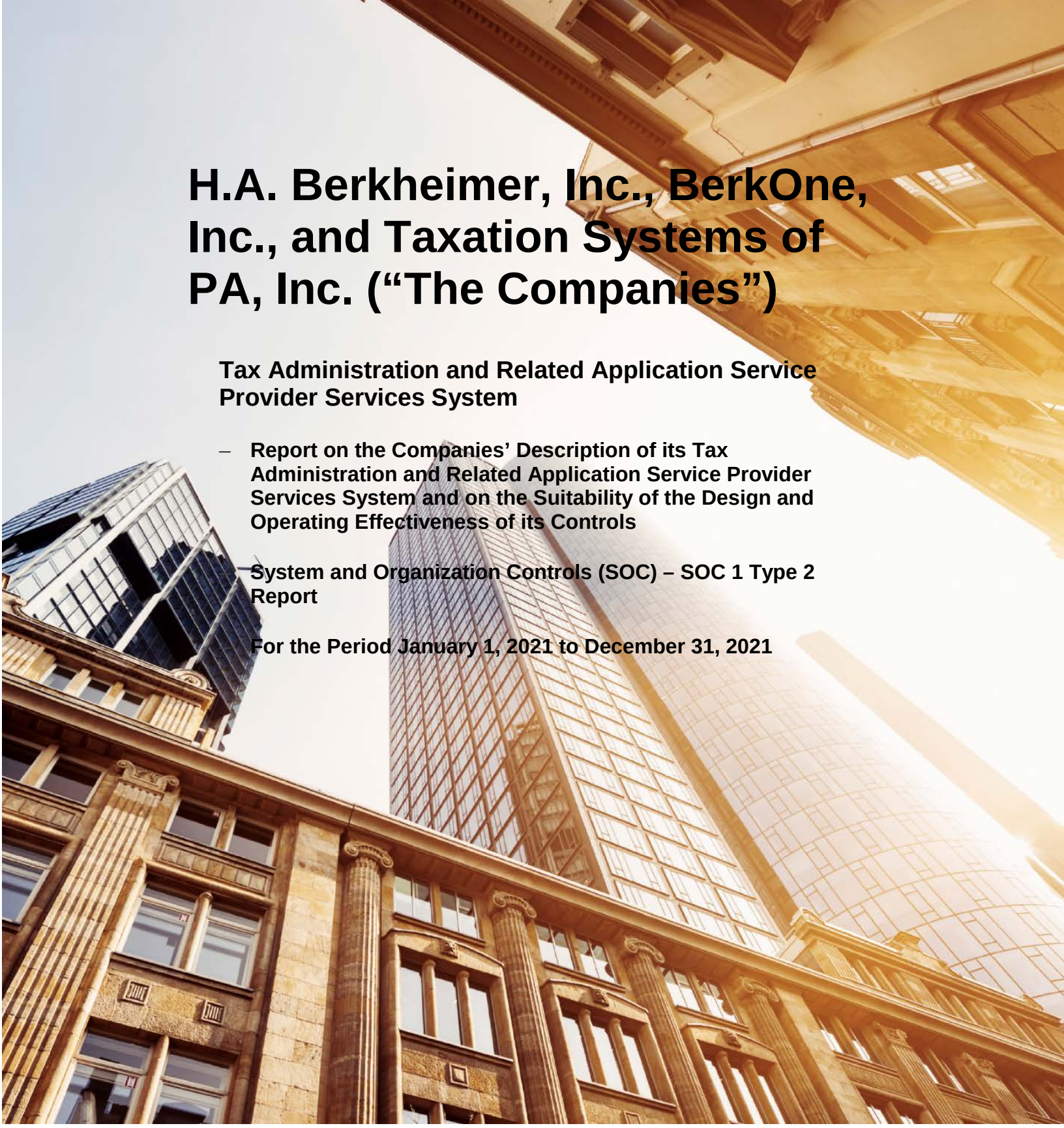

H.A. Berkheimer, Inc., BerkOne, Inc., and Taxation Systems of PA, Inc. (“The Companies”)

Tax Administration and Related Application Service Provider Services System

– **Report on the Companies’ Description of its Tax Administration and Related Application Service Provider Services System and on the Suitability of the Design and Operating Effectiveness of its Controls**

System and Organization Controls (SOC) – SOC 1 Type 2 Report

For the Period January 1, 2021 to December 31, 2021

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations ™

bakertilly

Contents

1. Independent Service Auditor's Report

To the Board of Directors of The Companies:

Scope

We have examined H.A. Berkheimer, Inc., BerkOne, Inc., and Taxation Systems of PA, Inc.'s (“The Companies”) description of its tax administration and related application service provider services system, entitled "Description of The Companies’ Tax Administration and Related Application Service Provider Services System" for processing user entities’ transactions throughout the period of January 1, 2021, to December 31, 2021 (description), and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "The Companies’ Assertion" (assertion). The controls and control objectives included in the description are those that management of The Companies believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the tax administration and related application service provider services system that are not likely to be relevant to user entities' internal control over financial reporting.

The information in Section 5, "Other Information Provided by The Companies", is presented by management of The Companies to provide additional information and is not a part of The Companies’ description of its tax administration and related application service provider services system made available to user entities during the period of January 1, 2021, to December 31, 2021. Information about The Companies business continuity and disaster recovery program has not been subjected to procedures applied in the examination of the description of the tax administration and related application service provider services 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 tax administration and related application service provider services system and, accordingly, we express no opinion on it.

The Companies use various subservice organizations to provide credit card processing, penetration testing, vulnerability scanning and security advisory services. The description includes only the control objectives and related controls of The Companies and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by The Companies can be achieved only if complementary subservice organization controls assumed in the design of The Companies’ controls are suitably designed and operating effectively, along with the related controls at The Companies. Our examination did not extend to controls of the subservice organizations and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of The Companies’ controls are suitably designed and operating effectively, along with related controls at the service organizations. 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 2, The Companies has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. The Companies is responsible for preparing the description and its assertion, including the completeness, accuracy, and method of presentation of the description and the 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 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 our examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period of January 1, 2021, to December 31, 2021. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

Inherent Limitations

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

Description of Tests of Controls

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

Opinion

In our opinion, in all material respects, based on the criteria described in The Companies' assertion,

- The description fairly presents the tax administration and related application service provider services system that was designed and implemented throughout the period of January 1, 2021, to December 31, 2021.

- 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 of January 1, 2021, to December 31, 2021, and the subservice organizations and user entities applied the complementary controls assumed in the design of The Companies' controls throughout the period of January 1, 2021, to December 31, 2021.

- The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period of January 1, 2021, to December 31, 2021, if complementary subservice organization and user entity controls assumed in the design of The Companies' controls operated effectively throughout the period of January 1, 2021, to December 31, 2021.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of The Companies, user entities of The Companies' tax administration and related application service provider services system during some or all of the period of January 1, 2021, to December 31, 2021, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Baker Tilly US, LLP

Philadelphia, Pennsylvania
March 24, 2022

2. The Companies' Assertion

We have prepared the description of H.A. Berkheimer, Inc., BerkOne, Inc., and Taxation Systems of PA, Inc.'s ("The Companies") tax administration and related application service provider services system entitled "Description of The Companies' Tax Administration and Related Application Service Provider Services System," for processing user entities' transactions throughout the period of January 1, 2021, to December 31, 2021 (description) for user entities of the system during some or all of the period January 1, 2021, to December 31, 2021, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by the subservice organizations and user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

The Companies use various subservice organizations to provide credit card processing, penetration testing, vulnerability scanning and security advisory services. The description includes only the control objectives and related controls of The Companies and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by The Companies can be achieved only if complementary subservice controls assumed in the design of The Companies' controls are suitably designed and operating effectively, along with the related controls at The Companies. The description does not extend to controls of the subservice organizations.

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 Companies' controls are suitably designed and operating effectively, along with related controls at The Companies. The description does not extend to controls of the user entities.

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

a. The description fairly presents the tax administration and related application service provider services system made available to user entities of the system during some or all of the period January 1, 2021, to December 31, 2021, for processing user entities' transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting.

