System and Organization Controls (SOC) 1 Type 2 Report

Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting (ICFR)

FTHC, LLC d/b/a Miami Data Vault
Data Center System (except the west side of the second floor)

For the Period August 1, 2020 to July 31, 2021

TABLE OF CONTENTS

I. INDEPENDENT SERVICE AUDITOR'S REPORT

To Management of FTHC, LLC d/b/a Miami Data Vault:

Scope

We have examined FTHC, LLC d/b/a Miami Data Vault's ("MDV", "Company" or "Service Organization") data center system (except the west side of the second floor) entitled "Description of FTHC, LLC d/b/a Miami Data Vault's Data Center System (except the west side of the second floor)" for user entities of the system throughout the period August 1, 2020 to July 31, 2021 ("description"), and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in MDV's Assertion ("assertion"). The controls and control objectives included in the description are those that Management of MDV believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the data center system (except the west side of the second floor) that are not likely to be relevant to user entities' internal control over financial reporting.

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 MDV's controls are suitably designed and operating effectively, along with related controls at the Service Organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

The information included in Section V, "Other Information Provided by FTHC, LLC d/b/a Miami Data Vault" is presented by Management of MDV to provide additional information and is not a part of MDV's description made available to user entities throughout the period August 1, 2020 to July 31, 2021. Information about MDV's Management's response to exceptions identified in the report 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 controls to achieve the related control objectives stated in the description and, accordingly, we express no opinion on it.

Service Organization's responsibilities

In Section II of the report, MDV 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. MDV is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service auditor's responsibilities

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

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in Management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period August 1, 2020 to July 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 in the description, and suitability of the criteria specified by the Service Organization in its assertion.

Inherent limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a Service Organization may not prevent, or detect and correct, all misstatements in storing data. 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 IV of the report.

Basis for qualified opinion

FTHC, LLC d/b/a Miami Data Vault states in the accompanying "Description Of FTHC, LLC D/B/A Miami Data Vault's Data Center System (except the west side of the second floor)" that zoned proximity access cards are utilized to manage physical access to the data center. However, as noted in section 4, due to a server failure during the period, authorized administrative MDV personnel were not able to add, modify, remove or generate listing of users from the access management software. As a result, we were unable to obtain sufficient audit evidence to determine whether control activities 8, 10 and 12 were suitably designed and operating effectively during the period August 1, 2020 to July 31, 2021, for control objective 2, "Controls provide reasonable assurance that the physical access to the facility, data centers, and computer and network equipment is restricted to authorized individuals."

Opinion

In our opinion, except for the matter described in the preceding paragraph, in all material respects, based on the criteria described in MDV's assertion—

- the description fairly presents the data center system that was designed and implemented throughout the period August 1, 2020 to July 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 August 1, 2020 to July 31, 2021, and user entities applied the complementary user entity controls assumed in the design of MDV's controls throughout the period August 1, 2020 to July 31, 2021.
- The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period August 1, 2020 to July 31, 2021, if complementary user entity controls assumed in the design of MDV's controls operated effectively throughout the period August 1, 2020 to July 31, 2021.

Restricted use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of MDV, user entities of MDV's data center system (except the west side of the second floor) during some or all of the period August 1, 2020 to July 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 misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Coral Gables, Florida
October 04, 2021

II. MANAGEMENT OF FTHC, LLC D/B/A MIAMI DATA VAULT ASSERTION

We have prepared the description of FTHC, LLC d/b/a Miami Data Vault's ("MDV", "Company" or "Service Organization") data center system (except the west side of the second floor) entitled "Description of FTHC, LLC d/b/a Miami Data Vault's Data Center System (except the west side of the second floor)" for user entities of the system during some or all of the period August 1, 2020 to July 31, 2021 ("description"), and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

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

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

1. The description fairly presents the data center system (except the west side of the second floor) made available to user entities of the system during some or all of the period August 1, 2020 to July 31, 2021, for storing data. The criteria we used in making this assertion were that the description:

    A. Presents how the system made available to user entities of the system was designed and implemented, including:

        i. The types of services provided.

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

        iii. How the system captures and addresses significant events and conditions.

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

        v. 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.

        vi. Other aspects of our control environment, risk assessment process, information and communication systems (including related business processes), control activities, and monitoring controls that are relevant to the services provided to user entities of the systems.

    B. Includes relevant details of changes to the data center system (except the west side of the second floor) during the period covered by the description.

C. Does not omit or distort information relevant to the system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors and may not, therefore, include every aspect of the data center system (except the west side of the second floor) that each individual user entity of the system and its auditor may consider important in its own particular environment.

2. Except for the matter described in paragraph below, the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period August 1, 2020 to July 31, 2021, to achieve those control objectives if user entities applied the complementary controls assumed in the design of MDV's controls throughout the period August 1, 2020 to July 31, 2021. The criteria we used in making this assertion were that:

   A. The risks that threaten the achievement of the control objectives stated in the description have been identified by Management of the Service Organization.

   B. 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.

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

   FTHC, LLC d/b/a Miami Data Vault states in the accompanying "Description Of FTHC, LLC D/B/A Miami Data Vault's Data Center System (except the west side of the second floor)" that zoned proximity access cards are utilized to manage physical access to the data center. However, as noted in section 4, due to a server failure during the period, authorized administrative MDV personnel were not able to add, modify, remove or generate listing of users from the access management software. As a result, we were unable to obtain sufficient audit evidence to determine whether control activities 8, 10 and 12 were suitably designed and operating effectively during the period August 1, 2020 to July 31, 2021, for control objective 2, "Controls provide reasonable assurance that the physical access to the facility, data centers, and computer and network equipment is restricted to authorized individuals."

