Keystone Collections Group

Report on Controls Placed in Operation and Tests of Operating Effectiveness

For the Period
July 1, 2012, to June 30, 2013

McGladrey

I. Independent Service Auditor’s Report

To Management or the Board of Directors of Kratzenberg & Associates, Inc. dba Keystone Collections Group

Scope

We have examined Kratzenberg & Associates, Inc. dba Keystone Collections Group’s description of its tax collection system throughout the period July 1, 2012, through June 30, 2013 and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of Kratzenberg & Associates, Inc. dba Keystone Collections Group’s controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization’s Responsibilities

In Section II of this report, Keystone Collections Group 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. Keystone Collections Group is responsible for preparing the description and for the 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, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Service Auditors’ 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. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period July 1, 2012, through June 30, 2013.

An examination of a description of a service organization’s system and the suitability of the design and operating effectiveness of the service organization’s controls to achieve the related control objectives stated in the description 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 those controls to achieve the related control objectives stated in the description. Our procedures included 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. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in Section III of this report. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions 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 inadequate or fail.

Opinion

In our opinion, in all material respects, based on the criteria described in Keystone Collections Group's assertion in Section II of this report:

a. The description fairly presents the tax collection system that was designed and implemented throughout the period July 1, 2012, through June 30, 2013.

b. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period July 1, 2012, through June 30, 2013, and user entities applied the complementary user entity controls contemplated in the design of Keystone Collections Group's controls throughout the period July 1, 2012, through June 30, 2013.

c. The controls tested, which, together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period July 1, 2012, through June 30, 2013.

Description of Tests of Controls

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

The information in Section V of management's description of the service organization's system, "Other Information Provided by Keystone Collections Group," that describes Keystone Collections Group's business continuity and disaster recovery plans, is presented by the management of Keystone Collections Group to provide additional information and is not part of Keystone Collections Group's description of its tax collection system made available to user entities during the period July 1, 2012, to June 30, 2013. Information about Keystone Collections Group's business continuity and disaster recovery plans has not been subjected to the procedures applied in the examination of the description of the tax collection system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the system and accordingly, we express no opinion on it.

Restricted Use

This report and the description of tests of controls and results thereof in Section IV of this report are intended solely for the information and use of Keystone Collections Group, user entities of Keystone Collections Group's tax collection system during some or all of the period July 1, 2012, through June 30, 2013, and the independent auditors of such user entities, who 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.

McGladrey LLP

October 11, 2013
Schaumburg, Illinois

II. Keystone Collections Group’s Assertion

We have prepared the description of Keystone Collections Group’s tax collection system for processing transactions for user entities of the system during some or all of the period July 1, 2012, through June 30, 2013, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities’ financial statements. We confirm, to the best of our knowledge and belief, that:

- The description fairly presents the tax collection system made available to user entities of the system during some or all of the period July 1, 2012, through June 30, 2013 for processing their transactions. The criteria we used in making this assertion were that the description:

    - Presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including:

        - The classes of transactions processed.

        - The procedures, within both automated and manual systems, by which those transactions are initiated, authorized, recorded, processed, corrected, as necessary, and transferred to the reports presented to user entities of the system.

        - The related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports presented to user entities of the system.

        - How the system captures and addresses significant events and conditions, other than transactions.

        - The process used to prepare reports or other information provided to user entities’ of the system.

        - Specified control objectives and controls designed to achieve those objectives.

        - Other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.

    - Does not omit or distort information relevant to the scope of the tax collection system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the tax collection system that each individual user entity of the system and its auditor may consider important in its own particular environment.

- The description includes relevant details of changes to the service organization’s system during the period covered by the description when the description covers a period of time.

- The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period July 1, 2012, through June 30, 2013 to achieve those control objectives. The criteria we used in making this assertion were that:

- The risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization;

- The controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

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

III. Description of Keystone Collections Group's System

Overview of Operations

Background

Keystone Collections Group (Keystone or the Company) is a tax billing and collection agency serving municipal governments and public school districts throughout Pennsylvania. The Company has grown consistently during each year of its 27-year history. The Company's management has maintained controlled growth during recent periods of business expansion, with its expressed intent of ensuring that the Company sustains its quality standards as it increases its client base and support personnel.

Keystone has 10 offices in Pennsylvania, with its headquarters facility located at 546 Wendel Road in Irwin, Pennsylvania. The headquarters complex houses multiple key components of mailing, printing, payment processing, digital scanning, tax accounting, customer service center, senior legal division, core department supervisors, as well as the firm's executive management. The information technology (IT) center is part of the corporate center.

Approximately, 180 professionals and trained support staff cover multiple disciplines in accounting, law, technology and customer communication. Keystone administers current collection and delinquent recovery in the following taxes and governmental fees: earned income, local services, business privilege and mercantile, occupational, real estate, per-capita and amusement taxes; and water, sewage and refuse collection fees. Keystone's business structure contains separate divisions covering payment processing technologies, legal enforcement and customer service. These various divisions are each designed to integrate with—and support—the other divisions as well as compliment each of their separate component services toward reaching an overall higher level of combined service performance.

Overview of Services Provided

The firm operates with proprietary technology for tax payment processing, automation and accountability. In addition, Keystone operates an online tax filing system on its website at www.keystonecollects.com. Its secure online system for individual taxpayers uses the trade name "e-File." Taxpayers may file as individuals or create a combined return with primary and secondary taxpayer status, adding the necessary supporting document information from W-2 forms and tax schedules. Taxpayers may pay taxes online via electronic check and by credit card. Tax preparers regularly use Keystone's system to file and pay taxes on behalf of their tax clients.

Similarly, businesses may report and pay employee withheld taxes online via Keystone's Web-based eFile Business Portal. This system allows filers the ability to pay online with both ACH credit, ACH debit and credit card options.

KNET is Keystone's integrated office productivity suite developed in a SharePoint model to track the assignment and resolution of Internet and online inquiries from taxpayers, employers, payroll companies, and municipal and school district officials, as well as internal staff inquiries and internally targeted education addressing points of Company interest and operation.

The legal division at Keystone is structured with two objectives: (1) Company compliance under federal, state and local tax laws and regulations, and (2) taxpayer/employer taxation compliance, audit and delinquent recovery enforcement. The firm's legal division attorneys actively pursue delinquent earned income tax (EIT) via auditing, coupled with legal enforcement (court) actions, including civil, bankruptcy, and judgment execution, as well as wage attachment proceedings.

Keystone provides toll-free telephone access to customer service representatives, who are trained and monitored in addressing taxpayer, employer, and municipal and school district officials' inquiries. Oversight of customer service includes real-time monitoring of taxpayer calls in progress, monitoring of telephone call statistics during the business day and recording of specified caller detail information.

Keystone has secured bonding coverage in excess of its statutory and contractual needs from an A.M. Best Company-rated provider (Excellent—A).

Scope of Report

The scope of the report includes certain control objectives related to the tax collections process and the supporting applications, including EIT Manager, which is used for tax return processing, and eFile and the eFile Business Portal, which are interfaces to EIT Manager for taxpayers to submit their returns online and pay taxes owed.