   The criteria we used in making this assertion were that the description:

   i. Presents how the tax administration and related application service provider services system made available to user entities of the system was designed and implemented to process relevant transactions, including, if applicable,

      (1) The types of services provided, including, as appropriate, the classes of transactions processed.

      (2) The procedures, within both automated and manual systems, by which services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.

      (3) The information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

      (4) How the system captures and addresses significant events and conditions, other than transactions.

      (5) The process used to prepare reports or other information provided to user entities.

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

(7) The specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls contemplated in the design of the service organization's controls.

(8) Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

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

iii. 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 tax administration and related application service provider services system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period January 1, 2021, to December 31, 2021, to achieve those control objectives if the subservice organizations and user entities applied the complementary controls assumed in the design of The Companies' controls throughout the period January 1, 2021, to December 31, 2021. The criteria we used in making this assertion were that:

i. The risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization.

ii. The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

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

Patricia McNamara

Patricia A McNamara, President
H.A. Berkheimer, Inc.

John A. Bojko

John A. Bojko, President
BerkOne, Inc.

John E. DeRemer III

John E. DeRemer III, President
Taxation Systems of PA, Inc.

3. Description of The Companies' Tax Administration and Related Application Service Provider Services System

Overview of The Companies

The Companies provide various tax administration services for over 1,500 municipalities and school districts throughout Pennsylvania. The Companies have decades of tax administration experience and were first to administer the Earned Income Tax in 1965. With a specialization in ACT 32 and ACT 50 tax administration, it enables the Companies to provide services for 32 Tax Collection Districts to help individuals, employers, tax preparers, and governments with their tax needs. The Companies' management focuses on continuously refining their systems and services to fit the needs of their diverse clients while maintaining their quality and control standards.

The Companies major administration and processing centers are located in Bangor and Bethlehem, Pennsylvania. The Bangor office encompasses 20,000 square feet of operating space for administration, operations, customer service, agency accounting, and houses a secure computer operations area. The Bethlehem office encompasses 46,000 square feet of operating space for the key components of remittance processing, digital scanning, document generation, and houses a secure computer operations area. In addition, 20 statewide offices are maintained for localized taxpayer and client services.

The Companies maintain a paperless processing system to provide the highest level of service to clients statewide. The Companies have approximately 449 professional staff members and offers continuous training in customer service and tax law changes.

Scope of the Description

This description addresses only The Companies' tax administration and related application service provider services system provided to user entities and excludes other services provided by The Companies. The description is intended to provide information for user entities of the tax administration and related application service provider services system and their independent auditors who audit and report on such user entities' financial statements or internal control over financial reporting, to be used in obtaining an understanding of the tax administration and related application service provider services system and the controls over that system that are likely to be relevant to user entities' internal control over financial reporting. The description of the system includes certain business process controls and IT general controls that support the delivery of the tax administration and related application service provider services system.

The Companies use various subservice organizations, ACI Payments, Inc. and Netizen, to provide credit card processing, penetration testing, vulnerability scanning and security advisory services. The description includes only the control objectives and related controls of The Companies and excludes the control objectives and related controls of the subservice organizations.

Internal Control Framework

This section provides information about the five interrelated components of control at The Companies, including

- control environment,
- risk assessment,
- monitoring activities,
- information and communications, and
- control activities.

Control Environment

Organization and Administration

The control environment sets the tone of an organization, influencing the control awareness of the organization and is embodied by the organization's awareness of the need for controls. Emphasis is given to the appropriate controls through management's actions supported by its policies, procedures, and organizational structure.

The following are the primary elements of The Companies' control environment:

- **Agency Accounting**: Responsible for recording, verifying, and reconciling all funds and transactions processed by the operating areas. Distributes collected funds to clients.
- **Application Service Group**: Performs regular maintenance programming and programming for user-requested enhancements.
- **Client Services**: Responsible for product support and for responding to client inquiries including research and resolution of identified problems.
- **Collections**: Identifies and applies collection efforts on delinquent taxpayer accounts.
- **Human Resources**: Administers and monitors personnel policies.
- **Internal Audit**: Reports directly to the Board of Directors. Responsible for the audits of the Companies including independent monitoring of compliance with policies, procedures, and laws.
- **IT Management**: Responsible for providing day-to-day computer operations, monitoring hardware service, maintaining and monitoring network communications and security administration, and developing/designing client forms.
- **Legal**: Legal Department in-house attorney provides guidance and oversight of all aspects of Act 32 collection administration for compliance with Act 32 and other local and state tax laws and regulations.
- **Marketing**: Provides analysis for new business prospects and new product planning.
- **Operations**: Serves as centralized support for earned income tax, remittance processing, imaging, and mail processing including Berk-e online filing and payments systems operation.
- **Risk Management and Compliance**: Identifies areas requiring controls and implements these controls. Performs systems planning, development, and implementation.
- **Training**: Responsible for the coordination of training and development needs of new staff, provides continuous training for current staff, and maintains and creates procedures for current and new processes or tax law changes.

Periodic management meetings are held to discuss special processing requests, operational performance, and the development and maintenance of projects in process.

Every position has a written job description that identifies responsibilities and is used as a basis for the required access for each position. The Companies will verify references for each applicant and conduct a criminal background check for all potential candidates. Other pre-screening checks may include consumer credit, motor vehicle records, educational accreditation, and others as required for the position. The confidentiality of user entity information is of high importance to the Companies. All employees are required to sign a confidentiality agreement upon being hired. The orientation program includes the acknowledgment of the Employee Handbook, the Information Security Policies, and the completion of the security awareness training, and is required to be reviewed when changes occur or annually thereafter. Supervised on-the-job training and formal in-house training classes are available to employees as required for each position.

The Companies' policy requires that all employees receive an annual performance evaluation and salary review. These reviews are based on employee-stated goals and objectives that are prepared and reviewed with the employee's supervisor. Completed appraisals become a permanent part of the employee's personnel file.

The Internal Audit group is responsible for performing a program of financial, operational, security and compliance audits based on an established risk model. Internal Audit evaluates the soundness, adequacy, and application of internal controls and determines the extent of compliance with established policies, procedures, and laws. Formal reports of audit findings are provided to management after each audit, and findings are summarized and reported to the Board of Directors.

The Companies engage in an annual earned income tax audit performed by an independent accounting firm.

The Companies maintain insurance coverage against major risks. Coverage is maintained at levels that The Companies consider reasonable given the size and scope of the operations and is provided by insurance companies that The Companies believe are financially sound.

Risk Assessment

Ultimate responsibility for determining acceptable levels of risk and managing those risks rests with the Board of Directors. The Board of Directors have delegated authority to senior management for the development of appropriate risk management policies and procedures.

The Board of Directors periodically meet with management to discuss goals, risks, and objectives. Management updates processes, procedures, and controls to address the identified risks.

The Companies' management meets periodically with the user entities and assesses the risks associated with transaction processing performed for user entities, including the risks that threaten the achievement of the control objectives included in this report.

The Companies' management recognizes that the risk assessment process is a critical component of its operations that helps The Companies identify, analyze, and manage risk relevant to its operations. The Companies have incorporated risk assessments throughout its processes. Management is responsible for implementing procedures to identify risk inherent in operations and for implementing procedures to monitor and mitigate the risks. The foundation of this process is management's knowledge of its operations, its close working relationship with its customers and vendors, and its understanding of the industry in which The Companies operates. Managers discuss and resolve issues as they arise within their areas and monitor and adjust the control processes for which they are responsible on an as-needed basis.

Monitoring Activities

Senior management and supervisory personnel monitor performance, quality, and internal controls as a normal part of their activities. With The Companies' various tracking and processing systems, a series of "key indicator" management reports that measure the results of various processes involved in processing transactions for user entities are used to monitor operations. Key indicator reports include reports of actual transaction processing volumes compared with anticipated volumes, actual processing times compared with scheduled times, and actual system availability and response times compared with established service level goals and standards. All exceptions to normal or scheduled processing related to hardware, software, or procedural problems are logged, reported, and resolved.