Management of FTHC, LLC d/b/a Miami Data Vault
October 04, 2021

III. DESCRIPTION OF FTHC, LLC D/B/A MIAMI DATA VAULT'S DATA CENTER SYSTEM (EXCEPT THE WEST SIDE OF THE SECOND FLOOR)

SCOPE AND PURPOSE OF DESCRIPTION

This description is intended to provide clients of FTHC LLC, Miami Data Vault ("MDV", "Company" or "Service Organization") with information about controls applicable to their data center system (except the west side of the second floor) in order for independent auditors of MDV's clients to plan their audits. As this description is intended to focus on features that may be relevant to the internal control structure of MDV's clients, it does not encompass all aspects of the services provided or procedures followed by the Service Organization.

The scope of this report is limited to the MDV's data center operations and does not apply to any other products or services of the Company. Additionally, this report does not cover any applications and/or related environments hosted at the facilities owned or operated by the Company's clients.

COMPANY OVERVIEW

MDV is a Florida Limited Liability Company formed in 2000 that provides data center space of various size and configurations to end user entities (referred to as "user entities" or "customers" throughout) at its Data and Disaster Recovery Center ("DDRC") facility in Miami, Florida. Coupled with this space, MDV provides dedicated power circuits of various capacities and interconnections to multiple telecommunications and internet-based networks located within the facility.

The overall goal of MDV is to provide 24/7 access to secure space within a hardened, hurricane resistant building. The Data Center ("DC") space is supported by redundant, high reliability systems throughout all aspects of the facility. From multiple power feeds from Florida Power and Light to redundant internal power circuits to redundant HVAC systems, the DDRC minimizes single points of failure. MDV monitors and manages the performance of all internal systems and associated applications in a proactive, predictive and preventative manner.

Another space option within MDV is dedicated Disaster Recovery ("DR") space. MDV DC customers have the option of contracting for DR space for use by their operating personnel during emergencies or outages at their main offices. Typically, these spaces are configured to replicate the operating systems within the customers' primary facility. In the event of an emergency of any kind (hurricane, fire, flood, etc.) the customer relocates key personnel to MDV for seamless business continuity.

Optional DDRC services include one-time installation charges for DC cages, DR cubes, power circuits and cross-connects.

MDV Service Offerings (Individually ordered by Customers)

Cages - Customers contract for cage space within various internal MDV suites. The cages are configured to customer specification using standard MDV wire mesh panels. Once in place, the customer is issued a unique key and only that particular customer is allowed into that cage during the term of their agreement with MDV. Cages range in size from 50 - 1000 square feet. MDV currently maintains four active cage/cabinet rooms and one expansion cage/cabinet room within the facility.

Cabinets - Smaller customers contract for one or more equipment cabinets. These are dedicated to single customer use. Once installed, the customer is issued a unique key and only that particular customer is allowed to open that cabinet during the term of their agreement with MDV. Cabinets have both front and rear doors for cabling access.

DC Suites - Larger customers, or those with specialty needs, may contract for private suite space within MDV's primary areas. These suites provide added security and privacy for the customer. Suites are designed and built to suit the specific customer requirements.

DR Cubes - MDV provides dedicated cube space within the Disaster Recovery area. The cubes are similar to modular office cubes and available only to current MDV Data Center customers. The DR area is designed to support people rather than servers or network equipment. DR customers configure their space to replicate their primary data processing systems. The DR cubes are primarily used only during customer emergencies or for disaster recovery testing drills.

DR Suites - As within the Data Center, some customers require additional security or privacy, MDV designs and builds DR suites to suit individual customer requirements.

Power - All MDV customers contract for power. Critical data center type equipment requires high reliability power. Power circuits are ordered by the Amp rating (20A, 30A, 50A, etc.) and charged on a monthly basis regardless of actual draw on the circuit. MDV Data Center power circuits are supported by a redundant Uninterruptable Power Supply ("UPS") system and diesel generator back-up power systems.

Cross-connects - The third MDV service offering is cross-connects. Once the customer installs and powers up their equipment, connections to the outside world are necessary. MDV manages a Master Cross-connect Network enabling any customer to connect to any network operating within the facility. The customer selects one or more network service providers and MDV connects their cage or cabinet to that provider. Cross-connect fees are charged monthly and vary by capacity.

HVAC - MDV HVAC units are monitored continually by MDV staff or security personnel. Any alarm activity is entered into shift activity and daily activity reports which are archived for 12 months. MDV personnel are immediately alerted to critical alarm conditions related to the HVAC units both electronically and by cell phone. All MDV suites are designed with redundant HVAC systems to eliminate single points of failure at all times.

MDV Features & Benefits (Included in all Customer Service Agreements)

Hurricane Hardened - The MDV facility was designed to the most stringent hurricane standards even before the current Category 1-5 designations were developed. MDV is a poured-in-place, steel reinforced, concrete bunker building. The building features a structurally integrated roof, 200 psf floor loading capacity and a dry, underground fiber entrance vault. MDV withstands any wind speeds without damage or flooding. The building is located on the 'Miami Ridge' above the floodplain.