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

Control Environment

Organization

Keystone's Executive Management Team provides the strategic direction for the Company and is responsible for managing areas of operations within the firm. Members of the board of directors are also part of the Executive Management Team, including the president, general counsel and vice president of operations. The Senior Management Team of the Company includes the vice president of client relations, manager of IT infrastructure, community liaison, processing supervisor and associate general counsel. The Senior Management Team handles direct management of daily operations and supervises the employees of the Company.

Individual	Position
Thomas J. Kratzenberg	President
Joseph W. Lazarro	Vice President and General Counsel
David Kratzenberg	Vice President of Operations
Rose Harr	Vice President of Client Relations
Matt Berkebile	Manager, IT Infrastructure
Rob Good	Community Liaison
Lynn Welsh	Processing Supervisor
Jayson Lawson	Associate General Counsel

The Company is separated into the following functional departments for operational purposes:

Processing Department—Mailing systems, payment processing, document scanning/imaging, return verification, form design and banking

Information Technology—Networking, software development, data conversion, communication systems, data security, data backup and Web management

Legal Division—Delinquent collections; EIT Manager System audit; judgment execution; wage attachment; rent attachment; special counsel case coordination; and Act 20 delinquent real estate tax, Act 192 delinquent EIT compliance and Act 32 (current EIT compliance)

Customer Service—Taxpayer phone assistance, call monitoring, call wait-time control, branch office operations, manual data entry, lien filing and credit card payment acceptance

Client Services—Addresses inquiries and requests of political subdivision officials and tax collections committee delegates, including but not limited to, development of special reports and projects

Human Resources

Management makes every effort to hire qualified candidates and has policies and procedures in place to vet employees prior to hiring. Credit and background checks are completed for new employees, and employees are required to sign a nondisclosure and confidentiality agreement. Employees are also required to sign a statement of compliance with the employee handbook, which includes policies concerning Internet and email usage, as well as acceptable uses of the technology systems.

An organizational chart and job descriptions, which describe the job functions and responsibilities for employees, are in place. Job descriptions, which include a position summary and describe major duties and responsibilities, are developed by the department managers and approved by executive management. Employees are cross-trained to ensure sufficient backup personnel are trained in the event of unexpected illness, termination, resignation or promotion at the firm.

Risk Assessment Process

The Executive Management Team meets weekly to discuss risks to the Company. Management identifies and evaluates risks to the business and prioritizes the responses to these risks based on legal, environmental and technology changes. This process is documented in the executive management meeting minutes.

Information and Communication Systems

Earned Income Tax Manager

EIT Manager is the in-house application utilized by Keystone for processing EIT on behalf of municipalities and school districts in the Commonwealth of Pennsylvania. It is designed and compiled in-house by Keystone. The application is written in VB and C#, with Microsoft Visual Studio and Team Foundation Server for the development environment and source repository. The application runs on Microsoft Windows Server 2008 with Microsoft SQL 2008 R2 as the database software. The servers are operated out of the Irwin facility.

eFile

eFile and eFile Business Portal are the respective Web applications that allow taxpayers and businesses in Pennsylvania to report and pay their taxes online. No credit card information is stored by the application. It is designed and compiled in-house by Keystone. The application is written in C# and .NET, with Microsoft Visual Studio and Team Foundation Server for the development environment and source repository. Keystone uses First Data for the credit card processing section of the website. The input of credit card data is passed directly to First Data. Customers can file and pay their taxes using a credit card or an electronic debit from their checking account or mailing a paper check. Keystone has the ability to originate ACH transactions and collect funds from a taxpayer's account if a taxpayer establishes this type of processing within the system.

Monitoring Controls

Management obtains an annual external financial statement audit by an independent certified public accounting firm. Executive management regularly monitors the performance of the Company through weekly executive and staff meetings. Management interacts with user entities on a regular basis and provides regular reporting of system activity to these user entities. Detailed minutes and agendas are maintained for all executive and senior management meetings to document management's decision making process and the monitoring of the Company. Executive management comprises members of the board of directors; therefore, the owners of the Company are directly involved in monitoring and day-to-day operations.

Tax Collection Controls

Keystone's primary business is to collect taxes, process tax returns, pay tax refunds and remit the collected taxes to the municipalities and public school districts that are member tax collection districts (TCD), as well as to nonmember tax collection districts. The tax collections process starts with the input of payments, then proceeds to processing of tax returns, W-2 forms and other information (via mail) or electronically (via eFile) and ends with the distribution of funds and reports to user entities.

Earned Income Tax Return Processing

Individual taxpayers have the ability to choose one of two alternatives for submitting Earned Income Tax Returns to Keystone: electronic filing (e-File) or manually filing a paper return.

The e-File system allows taxpayer to file electronically via the Internet once an account is created and approved on Keystone's website. The eFile system requires a taxpayer to submit the Social Security number and either Tax Identification Number or the prior year's earned income tax liability amount. Once electronic returns are submitted, the e-File software automatically flags returns for manual review, based on refund thresholds and estimated quarterly payment overrides by the taxpayer. Manually prepared and submitted tax returns are scanned through the image scanning system by an operator. Once scanned, two levels of review are performed on the data; the first level of review identifies the form being scanned and the second level of review is performed to ensure that the data on the identified form has been read and scanned correctly by the image scanning system. These reviews are integral to the quality assurance process.

After the data is input and processed through the automated review process for both filing alternatives, the data is transferred to EIT Manager. EIT Manager validates each return input of the scanning system using a proprietary algorithm and verifies that the tax return is calculated correctly. Exceptions identified by the application are manually reviewed.

Additionally, EIT Manager automatically flags and halts processing of duplicate tax returns.

Payment Processing

All payments received via the mail are assigned a unique batch number and control number, stamped with a receipt date and scanned into the remittance processing system (RPS). Written quality control procedures require operators to inspect check images to confirm that the dollar amount of the check agrees to the amount indicated on the payment voucher. Once the batch is manually verified, the RPS process is completed, and funds are sent to the bank for deposit.

A check processing operator converts the previous day's RPS batch to a Check 21 ICL file, which is electronically remitted to the bank. The check processing operator compares the previous day's RPS batch totals to the Check 21 ICL totals to ensure complete and accurate processing. All inbound ACH payments, check payments (ICL files) and cash deposits are reconciled on a daily basis before approval of posting by the banking coordinator.

Online credit card transactions submitted for tax payments are automatically reconciled by the banking coordinator and deposited into the Keystone bank account by a third-party software utility.

Geocoding and Revenue Distribution

Geocoding is a system-generated process that uses a taxpayer's physical address to determine the geographic coordinates (using longitude and latitude). The EIT Manager software has the capability to automatically determine, verify and validate the appropriate political subdivision (PSD) for an individual taxpayer based on the geographic coordinates of their physical address. The Pennsylvania Department of Community & Economic Development (DCED) maintains the geocode location of each PSD on the municipal statistics website. The PSD code is legislatively mandated by Pennsylvania Act 32 of 2008. Taxpayers are encouraged to utilize the municipal statistics website to determine their appropriate PSD codes based upon their physical address.