<u>Monitoring of the Subservice Organizations</u>

The Companies use subservice organizations to provide credit card processing and vulnerability scanning. The Companies review the SOC 1® type 2 report and PCI Certification for ACI Payments, Inc. and the ISO Certification 27001 for Netizen in addition to requiring a vendor assessment be completed. Through its daily operational activities, management of The Companies monitors services performed by the subservice providers to help determine that operations and controls expected to be implemented at the subservice organizations are functioning effectively.

Information and Communication

To help align The Companies' business strategies and goals with operating performance, management is committed to maintaining effective communication with all personnel. Information comes from both inside and outside the organization and is used to guide The Companies' strategic and tactical decision-making and to measure performance. The Companies' management has focused on establishing multiple formats and channels of internal and external communications to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner.

Information Systems

As with all information contained in this report, the following information is considered sensitive and should be kept confidential.

Networks are isolated within data centers using logical segmentation and virtual local area networks (VLAN). Access to the wide area network (WAN) is via the internet utilizing virtual private networking ("VPN") and firewall security. The rules of exchange are set respectively allowing what ports, protocols and servers are accessible. There are redundant firewalls at each data center that utilize failover as a backup system.

In addition to the firewall technology described above, an intrusion detection system (IDS) provides a sophisticated real-time detection mechanism, accomplished by monitoring all network inbound traffic to the processing center. This complements existing security countermeasures by offering dynamic network intrusion detection that transparently examines network access. It identifies and logs unauthorized use, misuse, and abuse of computer systems. When suspicious "signatures" are recognized, the event is logged. The Companies utilize a log monitoring tool to allow for real-time alerts and dashboards for monitoring various events.

Vulnerability scanning is conducted internally and externally on a regular schedule. Additionally, penetration testing is conducted that includes five components: External Penetration, Internal Penetration, Physical Security, Social Engineering, and Wireless Network Penetration.

Real-time virus detection on all production servers provides protection against viruses. Virus protection has also been deployed to all workstations, providing for central virus reporting, automatic software updates, and remote management. Virus definitions are updated daily to provide protection from new viruses.

A secure server and encrypted connection secure all communications to the E-File System, which allows employers and individuals to file payroll and tax returns online. The web site has a digital certificate, which verifies The Companies' identity on the internet. Logical access controls have been implemented.

There are some servers that are located in a DMZ or otherwise public network zone. In this location resides the Web server, e-mail server, and a server that provides public information to specific clients. All mail is scrubbed for any viruses prior to entering the e-mail server.

The Internal Document Tracking ("IDT") System is used to log all incoming returns and track all phases of processing from start to finish. Before routing incoming returns to the various processing units, the mail processing area uses the IDT System's barcode track technology to capture the date received, generate total tray count, and assign batch numbers for the various types of work to be processed.

The Job Tracking System, an automated job scheduler, is used to capture and monitor the work orders for batch printing of reports, forms, and negotiable instruments. Extract files from the internal system are used to enter record counts and, if applicable, dollar aggregates into the Job Tracking System. All jobs processed in the computer operations and mail processing areas are reconciled to the record counts and, if applicable, to dollar aggregates in the Job Tracking System.

Ticketing systems, “Track-It” and “ConnectWise”, are utilized to document and track all Help Desk requests for assistance, technical problems, applicable technical maintenance, and project tracking.

A turnkey core application system is utilized for collecting and monitoring delinquent tax payment history.

Optical character recognition (“OCR”) for Forms, which is a base level capture product supported by a third-party provider, is used as the front-end scanning and image conversion software.

Communication

The Companies implemented various methods of communication so that all employees understand their individual roles and responsibilities over transaction processing and associated controls, and so that significant events are communicated in a timely manner. These methods include orientation and training programs for newly hired employees and periodic staff meetings. Every employee has a written job description that includes the responsibility to communicate significant issues and exceptions to an appropriate higher level of authority in a timely manner.

The Companies also implemented various methods of communication to user entities, so they understand the roles and responsibilities of The Companies in processing their transactions, and so significant events are communicated to users in a timely manner. Users are also encouraged to communicate questions and problems to the management at The Companies, and such matters are tracked until resolved, with the resolution also reported to the user entity.

Events affecting user entities are reported to Client Services personnel so that they may facilitate proactive communication with the user entities. The client services area also communicates information regarding changes in processing schedules, system enhancements, and other information to user entities. A Change Advisory Board has been established to review changes affecting the production environment on a weekly basis.

Control Activities

The Companies have developed a variety of policies and procedures including related control activities to help ensure The Companies’ objectives are carried out and risks are mitigated. These control activities help ensure that processing services are administered in accordance with The Companies’ policies and procedures.

Control activities are performed at a variety of levels throughout the organization and at various stages during the relevant business process. Controls may be preventive or detective in nature and may encompass a range of manual and automated controls, including authorizations, reconciliation, and IT controls. Duties and responsibilities — such as duties related to the processing and recording of transactions and control monitoring — are allocated among personnel where applicable, to ensure that a proper segregation of duties is maintained.

A formal program is in place to review and update The Companies’ policies and procedures on a periodic basis. Any changes to the policies and procedures are reviewed and approved by management and communicated to employees.

Tax Administration and Related Application Service Provider Services System

Overview of Services Provided

The Companies provide various tax administration services of all local tax types to clients through proprietary collection systems. These systems are developed, maintained, and enhanced by a complete full-time programmer/analysts/development staff. The systems allow for sending appropriate customized forms and making available electronic filing options for individuals and employers on behalf of the client for the taxpayer to remit accordingly, processing payments to the bank electronically and posting transactions to the systems in real time by utilizing OCR, distributing identified collections electronically to clients and non-clients, and enabling detailed reporting for all tax types that can include Earned Income Tax (EIT), Local Services Tax (LST), Per Capita Tax, Business Privilege Tax, Mercantile Tax, Mechanical Devices Tax, Amusement Tax, and Real Estate Tax.

The following tax services are also provided:

- **BerkApp:** Mobile app that provides taxpayers a safe and secure method for filing returns, making payments, and sending correspondence.
- **Budgeting Assistance**: Client Services staff can provide budgetary consulting through the utilization of the Companies' tax administration accounting system.
- **Claims Processing***:* To ensure timely exchange of money between collectors, the Companies have full responsibility of claiming money due from other tax collectors and have the ability for instant reciprocation to other collectors on a monthly basis.
- **Commercial Census:** A complete survey of all areas of business and industries can be provided to clients by the Companies' representatives.
- **Delinquent Taxpayer reporting**: The delinquent collection system identifies, pursues and reports activities of delinquent accounts for as many years as the law allows.
- **Document Imaging**: Images of all tax-related documents are captured and stored in a secure environment.
- **E-file***:* berk-e is the Companies' suite of industry leading electronic tax filing, payment, and management services. It provides the taxpayer with a safe and secure method of electronically filing tax returns and allows payments on the Companies' secure website.
- **EFT/EDI**: Tax revenues may be electronically transferred to the accounts authorized by the client.
- **Financial Reconciliation:** Each month, clients receive detailed reports reconciling all disbursements for the month. The financial system provides agency accounting staff information to constantly monitor collections.
- **Legal Representation/Attorney:** In-house legal representation in all matters pertaining to tax collection administration is available.
- **Remittance Processing**: The remittance processing system has the ability to process checks, post payments, transfer funds, and provide digital images of all payment information via the Internet. The utilization of high-speed equipment enables automated encoding and endorsement of checks. An in-house programming staff seamlessly integrates data with the financial system.
- **Taxpayer Audits**: An audit staff is trained to audit returns to check that taxes are properly reported and remitted.
- **Taxpayer Services**: Representatives are trained to provide taxpayers with prompt service. Each representative has access to the Companies' imaging system, providing on-line taxpayer information as they respond to taxpayers' telephone inquiries.
- **Up-to-date Tax Rolls**: A comprehensive system of tax roll analysis. Tax rolls are updated daily by taxpayer questionnaires and external census tools that provide up to date information.

