linford&co llp
cpa firm

linford&co llp
1550 wewatta st, 2nd floor
denver, co 80202

tel: +1 (720) 330 7201
email: info@linfordco.com
www.linfordco.com

June 16, 2022

Mark43, Inc.
28 E. 28th St., 12th Floor
New York, NY 10016

Type II SOC 2 & SOC 3 Completed

Mark43 has completed a Type II SOC 2 examination related to the public safety services covering the Security, Availability, and Confidentiality Trust Services Criteria. This report covered the period of April 1, 2021 through March 31, 2022. The examination resulted in an unqualified (clean) report opinion and was performed by Linford & Company LLP a Certified Public Accounting firm. The next examination will cover the period of April 1, 2022 through March 31, 2023.

Additionally, Mark43 completed a Type II SOC 3. The SOC 3 examination is designed to meet the needs of the general public that require assurances about the company controls and the company's compliance with the designed AICPA trust services criteria at a service organization. In Mark43's case, the Company SOC 3 includes the AICPA Trust services criteria of Security, Availability, and Confidentiality. The SOC 3 is for use by a general audience; a general audience does not have the need for the more detailed SOC 2 report. A SOC 2 report is a restricted report with a defined set of users, while the SOC 3 report can be distributed to the general public. The Type II SOC 3 report received by Mark43 provides an opinion about the effectiveness of the controls at the service organization relevant to the Security, Availability, and Confidentiality Trust Services Criteria. The Type II SOC 3 examination also resulted in an unqualified (clean) report opinion and was performed by Linford & Company LLP. The next SOC 3 examination will cover the period of April 1, 2022 through March 31, 2023.

The Type II SOC 2 and Type II SOC 3 opinions rely on the same controls and associated design and operating effectiveness testing. The Type II SOC 3 is a high-level overview of the results of the procedures and the Type II SOC 2 contains the detailed testing procedures and results.

Sincerely,

linford&co llp

linford&co llp
cpa firm

MARK43

SOC 3

REPORT ON CONTROLS RELEVANT TO SECURITY, CONFIDENTIALITY, AND AVAILABILITY

APRIL 1, 2021 TO MARCH 31, 2022

linford&co llp
cpa firm

▪ linford&co llp
1550 wewatta st, 2nd floor
denver, co 80202

▪ tel: +1 (720) 330 7201
email: info@linfordco.com
www.linfordco.com

Section I – Independent Service Auditor's Report

To the Management of Mark43 LLC:

We have examined Mark43 LLC's (Mark43 or the Company) accompanying assertion titled, "Assertion of Mark43's Management" (assertion) that the controls within Mark43's public safety services (system) were effective throughout the period April 1, 2021 to March 31, 2022 to provide reasonable assurance that Mark43's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Mark43 is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Mark43's service commitments and system requirements were achieved. Mark43 has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Mark43 is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- ✓ Obtaining an understanding of the system and service organization's service commitments and system requirements.
- ✓ Assessing the risk that controls were not effective to achieve Mark43's service commitments and system requirements based on the applicable trust services criteria.
- ✓ Performing procedures to obtain evidence about whether controls within the system were effective to achieve Mark43's service commitments and system requirements based on the applicable trust services criteria.

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within Mark43's public safety services were effective throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that Mark43's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

linford&co llp

April 28, 2022
Denver, Colorado

Section II – Assertion of Mark43's Management

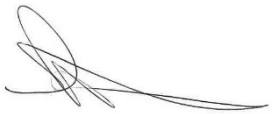
April 28, 2022

We are responsible for designing, implementing, operating, and maintaining effective controls within Mark43 LLC (Mark43 or the Company) public safety services (system) throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that Mark43's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in Section III and identifies the aspects of the system covered by our assertion.

We performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that Mark43's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust service criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Mark43's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented Section III.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that Mark43's service commitments and system requirements were achieved based on the applicable trust services criteria.