Access Control - DDRC access is controlled by MDV issued security cards. Authorized cards open the entrance gate, main entrance door and authorized interior doors. Customers with access cards may only access their designated area of the facility. As an additional security level, once inside MDV, customers again present their card to the scanner located outside their designated area of the facility. Then they are required to press their index finger onto the biometric reader adjacent to the card reader. All ingress-egress access activity is stored for a period of 12 months.

Video Monitoring - MDV is equipped with an extensive network of video surveillance cameras. Interior and exterior activity is monitored 24/7. The guards monitor exterior and building core cameras in real time. Interior DDRC cameras are motion sensitive, creating a video archive of all interior activity. Images are stored for as long as there is memory available in case a reference to an event is required.

Standard Systems Monitoring - Primary MDV systems are monitored physically, electronically or both 24/7. MDV and security personnel physically tour the facility at regularly scheduled intervals checking for proper system performance and monitoring certain critical systems (UPS, stand-by generators, chillers, power distribution units (PDUs), and fire detection/suppression). Security personnel are alerted to critical alarm conditions both visually and audibly.

Security - DDRC customers require 24/7 access to their critical equipment. MDV has security guards on site 24/7. Guards are positioned within the Master Control Room at the entrance to the MDV facility. All incoming customers, visitors or vendors must register with the security guards before entering the restricted areas of the building.

Fire Detection - Fire detection systems are required in all commercial buildings. Due to the overall value of and the critical nature of the equipment operating within MDV, advanced fire detection systems are in place. Security personnel are immediately notified of even the slightest of a potential of a fire event. The fire alarm must be acknowledged and continues to alarm until appropriate action is taken. All alarms with associated actions are entered into MDV's daily logbook reporting system.

Fire Suppression - Due to MDV's design, construction and advanced Fire Detection systems an actual fire is highly unlikely. MDV is equipped with a double pre-action, dry-pipe, zoned fire suppression system. On an everyday basis the fire sprinkler system throughout the facility contains only compressed air to prevent unintended water leakage. Should the fire detection system within a specific area of the building not be acknowledged properly, the affected zone is energized with water in preparation of extinguishing a fire. Water is not released, however, until a sprinkler head in the affected zone melts indicating substantial fire presence. The dual action system functions automatically while allowing personnel to abort the discharge if deemed appropriate.

Backup Power - Power is an essential element of all Data Centers. MDV's Data Center power circuits are supported by a redundant UPS system. The UPS systems clean the power fed from the public utility, eliminating power spikes or surges. During a power outage, the UPS also serves as the immediate power source through an extensive battery back-up system. The UPS seamlessly picks up the power load allowing the emergency generators time to start up and stabilize before taking on the electrical load.

Once the generators warm up and are ready to handle the power load, a matter of minutes, the units automatically engage to send power throughout the internal electrical distribution system. MDV's customers' critical equipment remains fully functional and are unaffected by this power transfer. MDV has a master diesel fuel storage system on site to support the generators for many days if necessary.

HVAC - Proper temperatures and humidity control is another essential element of Data Centers. Each cage/cabinet room within MDV is equipped with redundant precision air conditioning and humidity control units. These units are zoned and designed to operate to allow ample time for servicing. Every area is maintained at a precise temperature range for the protection of the customers' equipment and a precise humidity range to control static electricity and eliminate condensation.

Network Access - Connection to local, regional and national telecommunications and data networks are also essential in a Data Center. MDV maintains a Master Cross-connect Network within the facility. This network provides each customer with nearly instant access to every network provider offering service at MDV. MDV network engineers provide all cabling from the network connection room, commonly referred to as a Meet-Me or POP room, to the individual customer cage or cabinet. Only MDV personnel are permitted to install or alter cabling outside the customers' designated space.

Fiber connections to MDV enter the building via diverse underground fiber vaults to prevent accidental cuts or inadvertent construction dig-ups. Once inside the building, the diverse fibers are then routed to the MDV Master Cross-connect Network for distribution throughout the facility.

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

The Company utilizes the Committee of Sponsoring Organizations (COSO) framework for its internal controls environment. The components of the COSO framework include the following:

- Control Environment: Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all components of internal control, providing discipline and structure.
- Risk Assessment: The entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks should be managed.
- Monitoring: The processes that assess the quality of internal control performance over time.
- Information and Communication: The identification, capture and exchange of information in a form and time frame that enable people to carry out their responsibilities.
- Control Activities: The entity has developed policies and procedures to help ensure the Service Organization's objectives are carried out and risks are mitigated.

The Company's internal control environment reflects the overall attitude, awareness, and actions of Management, the board of directors, and others concerning controls and the emphasis given to controls, as expressed by the Company's policies, procedures, methods, and organizational structure. The following is a description of the components of internal control pertaining to the Company's system.