Processing of Transactions:

- All incoming documents are sorted and batched to allow operations to track incoming tax returns throughout all stages of processing. This is done through the barcode system, Internal Document Tracking System (IDT). The IDT system reconciles the number of trays received to the number of trays that were logged into the IDT System by mail processing. It also integrates with in-house applications to monitor and report each phase of the process in real time. All exceptions and discrepancies are timely researched and resolved.
- The imaging system captures an image of each tax return and extracts the data from the return into a preprogrammed template. Once verified the data is uploaded to the Earned Income Tax system. The system generates a daily report that summarizes the number of imaged returns (E-1's) uploaded to the system queue for review/maintenance by EIT personnel. All imaged tax returns are made available in the system to each processor allowing the processor to locate and view complete image enabled taxpayer data at each workstation.
- The use of high-speed laser printing technology allows the Companies to design tax forms to include remittance stubs with an OCR scan line.
- All print/mail projects are accounted for in the Job Tracking System. Personnel enter record counts onto the Job Tracking System, which automatically reconciles record counts for the completed phase of processing to the control totals. If there are differences, the Job Tracking System generates a Discrepancy Report. If print/mail projects are not completed by the due date, exception reports are also generated. The forms coordination area investigates all record count differences and past due projects.
- Managers inspect and approve printed documents within the Job Tracking System before being mailed. If completed jobs are not properly approved, the system generates an exception report.
- If employees experience technical problems, they must call the Help Desk to report the incident.

The tax application software and technology environment are also offered to clients that want to maintain their own in-house staff to process and collect taxes. The TaxSys product line includes the software to support the following taxes: EIT, Per Capita, Real Estate, LST, Business Privilege/Mercantile, Mechanical Devices, and Amusement.

The following tax administration and related application service provider services are included in the scope of this report:

- Earned Income Tax ("EIT")
- Per Capita Tax
- Local Services Tax ("LST")
- Business Privilege Tax/Mercantile Tax/Mechanical Devices Tax/Amusement Tax
- Real Estate Tax

COVID-19 Response

Impacts due to COVID-19 has been minimal, as the Companies' have the technologies and work arrangements in place to meet processing needs. In the unlikely event mail delivery should cease for any amount of time, this mailing delay would have a direct impact on any items sent or received via USPS. A large part of the Companies' Earned Income Tax collections from employers is provided electronically. See table below for information regarding impact of COVID-19 to controls at the Companies'.

Description of Control	Related Control Objective (CO)	Impact and Response
10.3 - A delinquency file containing delinquent taxpayer information is created via the Commonwealth of Pennsylvania's ("Commonwealth") income tax filings and automatically interfaced into the EIT system via computer operators.	CO10	Due to COVID-19, the Commonwealth of Pennsylvania ("Commonwealth") was unable to provide a file to The Company timely. On a weekly basis, an error report identifying delinquent taxpayer differences between the EIT system and the CUBS system was generated and reviewed by Berkheimer. This review was not impacted by the inability of the Commonwealth of Pennsylvania to provide the delinquency file to Berkheimer.
11.1 - State return information is requested annually from the Commonwealth. The Commonwealth prepares an electronic file that is loaded to The Companies' local tax return system and compared to the local tax records to determine if local tax should have been filed for previous years.	CO11	Due to COVID-19, the Commonwealth of Pennsylvania ("Commonwealth") was unable to provide a file to The Company timely.

Key Reports Provided to User Entities

The Companies provides a variety of reports to user entities related to the user entities' internal controls over financial reporting. These key reports include:

- ACH Confirmation Report
- ACT 32 Annual Report
- ACT 32 Report
- Monthly Distribution Report
- Delinquent Tax Statement
- Invoice Report

Control Objectives and Related Controls

The Companies has specified the control objectives and identified the controls that are designed to achieve the related control objectives. The specified control objectives, related controls, and complementary user entity controls are presented in Section 4, and are an integral component of The Companies' description of its tax administration and related application service provider services system.

Complementary Subservice Organization Controls

The Companies' controls related to the tax administration and related application service provider services system cover only a portion of overall internal control for each user entity of The Companies. It is not feasible for the control objectives related to The Companies' tax administration and related application service provider services system to be achieved solely by The Companies. Therefore, each user entity's internal control over financial reporting must be evaluated in conjunction with The Companies' controls and the related tests and results described in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below.

Complementary Subservice Organization Controls	Related Control Objective (CO)
ACI Payments, Inc. is responsible for securely and timely processing of credit card transactions.	CO2, CO3, and CO7
Netizen is responsible for penetrating testing on an annual basis and vulnerability scanning on a monthly basis and for providing security advisory services to the Companies.	CO3

Complementary User Entity Controls

The Companies' controls related to the tax administration and related application service provider services system cover only a portion of internal control for each user entity of The Companies. It is not feasible for the control objectives related to tax administration and related application service provider services system to be achieved solely by The Companies. Therefore, each user entity's internal control over financial reporting should be evaluated in conjunction with The Companies' controls and the related tests and results described in Section 4 of this report, taking into account the related complementary user entity controls identified under each control objective, where applicable. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control to determine whether the identified complementary user entity controls have been implemented and are operating effectively.

4. Description of The Companies' Control Objectives and Related Controls, and Baker Tilly's Description of Tests of Controls and Results

Information Provided by Baker Tilly

This report, when combined with an understanding of the controls at user entities, is intended to assist auditors in planning the audit of user entities' financial statements or user entities' internal control over financial reporting and in assessing control risk for assertions in user entities' financial statements that may be affected by controls at The Companies.

Our examination was limited to the control objectives and related controls specified by The Companies in Sections 3 and 4 of the report, and did not extend to controls in effect at user entities or subservice providers.

It is the responsibility of each user entity and its independent auditor to evaluate the information in conjunction with the evaluation of internal control over financial reporting at the user entity in order to assess total internal control. If internal control is not effective at user entities, The Companies' controls may not compensate for such weaknesses.

The Companies' internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by The Companies. In planning the nature, timing, and extent of our testing of the controls to achieve the control objectives specified by The Companies, we considered aspects of The Companies' control environment, risk assessment process, monitoring activities, and information and communications.

The following table clarifies certain terms used in this section to describe the nature of the tests performed:

Type of Test	Description
Inquiry	Inquiry of appropriate personnel and corroboration with management
Observation	Observation of the application, performance, or existence of the control
Inspection	Inspection of documents and reports indicating performance of the control
Re-performance	Reperformance of the control

In addition, as required by paragraph .35 of AT-C section 205, Examination Engagements (AICPA, Professional Standards), and paragraph .30 of AT-C section 320, when using information produced (or provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Control Objective 1: (Physical Security) – Controls provide reasonable assurance that physical access to computer equipment, storage media and program documentation is restricted to properly authorized individuals.		
Description of Controls	**Tests Performed by Baker Tilly**	**Results of Tests**
Bethlehem Facility		
1.1 - The building is equipped with the following security and environmental technologies: motion detection system, fire protection system, emergency lighting, and a security access card system. The system is monitored twenty-four hours a day, seven days a week.	Observed the facility to determine that the following security and environmental technologies were in place: motion detection system, fire protection system, emergency lighting, and a security access card system.	No exceptions noted.
	Inspected monitoring contracts to determine that the system was being monitored twenty-four hours a day, seven days a week.	No exceptions noted.
1.2 - Employees are issued a security access card to gain access into the Bethlehem processing center. The profiles of terminated employees are purged from the system in a timely manner.	Observed the physical access restriction procedures for unused access cards to determine that unused cards were safeguarded.	No exceptions noted.
	Selected a sample of personnel with security access cards to the Bethlehem facility and inspected the related access authorization forms to determine that management authorized the personnel access.	No exceptions noted.
	Selected a sample of terminated employees and inspected EAL system access rights and the active card listing to determine that their profiles had been removed from the card access system.	No exceptions noted.
1.3 - Vendors and other persons not having a security access card are required to sign a visitor's log in the main reception area. Logged information includes the visitor's name, destination, time in, and time out. Visitors are required to wear a visitor badge while in the building.	Inspected the visitor's log for the Bethlehem location to determine that the visitor's log was maintained and logged information including the visitor's name, company, destination, time in, and time out.	No exceptions noted.
	Observed the use of required visitor badges while onsite.	No exceptions noted.
1.4 - Access to the data center is secured by a card access system. Vendors and other persons not having a security access card are required to sign a visitor's log maintained within the data center.	Observed the physical access restrictions to the data center to determine that access was restricted using a security access card system.	No exceptions noted.