Once determined, verified and validated, the completion process of the geocode process systematically updates the taxpayer's account in EIT Manager with the appropriate PSD code.

Commissions Earned

Keystone enters into a contract with each of the member TCDs whose Tax Collection Committee (TCC) has selected Keystone as their Act 32 tax officer. During the contractual negotiations, Keystone proposes and negotiates a commission rate with each TCC. The commission rate is earned on resident tax collections within the TCD.

Designated administrators are informed of the applicable commission rates for each TCD from a member of the Executive Management Team. The database administrators maintain restricted access to the commission change module within EIT Manager. Commission rate change logs are monitored by the IT infrastructure manager.

Quarterly Tax Return and Payment Processing

Keystone collects quarterly estimated tax payments from individual taxpayers as well as employer quarterly withholding returns. Individual taxpayers have the ability to choose one of two alternatives for submitting earned income tax data to Keystone: electronic filing (e-File) or manually filing a quarterly estimated tax voucher. Electronic filing requires the taxpayer to submit their Social Security number along with their Tax Identification Number. Individual filers using the eFile system can submit payment utilizing an electronic check or credit card only. Taxpayers mailing paper-based quarterly tax estimates are required to submit an earned income tax estimated voucher along with their tax payment (e.g., check). Keystone scans paper-based individual tax estimates in batches, which are reviewed by manual check processors who verify that data fields are accurately input and processed.

Businesses have the two options available: eFile Business Portal or manually filing paper-based returns. Employers utilizing the e-File Business Portal may submit their data in the following manners:

- Common separated value (CSV) upload
- Pennsylvania standard file format upload (.txt file)
- Manual input of data through an electronic portal

Returns cannot be submitted electronically unless the employer submits the following criteria:

- Employer PSD
- Federal Employer Identification Number (FEIN)
- Employee name

- Employee PSD
- Employee Social Security number
- Employee address

Employers filing through the eFile Business Portal are permitted to submit withholding payments utilizing an electronic check, credit card, voucher and paper check, or ACH credit/debit. Employers manually filing quarterly returns are assigned control numbers that connect the tax payment to the appropriate employer return, as checks and returns are scanned in separately. Once the check has been processed, a processing specialist will input the employee information and withholdings to ensure the tax withholdings are credited to the proper taxpayer accounts. EIT Manager has automated controls to ensure the withholding amounts are properly applied and the applicable PSD code has been used.

Mandatory Reporting in Accordance With Pennsylvania Act 32 of 2008

The DCED mandates the use of required forms (CLGS-32-7 and CLGS-32-7A) for Act 32 tax officers. These reports must be issued to the appropriate TCD members by the 20th day of the subsequent month following the tax collection activity. These reports provide a summary of collection and disbursement activity performed by Keystone on behalf of the TCC and each individual member of the TCC.

Using automated controls in the EIT Manager application, Keystone prepares CLGS-32-7 and CLGS-32-7A reports to be used for reporting to TCDs and the respective members of the TCDs. These reports were vetted and approved by DCED for these reporting purposes.

Taxpayer Reconciliation and Delinquent Taxes

On an annual basis, Keystone reconciles the data in the EIT Manager tax collection system to the Pennsylvania Department of Revenue's (PA DOR's) taxpayer-submitted data. Keystone requests the electronic data from PA DOR, which includes the taxpayer's name, spouse's name, Social Security numbers, state filing status, address and data from Lines 1 and 4 of the PA-40 income tax return form. This information is imported directly into EIT Manager.

Keystone initiates a geocode query on the address received from PA DOR to determine the taxpayer's local tax rate. Using the local tax rate and the income data, Keystone recalculates the taxpayer's earned income tax liability. An automatic process compares discrepancies between the PA DOR calculation and the tax liability originally processed by Keystone. An automated exceptions report is generated for discrepancies.

Keystone's audit and legal department work together to review the discrepancy report and determine further actions to be taken to resolve the delinquent liability. Typically, step one is to send a delinquency notice. If the delinquency is not resolved within a timely manner, a final notice is sent. Legal proceedings incur when the final notice does not produce acceptable resolution of tax liability.

Tax Disbursements to Member and Nonmember Tax Collection Districts

Keystone remits payment to member and nonmember tax collection districts based upon data generated from automated output reports from EIT Manager. Using IT logic and data maintained in EIT Manager, Keystone has constructed an in-house report based on PSD codes. Reports for nonmember tax collecting districts are generated on a monthly basis and uploaded to a secure portal for the nonmember TCD. Keystone generates a paper-based check monthly to the nonmember TCD after the month-end reconciliation process is complete.

Member TCCs receive payment from Keystone on a weekly basis via ACH. Each member of the TCC receives a monthly report depicting the monthly receipts and disbursements activity of the member TCC.

Information Technology General Computer Controls

Computer Operations

System Monitoring

Automated software utilities are in place to monitor the EIT Manager and eFile applications and the underlying network and infrastructure supporting the applications. Monitoring is performed at the network, server and database level for the systems. eFile is monitored from the Internet to verify the Web server is available. IT department personnel monitor the systems using their mobile devices and are notified of processing interruptions after business hours.

Quarterly vulnerability assessments are performed by management who monitor the network and verify that the network is protected from unauthorized access. Scans are performed on the external network and at the application layer for the eFile system. Management performs ad hoc internal scanning to verify that patch management on the internal network is effective.

Backup and Recovery

Keystone has a backup policy in place that identifies the processes and actions required to back up organizational and user entities data. The backup policy is reviewed and approved by executive management on an annual basis. The policy encompasses internal data on the network and the EIT Manager and eFile applications. Incremental (differential) backups are performed on a daily basis to tape and are stored in the secure computer room in the Irwin facility. Full backups are conducted weekly, and tapes are also rotated off-site weekly for storage at a third-party service provider, Iron Mountain. Daily differential backups are performed for EIT Manager and eFile and are retained locally. A tape inventory is maintained showing the location of all tapes on a SharePoint portal. Weekly tapes are rotated back into the cycle after a period of 12 weeks, and month-end backups are retained for a period of at least one year.

The IT department performs quarterly restorations tests to verify the efficacy of backup media and the integrity of data backups. Both file-level and database backups are performed as part of the restoration testing. Restoration testing is performed to a separate location to verify that site-level redundancy is in place.

Environmental controls are in place to protect the computer room at Keystone’s primary processing facility. Critical systems within the facility, including IT infrastructure and key processing work areas have uninterruptible power supply (UPS) systems. The facility is equipped with a natural gas-based generator to power the systems during an extended power loss. The generator is tested on a weekly basis to verify that it is functioning properly. The data center has a raised floor, and temperature sensors to alert management in the event of a malfunction with the cooling systems. Handheld dry chemical fire extinguishers are also in place throughout the computer room.