Steven Salberta
CFO

Section III – Mark43's Description of Its Public Safety Services

Overview of Operations and System Boundaries

Incorporated in 2012, Mark43 maintains its headquarters in New York City, and employs approximately 450 people with operational, technical, and project management expertise. Mark43 focuses on the design, development, implementation, and management of its products. Currently, Mark43 software is being used by over 100 different police agencies across the United States, with plans for future growth.

Mark43 is a provider of cloud-based enterprise software that allows law enforcement agencies to collect, manage, analyze, and share data seamlessly. With a mission to empower communities and their governments with new technologies that improve the safety and quality of life for all, Mark43's platform is made up of a Records Management System (RMS), a Computer-aided Dispatch System (CAD), an Analytics Suite, and a Property and Evidence System (EVD). Data from all Mark43 products is hosted on Amazon Web Service's (AWS) Government Cloud or Microsoft Azure Government Cloud.

Components of the System Used to Provide the Services

Infrastructure

Mark43 uses subservice organizations to achieve operating efficiency and obtain specific expertise. The following is the principal subservice organization used by Mark43:

- ✓ **Amazon Web Services (AWS):** AWS hosts Mark43's production IT environment. AWS undergoes semi-annual Type II SOC 2 examinations, and the current report may be obtained directly from them. Mark43 obtains and reviews the SOC 2 report provided by AWS related to their hosting operations to determine if controls are designed and operating effectively at AWS. Additionally, any listed complementary user entity controls in the AWS SOC reports are also reviewed and addressed by Mark43.
- ✓ **Microsoft Azure Cloud Services (Azure):** Azure hosts Mark43's production IT environment. Azure undergoes an annual Type II SOC 2 examination, and the report may be obtained directly from them. Mark43 obtains and reviews the SOC 2 report provided by Azure related to their hosting operations to determine if controls are designed and operating effectively at Azure. Additionally, any listed complementary user entity controls in the Azure SOC reports are also reviewed and addressed by Mark43.

Software

Mark43 is a public safety services solution for its user entities. The application is run on Windows and Linux servers and is developed and maintained by Mark43's engineering team. The software engineering team maintains the Mark43 application to provide services to its user entities. The application is a web-based software-as-a-service application with a network of verification providers that facilitates the identity verification process.

People
Mark43 has a staff of personnel organized into functional areas so personnel understand their responsibilities within the organization.

Data
Sensitive client data is stored within the Mark43 production database instance. Mark43 has implemented security controls to protect the confidentiality of the data. Client data within the application database is encrypted at rest. Additionally, all data transfers between users and Mark43 are secured using Transport Layer Security (TLS) and industry-standard encryption.

Processes and Procedures
Mark43 has established and maintains security policies and procedures over the public safety services. A subset of those policies and procedures includes the following areas:

- Information Risk Management
- Personnel Security
- Information Classification and Handling
- Information Security
- Physical Location
- Security Incident Response
- Change Management
- Business Continuity

Mark43 makes these internal policies and procedures, including security policies, available to its personnel on its company-wide document management system to provide direction regarding their responsibilities related to the functioning of internal control.

Mark43 also provides information to clients and employees on how to report failures, incidents, concerns, or complaints related to the services or systems provided by Mark43 in the event there are problems and takes actions as appropriate when issues arise.

Principal Service Commitments and System Requirements: Mark43 designs its processes and procedures to meet objectives for its public safety services. Those objectives are based on the service commitments that Mark43 makes to user entities and the compliance requirements that Mark43 has established for their services.

Security, availability, and confidentiality commitments to user entities are documented and communicated in their customer agreements, as well as in the description of the service offering provided online. Security, availability, and confidentiality commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental design of the Mark43 public safety services are implemented to permit system users access to the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Controlled access to the production infrastructure and client data.
- Segregation of client data.
- Data backups.
- Monitoring of system performance metrics and critical application services.

Mark43 establishes operational requirements that support the achievement of security, availability, and confidentiality commitments and other system requirements. Such requirements are communicated in Mark43 system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal networks are managed, and how employees are hired and trained.

(The remainder of this page is left blank intentionally.)