Control Objective 1: (Physical Security) – Controls provide reasonable assurance that physical access to computer equipment, storage media and program documentation is restricted to properly authorized individuals.		
Description of Controls	**Tests Performed by Baker Tilly**	**Results of Tests**
	Selected a sample of special access employees and inspected the employee authorization forms to determine that only authorized users were permitted into the data center.	No exceptions noted.
	Inspected the Policy for Server Room Access to determine that various security-related controls such as physical access to the server room, visitor procedures, and access card usage were addressed.	No exceptions noted.
	Inspected the server room visitor log to determine that an access log was maintained for individuals without security access to the server room and the information logged included date, responsible employee, purpose of task, time in, and time out.	No exceptions noted.
1.5 - A Building Security Policy, which outlines various security-related controls, has been developed.	Inspected the Building Security Policy to determine that various security-related controls such as physical access to the facility, visitor procedures, and access card usage were addressed.	No exceptions noted.
Bangor Facility		
1.6 - A Building Security Policy, which outlines various security-related controls, has been developed.	Inspected the Building Security Policy to determine that various security-related controls such as physical access to the facility, visitor procedures, and access card usage were addressed.	No exceptions noted.
1.7 - Employees are issued a security access card to gain access into the Bangor processing center. The profiles of terminated employees are purged from the system in a timely manner.	Selected a sample of personnel with security access cards to the Bangor facility and inspected their related access authorization forms to determine that management authorized their access.	No exceptions noted.
	Selected a sample of terminated employees and inspected EAL system access rights and the active access card listing to determine that their profiles had been removed from the card access system in a timely manner.	No exceptions noted.

Control Objective 1: (Physical Security) – Controls provide reasonable assurance that physical access to computer equipment, storage media and program documentation is restricted to properly authorized individuals.		
Description of Controls	**Tests Performed by Baker Tilly**	**Results of Tests**
1.8 - The facility is equipped with a motion detection system that is monitored twenty-four hours a day, seven days a week.	Observed the facility to determine that perimeter controls were implemented including motion detection, intruder alarm, security access card system, and video surveillance monitoring devices.	No exceptions noted.
	Inspected monitoring contracts to determine that the system was being monitored twenty-four hours a day, seven days a week.	No exceptions noted.
1.9 - Surveillance cameras are used at the processing center to monitor the facility perimeters, entrances, restricted interior locations, and selected common interior areas. Cameras are reviewed on a weekly basis.	Selected a sample of weeks and inspected security camera reviews to determine that on a weekly basis security cameras were reviewed.	No exceptions noted.
1.10 - Vendors and other persons not having a security access card are required to sign a visitor's log in the main reception area. Logged information includes the visitor's name, company, destination, time in, and time out.	Inspected the visitor's log for the Bangor location to determine that the visitor's log was maintained.	No exceptions noted.
1.11 - All major computing equipment and the wiring closets are physically secured within the computing area. Access to the data center is controlled by a card access system and access is based on an employee's job requirements. Access to the data center is secured by a card access system. Vendors and other persons not having a security access card are required to sign a visitor's log maintained within the data center.	Selected a sample of computing area access cards and inquired of management to determine that access to the computing area was restricted to authorized individuals and necessary based upon job responsibilities.	No exceptions noted.
	Inspected the Policy for Server Room Access to determine that various security-related controls such as physical access to the server room, visitor procedures, and access card usage were addressed.	No exceptions noted.
	Inspected the server room visitor log to determine that an access log was maintained for individuals without security access to the server room and the information logged included date, responsible employee, purpose of task, time in, and time out.	No exceptions noted.

Control Objective 1: (Physical Security) – Controls provide reasonable assurance that physical access to computer equipment, storage media and program documentation is restricted to properly authorized individuals.		
Description of Controls	**Tests Performed by Baker Tilly**	**Results of Tests**
Complementary User Entity Controls		
1. User entities with remote access to The Companies' internal networks are responsible for establishing physical and logical access controls over terminals and procedures manuals.		

Control Objective 2: (Logical Security) – Controls provide reasonable assurance that logical access to programs and data is restricted to authorized users.		
Description of Controls	**Tests Performed by Baker Tilly**	**Results of Tests**
2.1 - An appropriate level of management must approve all users before access to information systems is permitted. The Employee Access Level (EAL) system is used to capture and approve the required levels of access. EAL reconciliations are performed by internal audit personnel and reported to management on a monthly basis.	Selected a sample of new employees and inspected EAL approvals to determine that new user access was approved.	No exceptions noted.
	Selected a sample of months and inspected the monthly EAL reconciliations to determine that internal audit personnel had reviewed employee access levels and reconciliations were reported to management.	No exceptions noted.
2.2 - Notice of employee terminations are communicated using the EAL system to the appropriate level of management so that system access can be timely revoked.	Selected a sample of terminated employees and inspected their EAL system access rights to determine that access was revoked in a timely manner.	No exceptions noted.
2.3 - Access to network accounts with special administrative privileges is restricted to a limited number of authorized individuals who have responsibility for performing network administration functions. Password settings are enforced for all accounts accessing the network.	Selected a sample of individuals who had been assigned administrator rights on the network and inspected job descriptions to determine that administrative rights were appropriate based on the job descriptions.	No exceptions noted.
	Inspected password configurations to determine that the following network security settings were activated: minimum password length, complexity, periodic password expiration, and automatic lockout after a prescribed number of unsuccessful logon attempts.	No exceptions noted.
2.4 - Access to the operating system is controlled through identification and authentication of users via a secure password and separation of application and system users into different access paths.	Inspected the operating system authentication configurations to determine that users were authenticated through network credentials via a secure password.	No exceptions noted.
2.5 - Password and user identification codes are required to access software applications and are configured to expire periodically.	Inspected the operating system, Earned Income Tax System (EIT), Financial System (FIN), and Integrated Billing System (IBS) configurations to determine that the following application software security configuration and settings were activated: • Use of passwords; • user identification codes; and, • password expiration frequency.	No exceptions noted.

Control Objective 2: (Logical Security) – Controls provide reasonable assurance that logical access to programs and data is restricted to authorized users.		
Description of Controls	**Tests Performed by Baker Tilly**	**Results of Tests**
2.6 - Administrator level access to the Roundtable Total Software Management System is restricted to the programming manager and supervisor and a separate computer is dedicated to program development.	Inspected the listing of the Roundtable Administrators and inquired of management and inspected job roles to determine that access was restricted to authorized individuals and commensurate with job responsibilities.	No exceptions noted.
	Selected a sample of system changes and inspected change records to determine that separate systems were used to segregate the development and production environments for each change.	No exceptions noted.
2.7 - Only supervisory personnel have the ability to assign access rights on the imaging system.	Inspected the listing of users with the ability to assign access rights on the imaging system and inquired of management to determine that access was restricted to authorized supervisory personnel.	No exceptions noted.

Complementary User Entity Controls

1. User entities with remote access to The Companies' internal networks are responsible for establishing physical and logical access controls over terminals and procedures.
2. The security administrators at user entities with remote access to The Companies' internal networks are responsible for determining the appropriate level of application access for each employee and for promoting segregation of duties when assigning access levels.
3. The security administrators at user entities are responsible for ongoing maintenance and monitoring of their users' access assignments.