Data Transmissions and Remote Access

Keystone uses various methods to secure data transmissions with user entities, business partners and taxpayers in the Commonwealth of Pennsylvania. The Data Access Policy specifies that transmission of confidential information must be protected using encryption when transmitted over public networks. Business partners are required to use a secure Web transfer portal, which is protected using Secure Shell (SSH) encryption to transmit records to Keystone. Employees of the Company are able to access the Company’s systems remotely using Citrix ICA sessions. Citrix sessions are protected using 256-bit encryption, and the encryption is required to activate the session. Individual taxpayers must log on to the Secure Sockets Layer- (SSL-) secured website when connecting to the eFile application to pay their taxes. Management has current SSL certificates on file for the public website.

Information Security

Logical Access

User administration policies are documented in the Data Access Policy, which has been reviewed and approved by executive management. Keystone tracks access control requests, including new access requests, access changes and access terminations, via the help desk ticking system. Changes in user access are logged into the help desk system. Human resources submits access requests. Department supervisors determine the level of access required for a new employee, and the request is fulfilled by the IT department. Termination requests are also submitted initially by human resources and fulfilled by the IT department. Termination for personnel in sensitive positions are followed up with a phone call or direct communication with the IT department in order to ensure that the individual's access and physical proximity badge is revoked in a timely manner.

The primary method of access control at Keystone is Microsoft's Active Directory, running on Microsoft Windows Server 2003 and 2008 servers. Database security and access to the EIT Manager application is controlled through Active Directory group memberships, and, overall, it is the primary method of access control for most business applications at the Company. Citrix-based thin clients are used at remote locations to reduce the storage of confidential data at other Keystone locations.

Automated authentication requirements are enforced by group policy for user accounts. Access requires a password with a minimum length of eight characters. Password complexity must be enabled, passwords are set to expire every 45 days and a password history of 24 iterations is retained. Accounts are locked out after 10 invalid access attempts for a period of 60 minutes.

Group policies within Active Directory are also used to enforce other security controls, including a screen saver timeout of 15 minutes, after which a desktop locks and requires a username and password for access. In addition, employees are restricted by group policy from local administrative rights to reduce the risk that malware or unauthorized software can be installed on the local systems.

Access to EIT Manager, the document imaging system and the MS SQL 2008 server database are integrated and controlled by Active Directory network login authentications. A check scanning system is in place, and only authorized users are given access to the application. Privileged access (e.g., payment process, adjustment to accounts in EIT Manager, key configuration table update, etc.) to systems and applications is limited and controlled inside these applications. User and administrative accounts are not shared between users. Keystone uses internal IT resources for maintenance and support of the e-File systems.

Network Security

Management has a detailed network diagram in place that identifies the locations of key servers, firewalls, routers, switches and other network infrastructure. Keystone separates their internal network from the Internet and other untrusted networks, such as vendor networks. High-risk inbound connections from the Internet terminate in the demilitarized zone (DMZ) and are filtered through a Microsoft ISA server. In addition, the firewalls have intrusion prevention system (IPS) features enabled to reduce the risk of attacks from the Internet, and an inline IPS appliance is connected to the firewall. The system has the ability to detect attacks from the network through the application layer of the OSI reference model to reduce the risk of attacks on the eFile system and other Internet-facing resources managed by the Company.

Physical Access

A management-approved physical security policy is in place. Access to the building's front door is monitored by a receptionist, and escorts are provided for visitors within the facility. Access via other doors is controlled by proximity badge readers. Access to the computer room and the check processing area is limited to authorized personnel via key reader badges. Keystone limits access to certain operation areas via a badge access control system. Terminated employees are required to return their magnetic keycard, and the card's access areas are immediately removed. Processing personnel operate around-the-clock shifts, and access to data input and processing areas is restricted via to the processing and IT groups.

Keystone has cameras strategically located throughout the check processing area, data center and entrances and exits to the facility. Cameras are enabled to record each stage of the check processing area. Designated individuals have access to view live and historical video footage.

Change Management

Software Development Life Cycle

The Software Development Policy and Procedures serve as Keystone's Software Development Life Cycle (SDLC). The policy is reviewed and approved by executive management on an annual basis and outlines the process for introducing new software and modifying existing operating software within Keystone's processing environment. The "Agile" or iterative approach to software development is used by Keystone. Projects are implemented and designed on a small scale to ensure that changes can be planned and deployed quickly to respond to different business needs that occur. This methodology provides structured design process for larger changes to applications. Both EIT Manager and eFile fall under the requirements of Keystone Software Development Policy and Procedures.

Management has four different separate database and application environments for the software development process. The development environment is where the initial code is tested and checked in for review. The quality assurance (QA) environment is where code is moved after it is initially reviewed by developers. The user acceptance testing (UAT) environment provides business operations personnel and management with the testing platform. Keystone has supervisors and other personnel involved in operations that will test various components and dependencies of the application to verify that changes do not negatively impact the stability and functionality of the application.

Source Repository

Microsoft Team Foundation Server is used as the source repository. Versions of EIT Manager and eFile are given build labels in the source repository. Software developers do not have access to the production servers for eFile and EIT Manager. Access is controlled using Active Directory group membership. Software developers are not domain administrators and cannot grant themselves access to production. Production support personnel do not write software code or check code into the repository. Access to the production database is also restricted to developers to prevent access to production data and stored procedures. Active Directory is used for database access, and mixed-mode authentication is not enabled at the database level.

Change Control

Change management requests are managed using an online SharePoint portal. A change management tracking system is in place using SharePoint. Management approves the deployment of new software releases. Dedicated environments exist for software development, QA, UAT and production. New builds are tested in QA and UAT prior to their deployment to production. Documentation of QA testing activities is informal; however, management's approval to deploy applications to production is documented in the change control records, and ad hoc details of testing activities may be included in the records.

Changes to network infrastructure, servers and database platforms are tracked using the change controls system, and changes to these platforms are coordinated with customer service and application development personnel, and approved by management prior to their deployment in the production environment.

Complementary User Entity Controls

Keystone's processing of transactions and the controls over the processing were designed with the assumption that certain controls would be placed in operation by user entities. This section describes some of the controls that should be in operation at user entities to complement the controls at Keystone. User auditors should determine whether user entities have established controls to provide reasonable assurance that:

User entities are responsible for notifying Keystone of any changes in employee roles or terminations of employees with logical access to Keystone resources.

Keystone may grant user entities' personnel access to transfer files or perform other actions to facilitate processing of municipal and school district tax collections. User entities must notify Keystone when an employee no longer requires such access or when an employee is terminated and access needs to be revoked.

User entities are responsible for reconciling funds received to reports produced by Keystone.

Keystone provides standard reports to both member and nonmember tax collection districts. User entities must reconcile these reports back to the actual payments received from Keystone to verify that all funds were completely distributed.

User entities must notify Keystone of changes in their tax rate structures and validate that they have been properly implemented by the system.

Keystone's systems have the ability to automatically calculate tax rates, but the rates must be communicated to Keystone by user entities accurately and in a timely manner. Users should review all tax rates that have been entered into the system for accuracy.