Control Environment

Integrity and Ethical Values

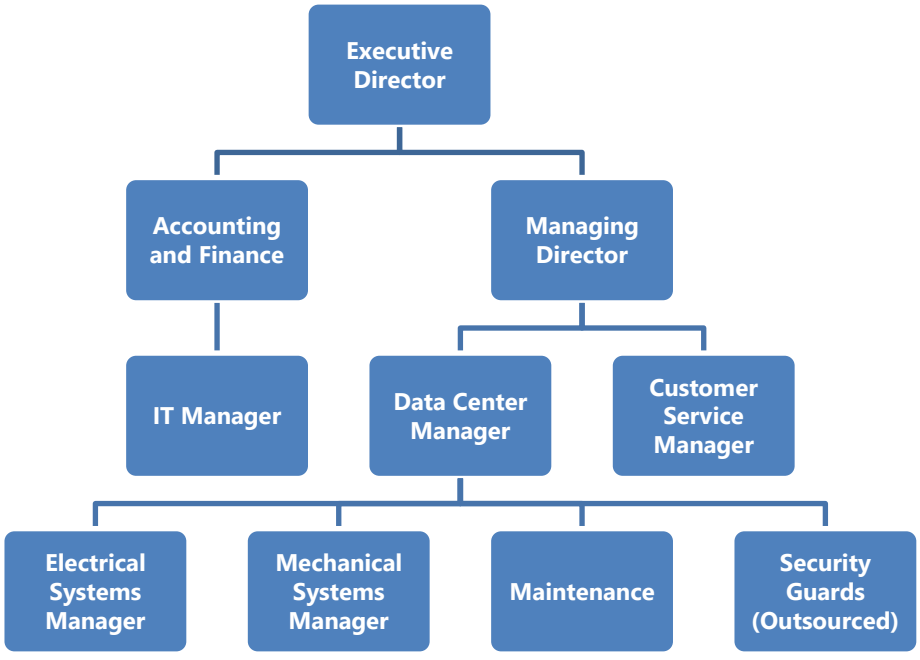
The Company and Management of MDV establishes a control environment within which employees must follow. It is a framework for all aspects of internal control. The control environment includes a commitment to the highest ethical standards that will never compromise the truth or the Company's values. Employees demonstrate professionalism through responsibility, accountability, and reliability in all interactions with clients and each other.

Management Oversight

The Company's control environment is the responsibility of its Executive Director and Managing Director as they oversee the activities related to MDV's service offerings. This team is responsible for establishing the overall policy and control environment and communicates regularly with the entire MDV staff to monitor the operations.

Organizational Structure

The Company maintains an organizational structure that provides a framework within, which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Significant aspects of establishing an effective organizational structure include defining key areas of authority and responsibility and establishing appropriate lines of reporting. The following organizational chart illustrates MDV's structure as of July 31, 2021.



Personnel Policies and Procedures

MDV strives to be a reliable and cost-effective Data Center operation. To achieve this, it is critical to keep turnover to a minimum. Each MDV employee has extensive experience in their field. Further, the electrical systems manager, mechanical systems manager, data center manager, and customer service manager each have additional specialized training as well as licenses and/or degrees in their respective technical areas. MDV covers the cost of third-party training and license renewal for these employees.

Security guards are provided by a third-party security services company. The guards are licensed through the completion of a 40-hour general security guard training course. Upon being assigned to MDV, security guards receive 16 hours of on-site training before working a shift alone. Security guards are provided with procedures during every shift.

The hiring practices are formalized and carefully performed. Approval by the Executive Director is required for all new employees. Before beginning employment, a candidate for any position must agree to a background check in writing. MDV utilizes the background screening and analysis services provided by a professional employer organization. MDV does not hire an employee without the professional employer organization's approval.

Each new employee is put through a formal orientation. The orientation process includes review of the policy manual, offers an organizational overview, a tour of the building, and discusses a range of procedures and job requirements.

Accountability

MDV's Management staff is the Executive Director and Managing Director. They have the ultimate responsibility for all activities within MDV, including the internal control system. This includes the assignment of authority and responsibility for operation activities, and establishment of reporting relationships and authorization protocols.

Risk Assessment

Through consideration of an entity's objectives and the strategies and plans for achievement of those objectives, Management specifies the competence levels required for particular jobs and translates those levels into requisite knowledge and skills. MDV Management has analyzed and defined the tasks and knowledge requirements that comprise the positions within the organization. They consider such factors to the extent to which individuals must exercise judgment and the extent of related supervision when making hiring decisions. MDV communicates this to personnel through the interview and ongoing Management processes. This commitment at all levels of the Company help ensure that a variety of risks, both internally and externally, are addressed.

Monitoring

Automated internal controls are monitored by MDV employees and Management. Remote enunciators are in operation to immediately alert the security staff and MDV Employees of alarms from the mechanical, electrical and fire suppression/detection units. All systems are monitored throughout the day by MDV staff or security personnel. Additionally, MDV's internal staff overseeing mechanical, electrical and fire suppression/detection systems are required to regularly perform and document performance readings from the various units.

Information and Communication

The Management team has an open door to clients and employees at all times and their direct contact information is openly communicated to ensure timely response occurs. This enables Management to participate in organizational controls. An operational emphasis is placed on building a team focused on working together to provide a secure facility that is protected from environmental threats.

MDV utilizes various methods of communication to ensure employees understand their individual roles and Company controls. Staff members are notified of changes and updates to security policies and procedures through ongoing email communication between MDV staff and Management.

Control Activities

The Service Organization has developed a variety of policies and procedures including related control activities to help ensure the Service Organization's objectives are carried out and risks are mitigated. These control activities help ensure that defined contribution plans are administered in accordance with the Service Organization's 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, investment trading, reconciliation activities, application development, compliance, and control monitoring, are allocated among personnel to ensure that a proper segregation of duties is maintained.

