service (BCRS) has been contracted to provide emergency recovery facilities in the event of catastrophic site or facility failures. The contract lists information for computer equipment and communication and equipment restoration procedures. A hot/cold site contract is in place for emergency recovery of computer operations with IBM/Kyndryl BCRS. This contract provides recovery services to MACC within a reasonable period of time after a disaster has been declared.

MACC's 2022 Disaster Recovery (DR) test was performed at the IBM/Kyndryl Business Continuity and Resiliency Service (BCRS) facility in Boulder, Colorado. The test period was scheduled from May 9 at 9:00 a.m. through May 12 at 9:00 a.m. MACC successfully restored the production environment consisting of network infrastructure, FTP/SFTP servers, Production servers, SQL database servers, IIS web server, Exchange email server, Domain Controller servers, as well as the MSaaS environment consisting of Domain Controllers, ADC/NetScaler servers, Storefront servers, Delivery Console servers, File server, License server, SQL Servers, and Hosting server.

MACC was able to achieve a successful DR test within the Recovery Time Objective (RTO). MACC simulated customer interface to the restored SFTP server and the transmission of customer files. Both toll and bill cuts were accomplished using multiple companies' data. All production processes to create new End-User files, reports, and PDF bills were tested on the restored systems.

CABS tests were successful using multiple companies' data. In addition, the MSaaS environment was also tested successfully.

All restores and testing were performed through remote connectivity from Blair, Nebraska.

Information Security

Mid America Computer Corporation (MACC) recognizes the value and importance of our customers' information, and is committed to providing adequate protection of this information while it is within our custody and care. We have designed and implemented procedures to help ensure appropriate steps are taken to protect both MACC and our customer's information.

MACC's Information Security program provides centralized responsibilities for the design, coordination, and implementation of information security practices, measures, and controls. Continuing reviews and improvements help ensure the program addresses ever-changing risks, technologies, business requirements, and legal and regulatory requirements, as well as reflects MACC's ongoing commitment to protecting our customer's valuable information.

Some of the key operational components include the following:

Information Protection

Responsibility for information protection lies with three key functions within MACC that work together to define and implement procedures to ensure MACC is collecting, creating, maintaining, and deleting data and information in accordance with applicable laws, regulations, and internal policies. These three areas are Physical Security, Information Security, and Data Privacy. The security program is supported by the technical expertise of MACC's Technology Services team, who work closely with all departments to implement policies as procedures. MACC also engages third-party expertise to help ensure we maintain a current view of worldwide security issues and leading industry practices.

Ongoing Assessments

Several types of assessments are conducted:

- Quarterly vulnerability assessments are conducted by an independent third party to identify any weaknesses or exposure in the corporate network infrastructure.
- An annual SOC 1 Type 2 assessment is conducted to help ensure appropriate controls have been implemented and are operating effectively for processing user entities' transactions.
- Annual external and internal penetration tests are conducted by an independent third party, which provides an in-depth technical evaluation of MACC's cybersecurity posture.
- Annual Disaster Recovery tests are performed at an off-site location to validate MACC's ability to restore operations and meet Recovery Time Objectives (RTO).

Weaknesses identified during these assessments, or those identified via alternate methods, are analyzed and assessed by the appropriate team.

Technical Safeguards

Technical safeguards are in place to help ensure dependable and secure day-to-day operations of information processing technologies.

- Firewalls are in place at all egress points to the external network. Firewalls are configured as default-deny and ports are enabled only as approved business needs require.
- A tiered security architecture is in place, making use of DMZ and internal secure network zones.
- MACC has implemented multifactor authentication (MFA) to enhance security. Administrators utilize MFA when performing administrative functions on the network. Employee VPN connections also require a second form of authentication before being allowed to connect to the network.
- MACC utilizes a secure remote access solution for connecting to customer systems. This solution requires all users to authenticate using MFA before being granted access.
- Anti-virus software is implemented on all gateways, servers, and workstations, and is configured to automatically update on a regular basis. Threat Prevention information is managed centrally and cannot be disabled by end users.

- MACC has implemented the Security Information & Event Management (SIEM) solution. SIEM provides vulnerability assessment, intrusion detection, behavioral monitoring, and log management. The solution is continuously monitored by a third-party Security Operations Center (SOC). Security issues are documented and escalated to MACC within the contracted response time.
- MACC has implemented an encrypted email message solution which allows for sending secure email to our customers and third-party vendors.
- For most desktop systems, content management is in place for web traffic using a web filter that restricts access to nonbusiness related websites.
- All laptops have hard drive encryption protection.

Incident Response Plan

An Incident Response Plan (IRP) exists for MACC and requires that incidents are recognized, acted upon, escalated, and resolved in a consistent, timely, repeatable, and reliable manner. The IRP is a confidential document due to the nature of its content, and therefore is not shared outside of MACC. The IRP provides instructions for handling the events and incidents. Specific roles for personnel and associated responsibilities are defined. The IRP is reviewed annually.

The IRP includes the process of customer notification that may be required if an incident results in unauthorized exposure of, or access to, data. A customer will be notified of a breach if their information is directly involved in the breach.

Employee Education

MACC ensures that employees undergo education to maintain safe practices on the MACC network. This education includes the following:

- Reviewing and acknowledging MACC's cybersecurity policies.
- Completing annual cybersecurity training courses.
- MACC's Cyber Security team performs regular phishing tests.
- Employees receive weekly micro training.
- MACC's Cyber Security team sends out educational emails highlighting various topics.