IV. Keystone Collections Group's Control Objectives and Related Controls and McGladrey LLP's Tests of Controls and Results of Tests

Keystone control objectives and related controls are an integral part of management's description and are included in this section for presentation purposes. McGladrey LLP included the description of the tests performed to determine whether the controls were operating with sufficient effectiveness to achieve the specified control objectives and the results of tests of controls, as specified below.

Tests of the control environment, risk assessment, information and communication, and monitoring included inquiries of appropriate management, supervisory and staff personnel, observation of Keystone's activities and operations, and inspection of Keystone documents and records. The results of those tests were considered in planning the nature, timing and extent of McGladrey's testing of the controls designed to achieve the control objectives. As inquiries were performed for substantially all of Keystone's controls, the tests were not listed individually for every control in the tables below.

Tax Collection Controls

<u>Control Objective 1:</u> Controls provide reasonable assurance that tax returns and payments are entered, processed and recorded accurately.			
Provided by Keystone Collections Group		***Procedures Performed by McGladrey LLP***	
Control		**Test Performed**	**Test Results**
1.1	Automated input controls are built into the eFile system, which verifies correct character formats for the input fields used. Automated system-level reviews are built into the eFile system, which flags tax returns for manual reviews based upon the system-level criteria.	Inspected the system and verified that input controls were in place for the following criteria: • Social Security number And one of the following: • Tax account ID • Last year's tax liability amount	No exceptions noted.
		Inspected the system output after entering a test transaction and verified that automated system-level reviews are generated based upon system-level criteria (e.g., refund thresholds and estimated quarterly payment overrides by the taxpayer).	No exceptions noted.
1.2	The image-scanning system for paper-based tax returns automatically evaluates that the tax return data agrees to the proper taxpayer account. Missing data or invalid data is manually reviewed by an operator for quality control.	Inspected the automatic evaluation and match process for filed tax return data to the taxpayer account ID in EIT Manager and verified that an automatic check occurred.	No exceptions noted.
		Observed quality control operators as they reviewed scanned images for missing or invalid data prior to submission to EIT Manager.	No exceptions noted.
		Inspected the system output and error screens from the system when invalid data was input to verify that the errors were documented.	No exceptions noted.

Control Objective 1: Controls provide reasonable assurance that tax returns and payments are entered, processed and recorded accurately.

Provided by Keystone Collections Group		***Procedures Performed by McGladrey LLP***	
Control		**Test Performed**	**Test Results**
1.3	Automated edit checks are built into the EIT Manager system, which verifies population of proper data fields; automated exceptions are triggered by criteria established by executive management. EIT Manager validates each return input into the system using a proprietary algorithm, and the system verifies that the tax return is calculated correctly. Exceptions identified by the application are reviewed by tax operators.	Inspected an example final return submitted into EIT Manager that included intentionally generated exceptions to verify EIT Manager-detected sample exceptions, including mismatches in data, invalid data, incorrectly added tax information and other exceptions.	No exceptions noted.

Control Objective 2: Controls provide reasonable assurance that tax payments are entered, processed and recorded timely.

Provided by Keystone Collections Group		***Procedures Performed by McGladrey LLP***	
	Control	**Test Performed**	**Test Results**
2.1	Checks scanned into the remittance processing system are assigned a unique batch number, control number and receipt date, ensuring complete and accurate recording in EIT Manager.	Inspected a sample of scanned batch of checks through the remittance processing system and validated the system-assigned unique batch number, control number and receipt date.	No exceptions noted.
2.2	During the image verification, process operators inspect check images to confirm that the dollar amounts on the check matches the amounts indicated on the payment vouchers.	Observed that the operators verify that the image amounts on the check agree to the amounts on the payment voucher.	No exceptions noted.
		Observed the operators compare the check and the voucher to the data input in the business portal of the eFile system.	No exceptions noted.
2.3	Batch totals from the previous day are reviewed by the check processing operator and automatically converted into a Check 21 ICL file to be remitted to the bank. The check processing manager compares the batch totals to Check 21 ICL totals to ensure complete processing.	Observed the check processing operator convert the remittance batch file to a Check 21 ICL file to be remitted to the bank and compare the batch totals to the Check 21 ICL file and manual deposit totals to verify that the operator reviewed the files for completeness and accuracy.	No exceptions noted.
		Inspected a sample of daily check batch control reports and verified that the totals of the check batches matched the file transmitted to the bank for deposit.	No exceptions noted.
2.4	Inbound ACH payments, check payments and cash deposits are reconciled by the banking coordinator and reviewed by management on a daily basis.	Inspected a sample of daily reconciliations and verified that ACH payments, credit card payments and cash deposits were reconciled by the banking coordinator and reviewed by management on a daily basis.	No exceptions noted.
2.5	Credit card transactions submitted for tax payments are automatically reconciled and deposited by a software utility that utilizes an authorization code and amount on a daily basis. Exceptions are investigated and resolved by management immediately.	Observed a log of credit card transactions as they were input in the software utility and verified that the software automatically reconciled the cash transfer using the authorization code and amount in the Customer Service Portal.	No exceptions noted.
2.6	ACH credit transactions submitted for tax payments are tracked by positive pay and manually reconciled to the online transaction system on a daily basis. Exceptions are investigated and resolved by management immediately.	Observed a log of ACH positive pay transactions sent from the financial institution and verified the reconciliation of cash transfer to the transaction within the Customer Service Portal.	No exceptions noted.

Control Objective 3: Controls provide reasonable assurance that commissions earned for tax collection services rendered are complete and accurate.

Provided by Keystone Collections Group		***Procedures Performed by McGladrey LLP***	
	Control	**Test Performed**	**Test Results**
3.1	Tax commission rates between the TCDs and Keystone are documented in the contract with the TCDs. EIT Manager is configured with the correct commission rates for each TCD.	Inspected the contractual agreements between the tax collector and the selected Tax Collection Committee and verified that an authorized commission rate was documented.	No exceptions noted.
		Inspected the commission rate in EIT Manager and verified that it agrees with the authorized commission rate stated in the contractual agreement with the Tax Collection Committee.	No exceptions noted.
3.2	Automated controls in EIT Manager calculate commissions earned for tax collection services rendered completely and accurately.	Reperformed the commission calculation for each TCD using raw data from the EIT Manager system and verified that it matched the output reports provided to clients.	No exceptions noted.
3.3	Commission rate changes are restricted to authorized personnel.	Inspected the access permissions in EIT Manager and verified that only designated administrators have access to the commission change module.	No exceptions noted.

Control Objective 4: Controls provide reasonable assurance that individual quarterly tax estimates and employer quarterly withholdings are entered, processed and recorded accurately.