A formal program is in place to review and update MDV's policies and procedures on at least an annual basis. Any changes to the policies and procedures are reviewed and approved by Management and communicated to employees.

CONTROL OBJECTIVES AND RELATED CONTROLS

Control Objective 1 – Policies and Procedures

Controls provide reasonable assurance that the organization of the MDV facility and the security policies and procedures provide for Management oversight, segregation of duties and administrative/security practices with regard to security over customer assets stored in the facility.

The Company's facility is located at 100 NE 80th Terrace, Miami, FL. MDV maintains formalized security policies and procedures that provide for Management oversight, segregation of duties, and document the administrative and security practices of the Company with regard to the security over customer assets stored in the facility. MDV security policies and requirements and human resource policies are communicated to all levels in the Company. Corporate security policies are reviewed yearly and updated and approved by Management to remain current. Staff members are notified of changes and updates to security policies and procedures through ongoing email communication between MDV staff and Management. Employees are provided with ongoing informal training through close daily supervision to enhance their knowledge, skills, and security awareness to perform their job effectively.

Control Objective 2 – Physical Security

Controls provide reasonable assurance that the physical access to the facility, data centers, and computer and network equipment is restricted to authorized individuals.

Physical Access

General access to the MDV facility is monitored by security personnel at the entrance reception area. Security personnel are on duty 24 hours per day, seven days per week, year-round. Physical access to the facility is limited to MDV employees and individuals pre-authorized by the customer. Customer representatives or MDV employees may authorize visitor access for individuals not listed on the permanent, pre-authorized access list by giving their name to the security personnel before their arrival. Security personnel compare picture identification to records of authorized individuals on the customer contact list, before providing initial access to the facility and a zoned proximity card and biometric fingerprint scan for future access. Visitors requesting access must present picture identification (that is held by the security personnel for the duration of the visit) and be signed in and out on the appropriate access log. Visitors are provided with a visitor identification badge, which is worn at all times while on-site. While on-site, new visitors are escorted by MDV employees or authorized customer representatives, with the exception of the main hallway and the conference room areas which are common areas that do not contain cages and equipment. Recurring service vendors who have been trained by MDV personnel do not require escorts.

Physical access to the facility is controlled by an entrance mantrap and locked doors between all functional areas of the facility. Critical interior doors are activated for entrance by the use of the combination of zoned proximity card readers and biometric fingerprint readers. Customer's equipment is secured and physically separated from other customer equipment in locked cabinets or cages depending on physical size requirements. Authorized individuals are provided with a zoned proximity card for physical access within the facility with access rights as authorized by the customer. Permanent customer contacts are added or removed from the access management software by authorized administrative MDV personnel. When a contact is removed from the customer contact list, the Customer Service Manager receives notification emails and revokes access to the facility by deactivating the particular zoned proximity card.

Security Cameras

CCTV cameras are installed within the facility including common customer areas, data center floor space, the parking lot entrance gate, and other key points. Surveillance camera images are recorded and monitored by security personnel. Surveillance camera images are recorded and backed up as long as there is memory available. MDV Management immediately communicates employee terminations to the personnel responsible for physical deactivation at the facility. The computers running the MDV software programs, including the zoned proximity card software and video surveillance program, are located in secured rooms using physical keys or zoned proximity cards and are separate from customer cages/equipment.

Control Objective 3 – Environmental Controls

Controls provide reasonable assurance that the facility is protected against environmental threats.

Shift Activity Reports are recorded by security personnel to note instances and responses to alarms, events or other issues that occur during a shift that takes place during non-business hours (i.e., when the MDV employees are off-duty). Security personnel monitor environmental alarms in the facility (uninterruptible power supply ("UPS") systems, stand-by generators, chillers, PDUs, and fire detection/suppression) by touring the facility at regularly scheduled intervals, which are followed-up by MDV or local emergency service personnel.

The UPS systems and generators protect MDV and customer systems against local power utility spikes and failures. Reserves of diesel fuel are also maintained on-site to keep the generators running in the event of an extended outage. The UPS and generators are regularly maintained, inspected, and tested at the facility by a licensed electrician who is part of the full-time MDV staff to facilitate these processes and is on call for emergencies.

Fire detection is provided by VESDA systems or equivalent smoke detection systems, and fire suppression is provided by dry pipe sprinkler systems. Periodic inspection of the fire detection and suppression systems is conducted and documented.

The facility is equipped with zoned heating, ventilation, and air conditioning ("HVAC") units to maintain a constant cool temperature and humidity levels. The HVAC systems are periodically maintained and inspected. A licensed HVAC technician is part of the full-time MDV staff to facilitate these processes and is on call for emergencies.

COMPLEMENTARY USER ENTITY CONTROLS

MDV's controls cover only a portion of the overall internal control structure of each user entity. Each user entity's internal control structure must be evaluated in conjunction with MDV's controls and related testing detailed in this section of the report and take into account the related complementary user entity controls identified under each control objective. It is not feasible for the control objectives to be solely achieved by MDV. Certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of MDV's controls are suitably designed and operating effectively, along with related controls at MDV. Therefore, each user entity's internal control structure must be evaluated in conjunction with MDV controls and related testing detailed in this report and take into account the related complementary user entity controls identified below. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control structure to determine if the identified complementary user entity controls are in place. Furthermore, the complementary user entity controls are intended to address only those controls surrounding the interface and communication between user entities and MDV. Accordingly, the complementary user entity controls listed in Section IV do not purport to be and are not a complete list of the controls, which provide a basis for the assertions underlying the financial statements of user entities.