Control Objective 3: (Network Security) – Controls provide reasonable assurance that data transmissions between users with remote terminal access and The Companies are from authorized users.		
Description of Controls	**Tests Performed by Baker Tilly**	**Results of Tests**
3.1 - Communication to the private network by remote users is secured using Virtual Private Network (VPN) software with encryption, Virtual Desktop Interface (VDI), and Remote Desktop Services. An appropriate level of management approval is required before remote access is granted. Multi-factor authentication (MFA) is required for access to VDI and Remote Desktop Services.	Inspected the VPN encryption protocol to determine that communication to the private network via remote users was secured.	No exceptions noted.
	Inspected the VDI configurations to determine that communication to the private network via remote users was secured.	No exceptions noted.
	Inspected the Remote Desktop Services configurations to determine that communication to the private network via remote users was secured.	No exceptions noted.
	Inspected MFA configurations to determine that MFA was required for access to VDI and Remote Desktop Services.	No exceptions noted.
	Selected a sample of new users that were setup for remote access and inspected their EAL authorization to determine that remote access was approved and documented.	No exceptions noted.
3.2 - Firewalls and routers are used to prevent unauthorized traffic to the private network from outside connections.	Observed the existence of the Cisco firewall appliance in the computer operations area.	No exceptions noted.
	Inspected the network topology diagram and firewall rulesets to determine that the network was configured to prevent unauthorized traffic from entering the private network.	No exceptions noted.
3.3 - Network Address Translation (NAT) is used to protect employees' private addresses when they are in public networks.	Inspected firewall NAT rules to determine that NAT was in use to protect employees' private addresses in public networks.	No exceptions noted.
3.4 - Access control list violations are logged and monitored using an automated Intrusion Detection System (IDS).	Inspected the network diagram and system configurations to determine that an IDS tool was in place.	No exceptions noted.

Control Objective 3: (Network Security) – Controls provide reasonable assurance that data transmissions between users with remote terminal access and The Companies are from authorized users.		
Description of Controls	**Tests Performed by Baker Tilly**	**Results of Tests**
	Selected a sample of access control list violations and inspected alert tickets to determine that access control list violations were logged and monitored.	No exceptions noted.
3.5 - Anti-virus software is used to protect the network servers and workstations against viruses.	Inspected the anti-virus definitions, distribution settings and update schedule to determine that anti-virus was used to protect the network servers and workstations and that updated definitions were deployed on a daily basis.	No exceptions noted.
3.6 - An independent vendor is engaged to perform a daily external vulnerability scan of systems connecting to outside networks and a weekly internal scan. An email report is provided to management for review, tracking, and monitoring of identified vulnerabilities.	Inspected the vendor contract, scan email report, and vulnerability issues log to determine that external vulnerability scans were performed daily and internal vulnerability scans were performed weekly by an independent vendor and scan results were provided to management for review, tracking, and monitoring of identified vulnerabilities.	No exceptions noted.
3.7 - An independent vendor is engaged to perform an annual penetration test of systems connecting to outside networks.	Inspected the annual external penetration test results to determine that a penetration test was performed annually on systems connecting to outside networks.	No exceptions noted.

Complementary User Entity Controls

1. User entities with remote access to The Companies' internal networks are responsible for establishing physical and logical access controls over terminals and procedures manuals.
2. User entities should properly protect their in-house network infrastructure with anti-virus software that is updated frequently.
3. User entities should report any actual or suspected security breaches.

Control Objective 4: (Program Development and Maintenance) – Controls provide reasonable assurance that new applications being developed and modifications to existing systems and programs are authorized, tested, properly implemented, and documented.		
Description of Controls	**Tests Performed by Baker Tilly**	**Results of Tests**
4.1 - A programming projects database is used to track and monitor each programmer's progress in completing assigned projects.	Observed that a programming projects database was used to track and monitor each programmer's progress in completing assigned projects.	No exceptions noted.
4.2 - Application software development and maintenance standards are documented in The Companies' Application Programming Guides and Standards Manual. The programmer, user/requestor, and programming manager must approve all program changes/new programs on the Companies' SharePoint.	Inspected the Application Programming Guide and Standards Manual to determine that development and maintenance standards were documented.	No exceptions noted.
	Selected a sample of programming projects and inspected the SharePoint process flows to determine that program changes were approved before they were migrated to production.	No exceptions noted.
4.3 - Roundtable is used to provide version control for application changes, program inventory, and configuration/release management controls for the following tax program applications: per capita tax, real estate, local services tax, business privilege tax, mercantile tax, mechanical devices tax, amusement tax, and real estate tax.	Observed the Roundtable system to determine that a version control system was in place for application changes.	No exceptions noted.
	Inspected the list of users with administrative access to Roundtable and inspected job roles to determine that access was restricted to authorized individuals and commensurate with job roles.	No exceptions noted.
4.4 - All changes must be tested prior to implementing in the production environment.	Selected a sample of changes and inspected the change records to determine that the changes were tested prior to implementing in the production environment.	No exceptions noted.
4.5 - The Change Advisory Board meets at least monthly to review changes affecting the production environment.	Selected a sample of weeks and inspected weekly meeting minutes to determine that the Change Advisory Board met on a weekly basis to assess changes affecting the production environment.	No exceptions noted.
Complementary User Entity Controls		
None.		

Control Objective 5: (Computer Operations) – Controls provide reasonable assurance that facilities that process and maintain information, equipment, storage media, servers and program documentation are protected against environmental hazards.		
Description of Controls	**Tests Performed by Baker Tilly**	**Results of Tests**
5.1 - Critical computing resources have technical support and preventative maintenance agreements with the vendors.	Inspected technical support and preventative maintenance agreements with vendors to determine that the agreements were current.	No exceptions noted.
5.2 - The data center has an environmental control system that maintains temperature and humidity levels.	Observed the data center to determine that it included an environmental control system, fire extinguishers, fire detectors, emergency lighting, and that there was no evidence of eating, drinking, or smoking.	No exceptions noted.
5.3 - Eating, smoking and drinking are prohibited inside the data center.		
5.4 - The building is equipped with fire detectors in the ceiling, which receive periodic maintenance. Hand-held fire extinguishers are located throughout the building.		
5.5 - Emergency lights are placed in strategic locations to assist in the evacuation of personnel should power be interrupted.		
5.6 - Insurance coverage includes facilities, computer equipment, business recovery, media recovery, cyber, and extra expense.	Inspected insurance policies to determine that coverage for facilities, computer equipment, business recovery, media recovery, cyber, and extra expense was included.	No exceptions noted.
5.7 - An Uninterruptible Power Supply (UPS) provides sufficient time to allow an orderly system shutdown in the event of a power failure**.**	Observed that critical servers were supported by a UPS device.	No exceptions noted.
5.8 - Critical information is backed up daily, weekly, and monthly. Encrypted backups are performed on a device-to-device basis and replicated daily to an offsite data domain environment.	Inspected backup procedures for the operating systems and network operation systems to determine that EIT and production information were required to be backed up daily.	No exceptions noted.
	Inspected the backup schedules to determine that information on the mainframe was scheduled to be backed up daily.	No exceptions noted.
	Inspected daily backup logs to determine that critical information was backed up on a daily, weekly, and monthly basis.	No exceptions noted

Control Objective 5: (Computer Operations) – Controls provide reasonable assurance that facilities that process and maintain information, equipment, storage media, servers and program documentation are protected against environmental hazards.		
Description of Controls	**Tests Performed by Baker Tilly**	**Results of Tests**
	Inspected backup configurations to determine that data was configured to be encrypted during the daily replication process.	No exceptions noted.

Complementary User Entity Controls
None.

