



# MaxMind, Inc.

## System and Organization Controls Report (SOC 3)

Independent Report of the Controls to Meet the Trust  
Services Criteria for the Security, Availability,  
Confidentiality, and Processing Integrity Categories for  
the Period of March 1, 2023, through February 29, 2024.



# Table of Contents

---

- Assertion of MaxMind, Inc. Management..... 1
  - Assertion of MaxMind, Inc. Management..... 2
- Independent Service Auditor’s Report..... 3
  - Independent Service Auditor’s Report..... 4
  - Scope..... 4
  - Service Organization’s Responsibilities..... 4
  - Service Auditor’s Responsibilities..... 4
  - Inherent Limitations..... 5
  - Opinion..... 5
- MaxMind, Inc.’s Description of Its IP Address Intelligence and Fraud Detection Services System ..... 6
  - Section A: MaxMind, Inc.’s Description of the Boundaries of Its IP Address Intelligence and Fraud Detection Services System..... 7
    - Services Provided..... 7
    - Infrastructure ..... 7
    - Software ..... 8
    - People ..... 9
    - Data ..... 9
    - Processes and Procedures..... 9
  - Section B: Principal Service Commitments and System Requirements..... 11
    - Regulatory Commitments..... 11
    - Contractual Commitments..... 11
    - System Design ..... 11



# **Assertion of MaxMind, Inc. Management**



## Assertion of MaxMind, Inc. Management

---

We are responsible for designing, implementing, operating, and maintaining effective controls within MaxMind, Inc.'s IP address intelligence and fraud detection services system (system) throughout the period March 1, 2023, to February 29, 2024, to provide reasonable assurance that MaxMind, Inc.'s service commitments and system requirements relevant to Security, Availability, Confidentiality, and Processing Integrity 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 March 1, 2023, to February 29, 2024, to provide reasonable assurance that MaxMind, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, and Processing Integrity (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*). MaxMind, 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 March 1, 2023, to February 29, 2024, to provide reasonable assurance that MaxMind, 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

---

Thomas Mather  
Chief Executive Officer  
MaxMind, Inc.  
51 Pleasant Street #1020  
Malden, MA 02148

## Scope

We have examined MaxMind, Inc.'s accompanying assertion titled "Assertion of MaxMind, Inc. Management" (assertion) that the controls within MaxMind, Inc.'s IP Address Intelligence and Fraud Detection Services system (system) were effective throughout the period March 1, 2023, to February 29, 2024, to provide reasonable assurance that MaxMind, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, and Processing Integrity (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

MaxMind, 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 MaxMind, Inc.'s service commitments and system requirements were achieved. MaxMind, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, MaxMind, 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 MaxMind, 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 MaxMind, 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

### **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.

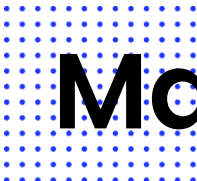
### **Opinion**

In our opinion, management's assertion that the controls within MaxMind, Inc.'s IP Address Intelligence and Fraud Detection Services system were effective throughout the period March 1, 2023, to February 29, 2024, to provide reasonable assurance that MaxMind, 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

May 31, 2024



# **MaxMind, Inc.'s Description of Its IP Address Intelligence and Fraud Detection Services System**



# Section A: MaxMind, Inc.'s Description of the Boundaries of Its IP Address Intelligence and Fraud Detection Services System

---

## Services Provided

MaxMind, Inc. (MaxMind) provides IP address intelligence (i.e., geolocation, proxy information, and other data associated with IP addresses) under the GeoIP brand, which is accessible via downloadable databases and web services. MaxMind also provides free versions of certain GeoIP services under the GeoLite brand. MaxMind also provides fraud detection services under the minFraud brand via web services, which is supplemented via online interfaces that feature additional supporting technology.

GeoIP provides geographical information, proxy information, registry information, country confidence subdivision, city postal, user type (residential, commercial, or mobile), average income, population density, user count static, and other types of information. The minFraud data analyzed may include device fingerprints, Card Verification Values (CVV), Address Verification System (AVS) results, Bank Identification Number (BIN), shipping addresses, networks, and location. This data is provided a machine-learned score to help clients to make a determination of whether the transaction is potential fraud. Fraud factors are initially created by applying the discovered online activity, GeoIP data, applied heuristics, machine learning, and fraud analysts to provide the overall data risk score. The minFraud and GeoIP can be used together as complementary services or can be used separately as standalone services.