IV. DESCRIPTION OF MDV CONTROL OBJECTIVES AND RELATED CONTROLS, AND HANCOCK ASKEW'S DESCRIPTION OF TEST OF CONTROLS AND RESULTS

Information Provided by Hancock Askew

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 MDV.

Our examination was limited to the control objectives and related controls specified by MDV in sections 3 and 4 of the report and did not extend to controls in effect at user entities.

It is the responsibility of each user entity and its independent auditor to evaluate this 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, MDV's controls may not compensate for such weaknesses.

MDV's internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by MDV. In planning the nature, timing, and extent of our testing of the controls to achieve the control objectives specified by MDV, we considered aspects of MDV's 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:

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
Reperformance	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 MDV, 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.

Sampling

Consistent with American Institute of Certified Public Accountants authoritative literature (AU Section 350 Audit Sampling), there are two general approaches to audit sampling; nonstatistical and statistical. Hancock Askew practitioners used professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Hancock Askew practitioners, in accordance with AU Section 350, utilized nonstatistical sampling methods to select samples in such a way that the samples were expected to be a representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event, low frequency rate of the event, or low overall population size.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as exceptions are noted by the phrase "No exceptions noted" in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing exceptions identified within the Testing Matrices are not necessarily weaknesses in the total system of controls as this determination can only be made after consideration of controls in place at user entities, and other factors.

Policies and Procedures

Control Objective 1: Controls provide reasonable assurance that the organization of the MDV facility and the security policies and procedures provide for Management oversight, segregation of duties and administrative/security practices with regards to security over customer assets stored in the facility.

	Description of Control Activity	Test of Controls	Results
1	*Corporate Policies:* MDV maintains formalized security policies and procedures that provide for Management oversight, segregation of duties, and document the administrative and security practices of the Company with regard to the security over customer assets stored in the facility.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that policies were communicated. Inspected the Company's policies and procedures documents, employee handbook, and security services procedures to determine that MDV maintains formalized security policies and procedures that provide for Management oversight, segregation of duties, and document the administrative and security practices of the Company with regard to the security over customer assets stored in the facility.	No exceptions noted. No exceptions noted.
2	*Communication of Corporate Policies:* MDV Security Policies and Requirements and Human Resources policies are communicated to all levels in the Company.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that policies are reviewed and kept current and are communicated to all levels in the Company.	No exceptions noted.
3	*Review of Policies:* Corporate security policies are reviewed yearly and updated and approved by Management to remain current.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that policies are reviewed and kept current. Inspected the Company's security policies and procedures to determine that they Company's policies are reviewed yearly and updated and approved by Management to remain current.	No exceptions noted. No exceptions noted.

	Description of Control Activity	Test of Controls	Results
4	*Notification of Changes to Policy:* Staff members are notified of changes/updates to security policies and procedures through ongoing email communication between MDV staff and Management.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that policy changes/updates are communicated through email. Observed emails from Management to MDV staff regarding changes to security policies and procedures to determine that staff members are notified of changes and updates to security policies and procedures through ongoing email communication between MDV staff and Management.	No exceptions noted. No exceptions noted.
5	*Training:* Employees are provided with ongoing informal training through close daily supervision to enhance their knowledge, skills, and security awareness to perform their job effectively.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that ongoing informal training takes place. Observed while on site MDV employees receiving instruction and supervision from their superiors to determine that employees are provided with ongoing informal training through close daily supervision to enhance their knowledge, skills, and security awareness to perform their job effectively.	No exceptions noted. No exceptions noted.

Physical Security

Control Objective 2: Controls provide reasonable assurance that the physical access to the facility, data centers, and computer and network equipment is restricted to authorized individuals.

	Description of Control Activity	Test of Controls	Results
1	*Security Personnel*: General access to the MDV facility is monitored by security personnel at the entrance reception area. Security personnel are on duty 24 hours per day, 7 days per week, year-round.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that security personnel are always on duty. Observed the presence of security personnel onsite to determine that general access to the MDV facility is monitored by security personnel at the entrance reception area. For a random selection of days during the period, inspected a copy of the daily shift report to determine that security personnel are on duty 24 hours per day, seven days per week, year-round.	No exceptions noted. No exceptions noted. No exceptions noted.
2	*MDV Access Authorization*: Physical access to the facility is limited to MDV employees and individuals pre-authorized by the customer (user entity). Customer representatives or MDV employees may authorize visitor access for individuals not listed on the permanent, pre-authorized access list by giving their name to the security personnel before their arrival.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that access to the facility is limited to pre-authorized individuals. Observed employees and customers using a combination of zoned-proximity cards and fingerprint scanners to enter the gate and gain access to the building. Observed the visitor authorization process through visiting the MDV facility as a visitor.	No exceptions noted. No exceptions noted. No exceptions noted.