Control Objective 6: (Document Production / Batch Scheduling) – Controls provide reasonable assurance that job processing, including batch printing, is scheduled and deviations from scheduled processing are identified and resolved.		
Description of Controls	**Tests Performed by Baker Tilly**	**Results of Tests**
6.1 - All print/mail projects are accounted for in the Job Tracking System. Personnel enter record counts into the Job Tracking System, which automatically reconciles record counts for the completed phase of processing to the control totals. If there are differences, the Job Tracking System generates a Discrepancy Report. If print/mail projects are not completed by the due date, exception reports are also generated. The forms coordination team investigates all record count differences and past due projects.	Selected a sample of print/mail projects and reconciled the control totals for record counts derived after the printing and mailing phases to determine that discrepancies were identified by the Job Tracking System. For any discrepancies identified, reconciled the projects to the Discrepancy Report and inquired with the forms coordination team to determine that the record count differences were investigated.	No exceptions noted.
	Inspected the Incomplete Jobs Report and Scheduled Print Jobs Not Printed Report to determine that past due or incomplete jobs generated exception reports.	No exceptions noted.
6.2 - Authorized personnel inspect and approve printed documents within the Job Tracking System before being mailed. If completed jobs are not properly approved, the system generates an exception report.	Selected a sample of print/mail projects and inspected manager approvals to determine that managers approved the documents before they were mailed.	No exceptions noted.
	Inspected the Jobs Without Required Approvals Report from the Job Tracking System to determine that job processing, including batch printing, was scheduled and deviations from scheduled processing were identified and resolved.	No exceptions noted.
6.3 - If employees experience technical problems, they are required to report technical problems to the Help Desk. Help Desk incidents are tracked in the ticketing system for resolution.	Inspected the Help Desk Procedures document to determine that procedures existed requiring employees to report technical problems to the Help Desk.	No exceptions noted.
	Selected a sample of Help Desk incidents reported and inspected the Help Desk tickets to determine that technical problems were reported by employees for resolution.	No exceptions noted.

Complementary User Entity Controls

1. User entities should review provided reports timely (paper and electronic).
2. User entities should balance and reconcile all provided reports on a timely basis.
3. User entities should report to The Companies any actual or suspected tax processing issues of which they are aware.

Control Objective 7: (Tax Returns and Taxpayer Remittances) – Controls provide reasonable assurance that income tax returns and taxpayer remittances are input and processed accurately, completely, and timely and taxpayers are notified if errors are identified.		
Description of Controls	**Tests Performed by Baker Tilly**	**Results of Tests**
EIT		
7.1 - An Internal Document Tracking System (IDT) is used to log and track incoming tax return documentation from the incoming mail through the completion of imaging. A barcode system is used to transfer documents for further processing, via a courier service. A courier Discrepancy Report is generated when there are discrepancies between the number of trays sent and received. An automated e-mail notification is sent to the business manager for courier items not received within 24 hours. Discrepancies are timely researched and resolved via a Warehouse Help Desk ticket.	Inspected the IDT configuration settings to determine that the system was configured to send an automated e-mail notification for courier items not received within 24 hours.	No exceptions noted.
	Selected a sample of days and inspected the daily Discrepancy Reports to determine that e-mail notifications were generated and received by the business.	No exceptions noted.
7.2 - The system generates a daily report that summarizes the number of imaged returns (E-1's) uploaded to the system queue for review/maintenance by the EIT personnel each business day.	Selected a sample of business days and inspected the daily aging report to determine that the system summarized the number of imaged returns (E-1's) uploaded to the system queue for review/maintenance by the EIT area.	No exceptions noted.
7.3 - To monitor that the correct amounts were encoded on tax payment checks, check tallies are reconciled to the batch totals from the encoding machine in remittance processing. The accounting area reconciles tax payment postings from the system to the amounts deposited in the bank.	Selected a sample of days and reconciled the amounts on batch report totals from the encoding machine summary to the encoding machine detail via the Remittance Processing System (RPS) to determine that amounts were processed accurately and completely.	No exceptions noted.
	Selected a sample of days and reconciled the daily amounts per the cash receipts journal to deposits on bank statements to determine that daily cash received was deposited accurately and completely.	No exceptions noted.
7.4 - The imaging system captures address information from tax returns and automatically assigns the funds to the related jurisdiction. The taxpayer identification number is automatically captured and uploaded to the EIT system.	Selected a sample of tax returns and compared the information on the tax return (in the imaging system) to the information in the EIT system to determine that both the correct jurisdiction and taxpayer identification number were captured and uploaded to the EIT system.	No exceptions noted.

Control Objective 7: (Tax Returns and Taxpayer Remittances) – Controls provide reasonable assurance that income tax returns and taxpayer remittances are input and processed accurately, completely, and timely and taxpayers are notified if errors are identified.		
Description of Controls	**Tests Performed by Baker Tilly**	**Results of Tests**
7.5 - Triannually, EIT supervisors perform quality control reviews of completed tax return desk audits and verify that the number of errors found are within the Companies' established tolerance rate.	Selected a sample of triannual periods and inspected EIT desk audit quality control reviews to determine that reviews were performed to identify that the number of errors found were within the Companies' established tolerance rate.	No exceptions noted.
7.6 - Taxpayers are notified when errors are identified. A log is maintained of all taxpayer correspondence.	Inspected the taxpayer correspondence log to determine that the notifying of taxpayers when errors were identified was completed on a timely basis.	No exceptions noted.
Business Privilege, Mercantile, Mechanical Devices, Amusement Taxes		
7.7 - To monitor that the correct amounts were encoded on tax payment checks, check tallies are reconciled to the batch totals from the encoding machine in remittance processing. The accounting area reconciles tax payment postings from the system to the amounts deposited in the bank.	See tests of operating effectiveness performed at control 7.3.	No exceptions noted.
7.8 - For business privilege and mercantile tax, personnel inspect each tax return to verify its completeness and to determine that there is proper supporting documentation for gross revenues.	Selected a sample of business privilege and mercantile tax return batches and inspected the tax return documentation to determine that tax returns were completed and support existed for gross revenues.	No exceptions noted.
7.9 - To avoid backlogs, outstanding batches that are pending review are monitored monthly using reports from remittance processing.	Selected a sample of months and inspected the Unposted Payment Reports to determine that supervisory personnel monitored tax return processing for backlogs on a monthly basis.	No exceptions noted.
Per Capita and Real Estate Taxes		
7.10 - To monitor the correct amounts were encoded on tax payment checks, check tallies are reconciled to the batch totals from the encoding machine in remittance processing. The accounting area reconciles tax payment postings from the system to the amounts deposited in the bank.	See tests of operating effectiveness performed at control 7.3.	No exceptions noted.

Control Objective 7: (Tax Returns and Taxpayer Remittances) – Controls provide reasonable assurance that income tax returns and taxpayer remittances are input and processed accurately, completely, and timely and taxpayers are notified if errors are identified.		
Description of Controls	**Tests Performed by Baker Tilly**	**Results of Tests**
7.11 - Bills that are rejected from the system are manually researched and re-posted for the correct amounts.	Selected a sample of days and rejected bills and inspected the batch detail to determine that rejected bills were manually researched and reposted for the correct amounts.	No exceptions noted.

Complementary User Entity Controls

1. User entities should report to The Companies any actual or suspected tax processing issues of which they are aware.
2. Instructions and information provided to The Companies from user entities should be in accordance with provisions in the servicing agreement between The Companies and the user entities.
3. User entities should request taxpayer rosters and perform inspections to monitor that the listings are current, complete, and accurate.
4. User entities should report to The Companies any actual or suspected inaccuracies in the tax records or tax information of which they are aware.

Control Objective 8: (Distributions) – Controls provide reasonable assurance that distributions made to jurisdictions are complete, timely and accurate.		
Description of Controls	**Tests Performed by Baker Tilly**	**Results of Tests**
8.1 - On a daily basis, the system generates an extract file that lists the total distributions that should be made, and the agency accounting area reconciles the total distributions from the extract file to batch totals for checks and ACH transactions processed by the computer operations area.	Selected a sample of days for distributions made via ACH and traced the total dollar amount of the distributions from the system-generated daily extract files to bank statements to determine that processing was accurate and complete.	No exceptions noted.
	Selected a sample of days for distributions made via check and traced the total dollar amount of the distributions from the system-generated daily extract files to the computer area's log of printed checks and check totals to determine that processing was accurate and complete.	No exceptions noted.
	Selected a sample of days for distributions made and inspected the job numbers that were assigned on the Job Tracking System to determine that the number of printed ACH notices and checks reconciled to extract totals and mail processing records to indicate that processing occurred timely.	No exceptions noted.
8.2 - The ACH Operator enters ACH totals in the control log. The ACH Approver then verifies the totals and transmits the totals to the bank.	Selected a sample of days for distributions made and inspected the daily control log to determine that the ACH operator entered daily ACH totals and the ACH approver verified the totals before transmitting to the bank.	No exceptions noted.