Provided by Keystone Collections Group		***Procedures Performed by McGladrey LLP***	
	Control	**Test Performed**	**Test Results**
4.1	Automated input controls in the eFile system prevent the input of incorrectly formatted or invalid information into the system. The system requires that the Social Security number, tax identification number and estimate tax amounts are input in the correct format.	Inspected the system and verified that input controls were in place for the criteria identified to prevent the input of invalid or incorrectly formatted data into the system.	No exceptions noted.
4.2	Automated input controls in the eFile Business Portal system prevent the input of incorrectly formatted or invalid information into the system. The following fields have input controls in place: • Collection area = Keystone Collections Group • Employer PSD • Employer FEIN • Employee PSD • Employee Social Security number • Employee street address (physical address) • Agreement of dollar amounts	Inspected the eFile Business Portal system and verified that input controls were in place for the criteria identified to prevent the input of invalid or incorrectly formatted data into the system.	No exceptions noted.
		Inspected the system and verified that the system-generated output and "failed" validations when invalid data was input into the Business Portal.	No exceptions noted.
4.3	The image scanning system automatically reviews individual quarterly tax estimates and employer quarterly withholdings that are scanned into the system. Operators perform QA reviews of images.	Inspected the report generated by the image scanning system after a return is input into the system and verified that the system could identify errors with the scanned returns.	No exceptions noted.
		Observed operators reviewing images as they were scanned by the system and transferred into EIT Manager for further processing.	No exceptions noted.
4.4	EIT manager automatically validates that individual quarterly tax estimates and employer quarterly withholdings are processed accurately, the payment amount matches the tax return invoice and the amount was credited to the correct taxpayer's account.	Inspected a sample of tax payments and corresponding transactional data and verified the following: • The payment received matched the invoice calculated by EIT Manager. • The payment was credited to the correct taxpayer's account, as indicated on the return.	No exceptions noted.

Control Objective 5: Controls provide reasonable assurance that tax collections and remittances are reported completely and accurately.

Provided by Keystone Collections Group		***Procedures Performed by McGladrey LLP***	
Control		**Test Performed**	**Test Results**
5.1	EIT Manager generates reports of tax activity. The reports are complete and are formatted to meet the PA Department of Community and Economic Development's (DCED's) report standards, CLGS-32-7, CLGS 32-7A, CLGS 32-7B and CLGS 32-7C.	Inspected the reports prepared by EIT Manager distributed to user entities on a monthly basis and verified that they followed the structure identified by CLGS-32-7 and DCED CLGS-32-7A, as established by PA Act 32 of 2008.	No exceptions noted.
5.2	Automated output controls in EIT Manager generate reports for member and nonmember tax collection districts and include the following information: • The type of tax collected and processed, denoted by description and amount • The type of nontax-related receipt collected, earned and processed, denoted by description and amount • The type of tax distribution processed, denoted by description and amount • The type of nontax-related disbursement processed, denoted by description and amount • Cash reconciliation, denoted by description and amount	Inspected an automated report prepared by EIT Manager. Queried the EIT Manager database manually for each of the criteria identified and verified that the data matched the reports produced by EIT Manager.	No exceptions noted.

Control Objective 6: Controls provide reasonable assurance that delinquent taxpayer accounts are identified during the PA Department of Revenue (PA DOR) reconciliation process.

Provided by Keystone Collections Group		***Procedures Performed by McGladrey LLP***	
Control		**Test Performed**	**Test Results**
6.1	Annually, delinquent taxpayer accounts are identified during the PA DOR reconciliation process. PA DOR data is imported into EIT Manager and geocoding automatically determines local tax liability.	Observed the retrieval of archived data files received from the PA DOR used for reconciliation of the PA DOR census information to the EIT Manager system.	No exceptions noted.
		Selected a test taxpayer record and verified that the PA DOR taxpayer information was properly imported into EIT Manager.	No exceptions noted.
		Selected a test taxpayer record and looked up the taxpayer's TCD from the PA DOR website, and compared the result to the EIT Manager system to verify that EIT Manager is properly geocoding the record.	No exceptions noted.
6.2	The EIT Manager system flags delinquent accounts automatically upon completion of the PA DOR reconciliation process.	Inspected the delinquent taxpayer information in EIT Manager and verified that the system identifies delinquent taxpayers automatically upon completion of the PA DOR reconciliation process.	No exceptions noted.
6.3	The audit department reviews system-flagged delinquent accounts and forwards the appropriate information to the legal department, which determines the process for legal filings.	Inspected the EIT Manager Audit Module, which indicates delinquent taxpayer and resolution actions, and verified that the taxpayer was notified of delinquency and pending legal proceedings.	No exceptions noted.

Control Objective 7: Controls provide reasonable assurance that distributions to member and nonmember tax collection districts are processed completely, accurately and timely.

Provided by Keystone Collections Group		***Procedures Performed by McGladrey LLP***	
	Control	**Test Performed**	**Test Results**
7.1	Taxpayer addresses are geocoded using the Geocode software, and the tax revenue collected is routed to the appropriate member and nonmember tax collection districts.	Inspected a sample of taxpayer records from the system and verified that the political subdivision (PSD) code was assigned by EIT Manager.	No exceptions noted.
		Inspected a sample of taxpayer records and compared the results from EIT Manager to the PA DCED's municipal statistics website and verified that EIT Manager accurately assigned PSD codes to taxpayers.	No exceptions noted.
7.2	Nonmember tax collection districts are provided reports (based off of geocoding software) indicating distributions due to them from Keystone.	Inspected a nonmember tax collection district report and compared it to manual queries against the EIT Manager database and verified that the reports accurately reflected the tax revenue collected for the month.	No exceptions noted.
	Checks distributed to nonmember TCDs agree to system-generated distribution reports.	Inspected a nonmember tax collection district report and compared it to manual queries against the EIT Manager database and verified that the tax revenue collected was disbursed to the nonmember tax collection district at the end of the month.	No exceptions noted.
7.3	Member tax collection districts are provided reports (based off of geocoding software) indicating distributions due to them from Keystone. Checks distributed to member TCDs agree to system-generated distribution reports.	Inspected a member tax collection district report and compared it to manual queries against the EIT Manager database and verified that the reports accurately reflected the tax revenue collected for the month and the revenue was disbursed on a weekly basis for the member tax collection districts.	No exceptions noted.
		Inspected a member tax collection district report and compared it to manual queries against the EIT Manager database and verified that the tax revenue collected was disbursed on a weekly basis for the member tax collection districts.	No exceptions noted.

Control Environment Controls

Control Objective 8: Controls provide reasonable assurance that personnel practices are in place to govern the hiring of new personnel.

Provided by Keystone Collections Group		***Procedures Performed by McGladrey LLP***	
Control		**Test Performed**	**Test Results**
8.1	Background checks are completed for new employees.	Inspected a sample of new hire records and verified that a background check was completed.	No exceptions noted.
8.2	Employees are required to sign a confidentiality agreement.	Inspected a sample of new hire records and verified that a confidentiality agreement was signed.	No exceptions noted.
8.3	Employees are required to sign an agreement stating that they read and understood the Employee Handbook, which includes acceptable-use policies.	Inspected a sample of new hire records and verified that a signed handbook was on file.	No exceptions noted.
		Inspected the Employee Handbook and verified that it includes acceptable-use details for email and Internet.	No exceptions noted.