	Description of Control Activity	Test of Controls	Results
3	*Access Identification Requirements:* Security personnel compare picture identification to records of authorized individuals on the customer contact list, before providing initial access to the facility and a zoned proximity card and biometric fingerprint scan for future access.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that picture identification is required before initial access to the facility is provided. Inspected picture identification for a selection of authorized individuals on site and matched their zoned proximity card identification number to the access management software.	No exceptions noted. No exceptions noted.
4	*Visitor Access Logs:* Visitors requesting access must present picture identification (that is held by the security personnel for the duration of the visit) and be signed in and out on the appropriate access log.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that picture identification is held for visitors and that a visitor log is maintained. Observed visitors are required to provide picture identification to security personnel through visiting the MDV facility as a visitor and viewed other visitors wearing visitor badges. Observed the visitor sign-in process through visiting the MDV facility as a visitor. Inspected a sample of visitor access logs.	No exceptions noted. No exceptions noted. No exceptions noted. No exceptions noted.
5	*Visitor Access:* Visitors are provided with a visitor identification badge, which is worn at all times while on-site. While on site visitors are escorted by MDV employees or authorized customer representatives, with the exception of the main hallway and the conference room areas which are common areas that do not contain cages and equipment.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that visitors are required to wear badges and be escorted. Observed visitors wearing badges and being escorted by employees. Observed the handling of visitors through visiting the MDV facility as a visitor. Inspected a sample of visitor access logs.	No exceptions noted. No exceptions noted. No exceptions noted. No exceptions noted.

	Description of Control Activity	Test of Controls	Results
6	*Physical Access:* Physical access to the facility is controlled by an entrance mantrap and locked doors between all functional areas of the facility. Critical interior doors are activated for entrance by the use of the combination of zoned proximity card readers and biometric fingerprint readers.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that physical access is controlled is controlled by an entrance mantrap and locked doors between all functional areas of the facility. Critical interior doors are activated for entrance by the use of the combination of zoned proximity card readers and biometric fingerprint readers. Observed mantrap and locked doors separating critical areas and the presence of card and fingerprint readers. Tested the accuracy of the zones assigned to cards and fingerprint readers through the use of temporary access.	No exceptions noted. No exceptions noted. No exceptions noted.
7	*Customer Separation:* Customer's equipment is secured and physically separated from other customer equipment in locked cabinets or cages depending on physical size requirements.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that customer equipment is physically separated and secured. Observed locked cages and cabinets separating customer equipment.	No exceptions noted. No exceptions noted.
8	*Zoned Proximity Card Access*: Authorized individuals are provided with a zoned proximity card for physical access within the facility with access rights as authorized by the customer.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that only authorized individuals are provided zoned proximity cards that are restricted to the areas the customer has rights to. Inspected access rights for a sample of customers to determine whether access had been provided only to authorized individuals and only to the appropriate suites for that customer.	No exceptions noted. Exception noted. Due to a server failure during the period, authorized administrative MDV personnel were not able to add or remove permanent customer contacts from the access management software.

	Description of Control Activity	Test of Controls	Results
9	*Addition/Removal of Permanent Customer Access at MDV:* Permanent customer contacts are added or removed from the access management software by authorized administrative MDV personnel. Logical access to management software requires the use of a user ID and password.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that only authorized MDV employees have access to the access management software. Observed access management software and verified that a user ID and password is required to use the software.	No exceptions noted. No exceptions noted.
10	*Removal of Permanent Customer Zoned Proximity Cards at MDV*: When a contact is removed from the customer contact list, the customer service manager receives notification emails and revokes access to the facility by deactivating the particular zoned proximity card.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that access is revoked upon notification from the customer. Inspected documents authorizing access for a sample of individuals that were active per the access management software.	No exceptions noted. We were unable to perform testing due to a server failure during the period, authorized administrative MDV personnel were not able to remove permanent customer contacts from the access management software. If a contact was removed from the customer contact list, the Customer Service Manager was not able to revoke access to the facility by deactivating the particular zoned proximity card.

	Description of Control Activity	Test of Controls	Results
11	*Surveillance Cameras:* CCTV cameras are installed within the facility including common customer areas, data center floor space, the parking lot entrance gate, and other key points. Surveillance camera images are recorded and monitored by security personnel. Surveillance camera images are saved digitally and backed up as long as there is memory available.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that all key points of the facility are monitored by cameras and that the video is recorded and saved. Observed cameras throughout the facility and observation monitors. Observed video footage for various days selected from the period.	No exceptions noted. No exceptions noted. No exceptions noted.
12	*Removal of Employee Access:* MDV Management immediately verbally communicates employee terminations to the personnel responsible for physical deactivation of user access to the facility.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that access for a terminated employee would be revoked. For a selection of customer access lists, inspected the zoned proximity card access listing for the authorized customers to determine that access is disabled as defined for the selected customer.	No exceptions noted. We were unable to perform testing due to a server failure during the period, authorized administrative MDV personnel were not able to remove permanent employees from the access management software. If an employee was terminated, the Customer Service Manager was not able to revoke access to the facility by deactivating the particular zoned proximity card.

	Description of Control Activity	Test of Controls	Results
13	*Physical Security and Separation of Equipment:* The computers running the MDV software programs including the zoned proximity card software and video surveillance program are located in secured rooms using physical keys or zoned proximity cards and are separate from customer cages/equipment.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that computers running MDV software programs are secured. Observed the computers running the major MDV software programs noting they were located in locked rooms separate from customer equipment.	No exceptions noted. No exceptions noted.
Complementary User Entity Controls – User entities should ensure that a list of user entity personnel authorized to access the MDV facilities is submitted to MDV on timely basis and updated as required. – User entities should ensure that MDV is notified immediately of any terminated personnel that should be removed from the list of personnel authorized access to the MDV facility. – User entities should ensure that keys to the user entities' cage or cabinet at the facility are provided only to authorized individuals and that upon termination, the key is collected immediately from the terminated individual.			

