xMatters, Inc.

System and Organization Controls Report (SOC 3)

Independent Report of the Controls to meet the criteria for the Security, Availability, and Confidentiality categories for the period of October 1, 2020 through September 30, 2021.

KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

ASSERTION OF XMATTERS, INC. MANAGEMENT

ASSERTION OF XMATTERS, INC. MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within xMatters, Inc.'s incident management software-as-a-service system (system) throughout the period October 1, 2020, to September 30, 2021, to provide reasonable assurance that xMatters, Inc.'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 A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2020, to September 30, 2021, to provide reasonable assurance that xMatters, Inc.'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*). xMatters, Inc.'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 in section B.

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 October 1, 2020, to September 30, 2021, to provide reasonable assurance that xMatters, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

Board of Directors
xMatters, Inc.
12647 Alcosta Boulevard, Suite 425
San Ramon, CA 94583

Scope

We have examined xMatters, Inc.'s accompanying assertion titled "Assertion of xMatters, Inc. Management" (assertion) that the controls within xMatters, Inc.'s incident management software-as-a-service system (system) were effective throughout the period October 1, 2020, to September 30, 2021, to provide reasonable assurance that xMatters, Inc.'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

xMatters, Inc. is responsible for its service commitment and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that xMatters, Inc.'s service commitments and system requirements were achieved. xMatters, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, xMatters, Inc. 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. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. 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 the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve xMatters, Inc.'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 xMatters, Inc.'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 were 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 xMatters, Inc.'s incident management software-as-a-service system were effective throughout the period October 1, 2020, to September 30, 2021, to provide reasonable assurance that xMatters, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

October 27, 2021

XMATTERS, INC.'S DESCRIPTION OF ITS INCIDENT MANAGEMENT SOFTWARE-AS-A-SERVICE SYSTEM

SECTION A:
XMATTERS, INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS INCIDENT MANAGEMENT SOFTWARE-AS-A-SERVICE SYSTEM

Services Provided

xMatters, Inc. (xMatters) offers a software-as-a-service (SaaS) platform that allows its clients to manage and communicate information technology (IT) incidents internally, as well as to support and manage communication as part of business continuity plans. The organization offers the following services:

- **Incident Management** enables response to service interruptions across teams, cultures, and systems, and includes the following features:
  - Automated Resolution
  - Dynamic Collaboration
  - Data-Driven Process Improvements
  - Scalable, Service-Centric Model
- **IT Event Management** filters and prioritizes the most important system alerts and includes the following features:
  - Filtering and Suppression
  - Alert Correlation
  - Enriched Notifications
  - Context-Based Routing
  - Prioritization
- **Integration Platform** enables collaboration between people, data, and tools to resolve issues and includes the following features:
  - Orchestrated Toolchains
  - Hybrid Cloud Support
  - Integration Builder
  - Built-In Integrations
- **Flow Designer** enables integration, synchronization, and automation of toolchains and includes the following features:
  - IT Ops
  - DevOps & SRE
  - Major Incident Management
- **Smart Notifications** condense alert information from monitoring and issue-tracking tools in actionable notifications and include the following features:
  - Resolutions Actions
  - Situational Context
  - Stakeholder Alignment
  - Major Incident Coordination
  - Conference Call Engagement
- **On-Call Management** tracks schedules and shifts to ensure that issues are sent to appropriate personnel and includes the following features:
  - Coverage & Scheduling Calendar
  - Escalations

    - User Self-Service
    - Data Synchronization
- **Workflow & Process Automation** orchestrates and automates key resolution processes to drive efficiency and includes the following features:
    - Orchestrated Toolchain Resolution
    - Structured Communication Plans
    - Scenario Management
    - Post-Mortem Analysis
- **Performance Analytics** provide the insights and visibility into customer-facing incidents, digital service downtime, or unmanaged responses to critical issues and include the following features:
    - Incident Timeline
    - Real-Time Event Visibility
    - Instant Replay of Events
    - Team Performance
- **Enterprise Grade Architecture** drives data ingestion, event processing, and user management to fulfill support needs and includes the following features:
    - Data Security & Reliability
    - Globally Distributed Cloud Infrastructure
    - Hybrid Environment Interoperability
    - Role-Based Access and Administration
    - Scalable Group Management
    - Uptime Guarantees

NOTE: The organization was acquired by Everbridge on May 7, 2021. All service controls remain the same.

Infrastructure

xMatters maintains an inventory of its systems and assets; all workstations are managed centrally by the IT Team and the servers are all managed in the Google Cloud Platform (GCP) by the Operations and Engineering Teams. The inventory includes a description and function of each device and includes all virtual systems, containerized solutions, and network infrastructure.

xMatters also maintains formal network diagrams and a Separation in Operation document that illustrates its networks, systems, and the separation of its environments. These diagrams are reviewed, updated, and approved annually and as needed, and the Information Assurance Team and Cloud Architect are responsible for these documents.

Software

The organization maintains a complete software inventory that is reviewed against security and privacy requirements, updated, and approved annually and as needed.

People

The organization established a board of directors that is responsible for the oversight and stewardship of xMatters. However, in May 2021, xMatters was acquired by Everbridge, Inc.

The organization has established an Information Security and Privacy Management System (ISPMS) Steering Committee that is responsible for maintaining independence from executive management and ensuring that best practices and necessary compliance controls are implemented. A formal organizational chart is maintained that illustrates xMatters' functional structure and represents its ISPMS. The chart illustrates the hierarchy and clear reporting lines of the organization.

Data

xMatters maintains a formal Privacy Notice to guide its data collection, handling, and retention requirements, and this policy is maintained and implemented in compliance with the organization's required regulations.

The organization's formal Cryptographic and Key Management Policy outlines its requirements regarding its use and management of encryption keys. The organization manages its server-side encryption keys and encrypts client data at rest using AES-256, and transport layer security (TLS) v1.2 is used to encrypt all data at rest and in transit. xMatters encrypts all its passwords at rest and in transit using an encryption solution and secure sockets layers (SSL).

xMatters maintains a formal Client Data External Transfer process that governs its use and handling of client data, and the organization securely processes, stores, and transmits client data that is used to support its services delivered. xMatters maintains formal data maps and Records of Processing Activities (RoPA) that illustrate the data life cycle across systems and jurisdictions.

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices
- Risk management
- Supplier assessment
- Competence and training
- Continual improvement
- Corrective actions

SECTION B:
PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Regulatory Commitments

xMatters has formally acknowledged its compliance with the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Personal Information Protection and Electronic Documents Act (PIPEDA), the Australian Privacy Act and the New Zealand Privacy Act (NZPA), among other applicable privacy regulations in effect in the regions where it operates. Personnel are required to review and acknowledge consent to the organization's applicable regulations and requirements and are required to complete privacy training annually.

Contractual Commitments

xMatters executes contracts with its clients outlining organizational and client responsibilities, include security breach reporting requirements. Contractual commitments also detail security and confidentiality of data, data retention and deletion, controlling access to data, transparency, and limiting the use of sub-processors to approved third parties. The organization employs service-level agreements (SLAs) with all clients and third parties, and xMatters uses publicly available status pages to externally communicate its uptime requirements and services provided.

System Design

xMatters designs its incident management SaaS system to meet its regulatory and contractual commitments. These commitments are based on the services that xMatters provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that xMatters has established for its services. xMatters establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in xMatters' system policies and procedures, system design documentation, and contracts with clients and xMatters Trust Portal (website) and Support Portal.