Information Technology General Controls

Control Objective 9: Controls provide reasonable assurance that systems are monitored and issues are identified and resolved.

Provided by Keystone Collections Group		*Procedures Performed by McGladrey LLP*	
Control		**Test Performed**	**Test Results**
9.1	Automated software utilities are in place to monitor the EIT Manager and eFile applications, and the underlying network and infrastructure supporting the applications. Monitoring is performed at the network, server and database level for the systems. eFile is also monitored from the Internet to verify that the Web server is available to taxpayers.	Inspected the monitoring systems for the network, database, servers, EIT Manager and eFile applications and verified that they were proactively monitored using automated software tools.	No exceptions noted.
		Observed the monitoring console used by the IT department to detect issues with applications, databases and servers, and verified that emails were sent to IT department members to notify them of technical issues with the systems.	No exceptions noted.
		Inspected the monitoring application for the eFile system and verified that it was monitored from the Internet to verify that the Web server is available to taxpayers.	No exceptions noted.
9.2	Quarterly vulnerability assessments are performed by management to verify that the network is protected from unauthorized access. Scans are performed on the external network and at the application layer for the eFile system.	Inspected a sample of quarterly vulnerability assessments and verified that they were completed and that high-risk or critical issues detected by the software were addressed by management and a timeline for correction was established and that issues were resolved.	No exceptions noted.

Control Objective 10: Controls provide reasonable assurance that data is backed up regularly and is available for restoration in the event of processing errors or unexpected processing interruptions.

Provided by Keystone Collections Group		***Procedures Performed by McGladrey LLP***	
Control		**Test Performed**	**Test Results**
10.1	A management-approved backup policy is in place that identifies the requirements for the types of backups to be performed, the frequency of backups and the rotation of backup tapes.	Inspected the backup policy and verified that it detailed the following: • Types of backups performed • Frequency of backups • Rotation of backup tapes	No exceptions noted.
		Inspected the backup policy and verified that it was management-approved.	No exceptions noted.
10.2	Transaction logs for EIT Manager and eFile are backed up hourly, and full database backups are performed on a daily basis.	Inspected the backup configuration and verified that EIT Manager and eFile transactions are configured to be backed up hourly.	No exceptions noted.
		Inspected the backup software configuration and verified that the database is fully backed up on a daily basis.	No exceptions noted.
10.3	Environmental controls are in place to protect the computer room at the processing facilities, including the following: • Uninterruptible power supply (UPS) systems with generator backup • Temperature sensors • Handheld dry chemical fire extinguishers • Raised floors	Observed the following environmental controls in the computer room: • UPS systems and generator backup • Temperature sensors • Handheld dry chemical fire extinguishers • Raised floor	No exceptions noted.
		• Inspected a sample of weekly generator test logs and verified that the generator was tested weekly.	No exceptions noted.

Control Objective 11: Controls provide reasonable assurance that data transmissions between the service organization and its user entities and other outside entities are from authorized sources and are secure.

Provided by Keystone Collections Group		***Procedures Performed by McGladrey LLP***	
Control		**Test Performed**	**Test Results**
11.1	The Data Access Policy requires that data transmissions from taxpayers and business partners are encrypted.	Inspected the Data Access Policy and verified that it required that data transmissions from taxpayers and business partners are encrypted to reduce the risk of unauthorized access.	No exceptions noted.
11.2	Remote access for employees requires an encrypted connection.	Inspected the configuration of the remote access system and verified that it required encryption for user sessions and would not permit unencrypted access to the system.	No exceptions noted.
11.3	Access to the eFile application over the Internet requires SSL connections. Taxpayers are redirected to a secured connection when they access the website. A current SSL certificate is maintained by Keystone.	Inspected the eFile application and verified that when connecting to the application, an SSL-secured connection was required.	No exceptions noted.
		Inspected the SSL certificate configuration and verified that it was current, from an established certificate provider and not a self-signed certificate.	No exceptions noted.

Control Objective 12: Controls provide reasonable assurance that logical access to programs, data and computer resources is restricted to authorized and appropriate users.

Provided by Keystone Collections Group		***Procedures Performed by McGladrey LLP***	
Control		**Test Performed**	**Test Results**
12.1	The Data Access Policy documents management's directives for information security management and includes the following topic areas: • Access control • User provisioning • Network security • System monitoring The policy is reviewed and approved by management on an annual basis.	Inspected the Data Access Policy and verified that the policies cover the following information security topic areas: • Access control of the network • User provisioning • Network security • System monitoring	No exceptions noted.
		Inspected the Data Access Policy and verified that it is approved by management annually.	No exceptions noted.
12.2	Access to the EIT Manager system uses a single sign-on mechanism and is based on Active Directory group membership.	Inspected the EIT Manager application and verified that the system used a single sign-on mechanism for access control and authentication that is dependent upon Active Directory and requires membership in a specific Active Directory group.	No exceptions noted.
12.3	Firewalls, intrusion prevention system and spam filters are in place at the perimeter of the network to reduce the risk of unauthorized access.	Observed the firewall and IPS system physically installed in the data center.	No exceptions noted.
		Observed management log on to the management consoles for the firewall and IPS systems.	No exceptions noted.
		Inspected the signature file for the spam filter system and verified that it was up to date and that the system was licensed.	No exceptions noted.
		Inspected the signature file for the IPS system and verified that it was up to date and that the system was licensed.	No exceptions noted.
		Inspected a network diagram and verified that the firewall was placed on the perimeter of the network and that all traffic was filtered through the firewall.	No exceptions noted.
12.4	Access to Active Directory is restricted to authorized personnel. Access authorization forms are used to document the approval for new system accounts.	Inspected a sample of Active Directory users and verified that user accounts were assigned to authorized personnel and that the purpose of service accounts were identified by management.	No exceptions noted.
		Inspected a sample of new hires and requested a copy of their access authorization form and verified that it was completed and approved.	No exceptions noted.

Control Objective 12: Controls provide reasonable assurance that logical access to programs, data and computer resources is restricted to authorized and appropriate users.