Environmental Controls

Control Objective 3: Controls provide reasonable assurance that the facility is protected against environmental threats.

	Description of Control Activity	Test of Controls	Results
1	*Activity Reports and Building Management:* Shift Activity Reports are recorded by security personnel to note instances and responses to alarms, events or other issues that occur during a shift that takes place during non-business hours (i.e., when the MDV employees are off-duty). Security personnel monitor environmental alarms in the facility (uninterruptible power supply ("UPS") systems, stand-by generators, chillers, PDUs, and fire detection/suppression) by touring the facility at regularly scheduled intervals, which are followed-up by MDV or local emergency service personnel.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that alarm activity noted during walkthroughs is recorded on a shift activity report. For a sample of days, verified that alarms were documented on a shift activity report. Inspected security personnel post orders noting that instructions on how to respond to alarms were included. Observed Management conducting alarm drills for the HVAC and generator alarms. Inspected fire safety permit as evidence of tests performed by government officials.	No exceptions noted. No exceptions noted. No exceptions noted. No exceptions noted. No exceptions noted.
2	*Alternate Power Supplies:* Uninterruptible Power Supply systems (UPS) and generators protect MDV and customer systems against local power utility spikes and failures. Reserves of diesel fuel are maintained on-site to keep the generators running in the event of an extended outage.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that alternative power supplies are deployed to sustain power during extended outages. Observed the presence of UPS units, battery cabinets, permanent generators, fuel reserve tanks, and hookups for portable generators.	No exceptions noted. No exceptions noted.

	Description of Control Activity	Test of Controls	Results
3	*Maintenance of Alternate Power Supplies:* The UPS and generators are regularly maintained, inspected, and tested at the facility. A licensed electrician is part of the full-time MDV staff to facilitate these processes and is on call for emergencies.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that electrical equipment is maintained and that a licensed electrician is on staff full-time. Inspected documentation of electrical systems manager license. Inspected documentation of periodic electrical equipment readings and inspections. Inspected a selection of vendor invoices as evidence of maintenance supplies purchased for electrical equipment and maintenance performed on electrical equipment by third-parties.	No exceptions noted. No exceptions noted. No exceptions noted. No exceptions noted.
4	*Fire Detection and Suppression:* Fire detection is provided by VESDA systems or equivalent smoke detection systems, and fire suppression is provided by dry pipe sprinkler systems.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed the type of fire detection system. Observed fire system hardware and alarm boxes. Inspected service documents that indicated the system was a VESDA type system.	No exceptions noted. No exceptions noted. No exceptions noted.
5	*Maintenance of Fire Systems:* Periodic inspection of the fire detection and suppression systems is conducted and documented.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that the fire systems are inspected periodically. Inspected maintenance logs and fire safety permit. Inspected a selection of vendor invoices as evidence of maintenance supplies purchased for fire equipment and maintenance performed on the fire detection and suppression equipment by third-parties.	No exceptions noted. No exceptions noted. No exceptions noted.

	Description of Control Activity	Test of Controls	Results
6	*HVAC Systems:* The facility is equipped with zoned heating, ventilation, and air conditioning (HVAC) units to maintain a constant cool temperature and humidity levels.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that the facility is kept at low temperatures and humidity levels by multiple HVAC units. Observed HVAC units throughout the facility. Observed cool temperatures and low humidity levels throughout the facility.	No exceptions noted. No exceptions noted. No exceptions noted.
7	*Maintenance of HVAC Systems:* The HVAC systems are periodically maintained and inspected. A licensed HVAC technician is part of the full-time MDV staff to facilitate these processes and is on call for emergencies.	Through corroborative inquiry of the Customer Service Manager and Data Center Manager, confirmed that maintenance is performed periodically on the HVAC systems and that a licensed HVAC technician is on staff. Inspected documentation of Mechanical Systems Manager license. Inspected documentation of periodic mechanical equipment readings and inspections. Inspected a selection of vendor invoices as evidence of maintenance supplies purchased for mechanical equipment and maintenance performed on mechanical equipment by third-parties.	No exceptions noted. No exceptions noted. No exceptions noted. No exceptions noted.
Complementary User Entity Controls			
– User entities should ensure that they monitor proper temperature and humidity controls on their equipment.			

V. OTHER INFORMATION PROVIDED BY FTHC, LLC D/B/A MIAMI DATA VAULT

MANAGEMENT'S RESPONSE TO EXCEPTIONS IDENTIFIED

Hancock Askew was unable to perform testing for control activities 8, 10 and 12 for control objective 2. Due to a server failure during the period, authorized administrative MDV personnel were not able to add or remove permanent customer contacts and employees from the access management software.

MDV implemented the following actions during 2021 to address the server failure:

- Installed a new server with biometrics access control and upgraded the software system.
- Installed a secondary server for redundancy purposes in the event the primary server fails.
- Installed a network-attached storage as backup for users as well as servers.
- Implemented procedures to backup user files to OneDrive in the event that offsite access is necessary or in the event of user PC failure.