Complementary User Entity Controls
1. User entities are responsible for providing The Companies with updates to various taxing ordinances.

Control Objective 9: (Non-Client Distributions) – Controls provide reasonable assurance that transfers to jurisdictions that are serviced by other tax administrators and other tax collectors (“non-clients”) are performed completely, accurately and timely.		
Description of Controls	**Tests Performed by Baker Tilly**	**Results of Tests**
9.1 - Within 30 days after the close of each calendar quarter, the Financial Reporting (“FIN”) and EIT systems are used to update “non-client” balances and generate distribution checks. The totals on the FIN and EIT systems are reconciled and the system is flagged to generate distribution checks. The agency accounting area verifies that the checks printed in computer operations are accurate and reconciles the bank account that is used for “non-client” distributions.	Selected a sample of “non-client” distributions and performed the following to determine that processing was accurate, complete, and timely: • Inspected system records to determine that distribution routines were being executed at least every 30 days; • Reconciled distribution amounts on the FIN and EIT systems; and, • Traced the total distribution amount to the positive pay report.	No exceptions noted.

Complementary User Entity Controls
None.

Control Objective 10: (Delinquent Account Processing) – Controls provide reasonable assurance that attempts are made to identify delinquent accounts for collection activities.		
Description of Controls	**Tests Performed by Baker Tilly**	**Results of Tests**
10.1 - An internally developed program identifies delinquent accounts with missing information and searches the entire tax database to find more complete information on a delinquent taxpayer**.**	Selected a sample of days and inspected the daily related companionation e-mails that listed the number of clients found to determine that the accounts were updated with more complete information.	No exceptions noted.
10.2 - Delinquent notices are flagged in the system and printed by Computer Operations. The note field is a system generated note that is populated into the account when it goes to the print file. Computer Operations sends notices directly to the taxpayers. The CUBS system is programmed to generate past due notices every 45 days after the first notice.	Selected a sample of delinquent accounts and inspected delinquent notices to determine that past due notices were generated by CUBS within 45 days after the first notice.	No exceptions noted.
EIT		
10.3 – A delinquency file containing delinquent taxpayer information is created via the Commonwealth of Pennsylvania's ("Commonwealth") income tax filings and automatically interfaced into the EIT system via computer operators. Management reviews the report annually.	Inspected the State List Summary File to determine that an electronic file was maintained to track the status of taxpayers by jurisdiction for updates and delinquencies and reviewed by management annually. *Note: Due to COVID-19, the Commonwealth of Pennsylvania ("Commonwealth") was unable to provide a file to The Company timely.*	*During the period, due to COVID-19, the Commonwealth of Pennsylvania ("Commonwealth") was unable to provide a file to The Company timely.*
10.4 - On a weekly basis, an error report identifying delinquent taxpayer differences between the EIT system and the CUBS system is generated and transmitted to the Delinquency department for review.	Selected a sample of weeks and inspected the weekly EIT to CUBS error report notification e-mails to determine that differences between the interfacing of delinquent taxpayers from the EIT to CUBS system were identified and reviewed by management for remediation on a weekly basis.	No exceptions noted.
10.5 - Upon identification of delinquent taxpayers in the CUBS system, delinquency letters are printed and sent to taxpayers.	Selected a sample of delinquent taxpayers and inspected the delinquency letter sent from the CUBS system and evidence of mailings to determine that a delinquency letter was printed and sent to the taxpayer.	No exceptions noted.

Control Objective 10: (Delinquent Account Processing) – Controls provide reasonable assurance that attempts are made to identify delinquent accounts for collection activities.		
Description of Controls	**Tests Performed by Baker Tilly**	**Results of Tests**
Per Capita Taxes		
10.6 - The CUBS database of taxpayers who have not paid their per capita tax is kept current through the following processes: (a) annually, a computerized program is used to automatically transfer past due tax records to the CUBS system so that collection efforts can be applied; (b) delinquent per capita tax that is forwarded from tax collectors is manually entered into the CUBS system so that collection efforts can be applied.	Selected a sample of delinquent accounts and traced the accounts to the records in the CUBS system to determine that past due tax records were transferred to the CUBS system from the IBS system.	No exceptions noted.
Business Privilege, Mercantile, Mechanical Devices, Amusement Taxes		
10.7 – Past due tax records are automatically interfaced into the CUBS system so that collection efforts can be applied. On a weekly basis, an error report identifying delinquent taxpayer differences between the Mercantile system and the CUBS system is generated and transmitted to the Delinquency department for review.	Selected a sample of weeks and inspected the weekly BPT FTP Correspondence Counts and Errors report notification emails to determine that differences between the interfacing of delinquent taxpayers from the Mercantile to CUBS system were identified and reviewed by management for remediation on a weekly basis.	No exceptions noted.
Real Estate Taxes		
10.8 - Past due real estate taxes are accumulated and sent to each county's tax claim bureau.	Selected a sample of real estate clients with delinquent taxes and inspected evidence of follow-up to determine that the past due real estate taxes were mailed to the county tax claim bureaus.	No exceptions noted.
Complementary User Entity Controls		
None.		

Control Objective 11: (Taxpayer Records) – Controls provide reasonable assurance that updates received from user entities and other sources are applied to taxpayer records.		
Description of Controls	**Tests Performed by Baker Tilly**	**Results of Tests**
EIT		
11.1 - State return information is requested annually from the Commonwealth. The Commonwealth prepares an electronic file that is loaded to The Companies' local tax return system and compared to the local tax records to determine if local tax should have been filed for previous years.	Inspected the State List Summary File to determine that an electronic file was maintained to track the status of taxpayers by jurisdiction for updates and delinquencies. *Note: Due to COVID-19, the Commonwealth of Pennsylvania ("Commonwealth") was unable to provide a file to The Company timely.*	*During the period, due to COVID-19, the Commonwealth of Pennsylvania ("Commonwealth") was unable to provide a file to The Company timely.*
Business Privilege, Mercantile, Mechanical Devices and Amusement Taxes		
11.2 - Business privilege, mercantile, mechanical devices and amusement taxpayer records are kept current through a process where listings are sent directly from the client with any updates to the accounts.	Selected a sample of taxpayer client updates and inspected the taxpayer records to determine that taxpayer records were kept current.	No exceptions noted.
Per Capita Taxes		
11.3 - Per capita taxpayer records are kept current through an annual process where EIT records of filed individual earned income tax returns are compared to the records of individuals paying the per capita tax.	Inspected the annual comparison file to determine that taxpayer records were kept current through an annual process where EIT records of filed individual earned income tax returns were compared to the records of individuals paying the per capita tax.	No exceptions noted.

Complementary User Entity Controls

1. Instructions and information provided to The Companies from user entities should be in accordance with provisions in the servicing agreement between The Companies and the user entities.
2. User entities should request taxpayer rosters and perform inspections to monitor that the listings are current, complete, and accurate.
3. User entities should report to The Companies any actual or suspected inaccuracies in the tax records or tax information of which they are aware.

5. Other Information Provided by The Companies

This information included in Section 5 is presented by management of The Companies to provide information about The Companies Disaster Recovery Program. Information included within Section 5 has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of the controls to meet the control objectives.

Disaster Recovery Program

In the event of a business disruption, The Companies have established policies, procedures, and responsibilities through a comprehensive Business Continuity/Disaster Recovery Plan ("BCP"). The BCP is an evolving document based on technology, telecommunication, operations, and environmental changes.

The plan assesses the needs and requirements for The Companies to be prepared to respond to an event and efficiently regain operation of the systems that may be inoperable from an event. Vendors of mission critical equipment and services have been taken into consideration in the development of the plan. The Companies weighed the economic and business factors versus the risk potential of an event when determining the level of contingency backup facilities.

The Companies maintain the plan in a ready status at all time. Quarterly Disaster Recovery events are initiated by the technical team to test processing areas. Annually, the overall plan is reviewed and an event is scheduled for testing of the plan. BCP changes as a result of the test and review are approved and distributed. Key contact information is reviewed periodically and distributed as necessary.

The Internal Audit group also reviews the procedures and processes to be followed if a disruption would occur.