Provided by Keystone Collections Group		***Procedures Performed by McGladrey LLP***	
Control		**Test Performed**	**Test Results**
12.5	Terminated employees' access to Active Directory is revoked when they leave the organization. Termination forms are used to document the revocation of access upon employee termination.	Inspected a sample of Active Directory users and compared it to a list of terminated users and verified that terminated users did not have access to the network.	No exceptions noted.
		Inspected a sample of terminated users and verified that completed termination forms were on file for the users.	No exceptions noted.
12.6	Administrative access to Active Directory is restricted to authorized and appropriate personnel.	Inspected a list of users with domain administrator privileges and verified that it was restricted to authorized and appropriate IT department personnel.	No exceptions noted.
12.7	Users are identified on Active Directory through the use of unique access credentials; shared accounts for user access are not used in the production environment. The purpose of service and application accounts are identified by management.	Inspected a sample of Active Directory accounts and verified that users were assigned unique accounts and that management could identify and justify the purpose of service and application accounts.	No exceptions noted.
12.8	Automated authentication controls are in place for Active Directory, including the following requirements: • Passwords have a minimum length of eight characters. • Password complexity is enforced. • Password rotation is required every 45 days. • A password history of 24 iterations is retained. • Accounts are locked out after 10 invalid access attempts for a period of 60 minutes. • Screensaver lockout occurs after 15 minutes.	Inspected the configuration of the domain and verified that the following password requirements were enforced for user accounts: • Passwords have a minimum length of eight characters. • Password complexity is enforced. • Password rotation is required every 45 days. • A password history of 24 iterations is retained. • Accounts are locked out after 10 invalid access attempts for a period of 60 minutes. • Screensaver lockout occurs after 15 minutes.	No exceptions noted.
12.9	Employees are restricted from local administrator access on their workstations.	Observed the manager of IT infrastructure log on to a sample of employee workstations and verified that the users did not have local administrative access.	No exceptions noted.
12.10	Access to the database is restricted to authorized personnel.	Inspected a list of SQL database groups and users and verified that user accounts were assigned to authorized personnel and that the purpose of service accounts was identified by management.	No exceptions noted.

Control Objective 13: Controls provide reasonable assurance that physical access to computers and other resources is restricted to authorized and appropriate personnel.

Provided by Keystone Collections Group		***Procedures Performed by McGladrey LLP***	
Control		**Test Performed**	**Test Results**
13.1	Physical access to the office facility is restricted to authorized personnel using proximity key cards. Terminated employees' proximity key cards are revoked when their employment is ended.	Inspected a sample of badges from the physical access system and verified that they were assigned to authorized personnel.	No exceptions noted.
		Inspected a sample of terminated employees and verified that they did not have active access badges for the facilities.	No exceptions noted.
13.2	Physical access to the computer room is limited to authorized personnel.	Inspected a sample of badges with access to the computer room and verified that they were assigned to authorized and appropriate personnel.	No exceptions noted.
13.3	Proximity badge readers and cameras are in place at entrances to the facility. The main entrance is also monitored by a receptionist during business hours and locked after hours.	Observed the placement of security cameras at entrances to the facility.	No exceptions noted.
		Observed proximity badge readers at all entrances with the exception of the main entrance.	No exceptions noted.
		Observed that the main entrance is monitored by a receptionist during business hours.	No exceptions noted.
13.4	Cameras are placed throughout the mailroom and check processing area to record activity within the facility.	Observed that cameras are in place in the mailroom and check processing area and at the entrances and exits to the mailroom/processing area.	No exceptions noted.
		Observed the camera system and verified that live footage is being transmitted to management's DVR computer.	No exceptions noted.
13.5	Access to the mailroom is restricted using a proximity card system.	Inspected a sample of proximity cards that had permissions to access the mailroom and check processing area and verified that the cards were assigned to authorized and appropriate personnel based on a review of the individual's title and job description.	No exceptions noted.

Control Objective 14: Controls provide reasonable assurance that changes to application programs and related data management systems are authorized, documented, approved and implemented.

	Provided by Keystone Collections Group	***Procedures Performed by McGladrey LLP***	
	Control	**Test Performed**	**Test Results**
14.1	The SDLC Policy details the SDLC and change management procedures for the infrastructure and applications. The SDLC Policy is reviewed and approved by management annually.	Inspected the SDLC Policy and verified that it defined the procedures for software development and change management for the organization.	No exceptions noted.
		Inspected the SDLC Policy and verified that the policy is reviewed and approved by management annually.	No exceptions noted.
14.2	A separate test environment is in place for QA testing and user acceptance testing.	Inspected a hardware inventory and the SDLC Policy and verified that separate environments were in place for the following: • Development testing • QA testing • User acceptance testing • Production	No exceptions noted.
14.3	A change ticket system is used to track changes to the applications. Requested changes are documented in the system. The changes are reviewed and approved by management before the change is completed.	Inspected a sample of application change documentation from the change ticketing system and verified that the changes were reviewed and approved by management.	No exceptions noted.
14.4	Application developers do not have access to the production server to make changes to the system. Only one server can push application changes into production. Access to this server is restricted to authorized and appropriate personnel.	Inspected the hardware inventory and verified that the production application server is documented.	No exceptions noted.
		Inspected the users with access to the production application server and verified that access is restricted to authorized and appropriate personnel.	No exceptions noted.
14.5	Access to the application source code is restricted to authorized and appropriate personnel.	Inspected a sample of users with access to the source code repository and verified that the users' access was authorized and appropriate.	No exceptions noted.
14.6	A change ticketing system is used to track changes to the network infrastructure. Tickets are appropriately documented and approved by management prior to implementation.	Inspected a sample of change tickets and verified that they were documented with the date, description, severity and urgency descriptions.	No exceptions noted.
		Inspected a sample of changes and verified that the they were and approved by management.	No exceptions noted.
14.7	An implementation plan and a back-out plan is documented for changes.	Inspected a sample of change tickets and verified that they included implementation instructions and back-out procedures.	No exceptions noted.

Control Objective 14: Controls provide reasonable assurance that changes to application programs and related data management systems are authorized, documented, approved and implemented.

Provided by Keystone Collections Group		***Procedures Performed by McGladrey LLP***	
Control		**Test Performed**	**Test Results**
14.8	Access to make infrastructure changes (e.g., operating system patch upgrades) are restricted to authorized users.	Inspected the administrative domain user groups in Active Directory and verified that they were appropriate and based on job responsibilities.	No exceptions noted.

V. Other Information Provided by Keystone Collections Group

Business Continuity and Disaster Recovery

Keystone has developed a Disaster Recovery Plan to be implemented in the event of an emergency, disaster or prolonged interruption of service to user entities. The purpose of the plan is to ensure information system uptime, data integrity and availability, and business continuity. The Disaster Recovery Plan provides directions, contact information and other steps to facilitate the recovery from different types of organizational interruptions and disasters. Keystone's Disaster Recovery Plan exercises reasonable measures to protect employees and safeguard assets and client data.

In the event of an extreme disaster that negatively effects the location of the primary applications, servers and infrastructure servicing user entities, the Disaster Recovery Plan provides for the ability to utilize a recovery site. The recovery site is a sufficient distance from the main processing facility and data center to provide reasonable assurance that an environmental disaster would not affect the secondary backup location. Backup copies of data needed for the tax collection system are retained at the secondary site so that both electronic and manual processing activities can continue at this location and other Keystone facilities.

The Disaster Recovery Plan was developed based on a risk assessment that determined the requirements for the disaster recovery plan. The Disaster Recovery Plan identified essential and critical infrastructure elements, systems and networks in accordance with key business activities. The Disaster Recovery Plan is periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed. Keystone's staff are trained on the Disaster Recovery Plan and their own respective roles in the recovery process. The Disaster Recovery Plan is kept up to date to take into account changing circumstances and risks that could affect Keystone's processing environment.