Many clients are onboarded to MaxMind through a self-service model. Free accounts are created online by users. Some clients are considered high value accounts and are set up with a true onboarding implementation driven by an assigned account executive. The onboarding with these clients may include executing a negotiated agreement, which sometimes incorporates a service-level agreement (SLA). MaxMind provides two options for clients to pay them:

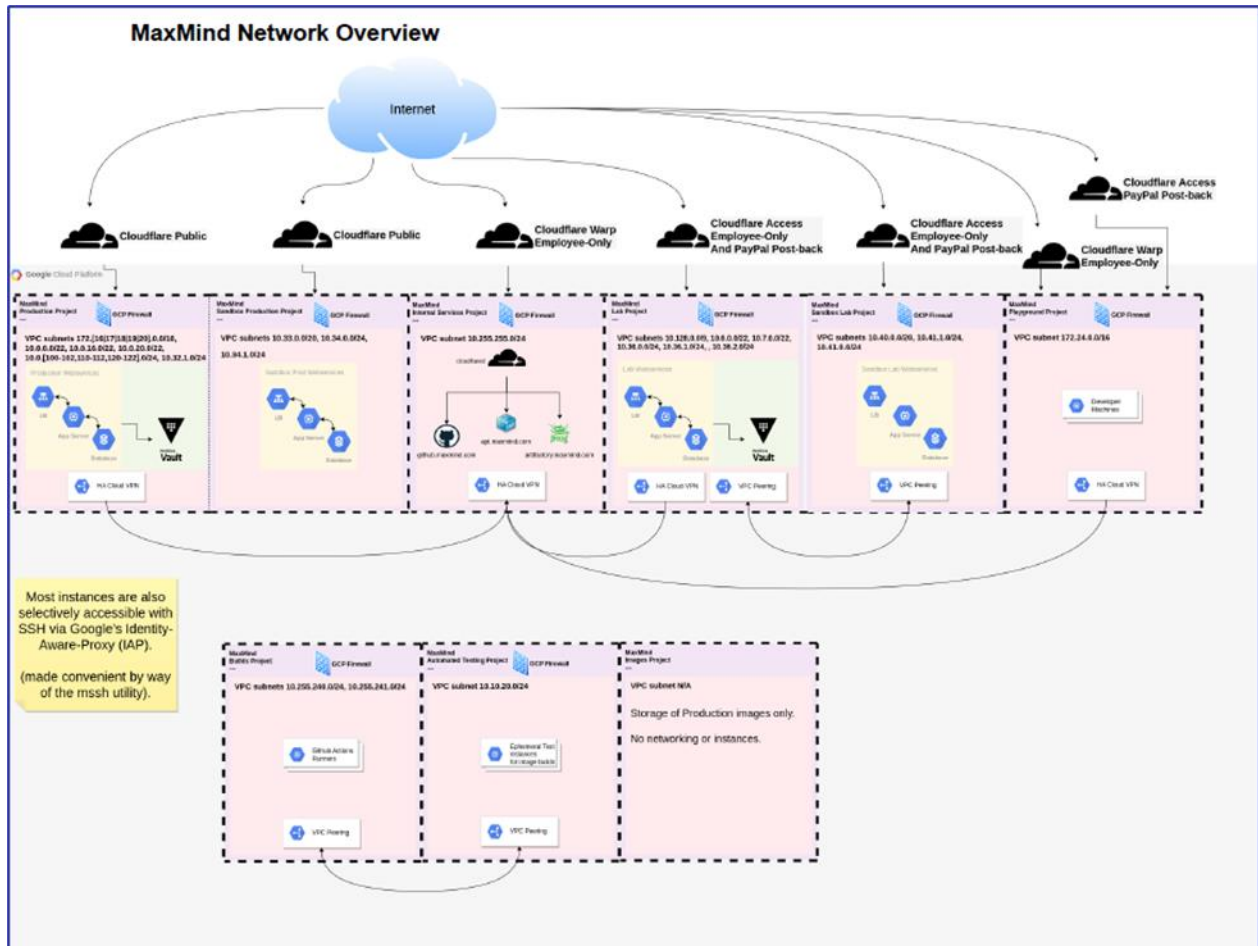
- An invoicing process wherein clients are invoiced and MaxMind receives payment directly by check or by automated clearing house (ACH)
- An online payment option via PayPal

The license ends when the license agreement is terminated in accordance with its provisions.

## Infrastructure

MaxMind maintains formally documented network diagrams, pictured below, that illustrate the company's architecture and network design. The organization has four distinct projects that are isolating access and protecting data between systems; these projects are the internal, development, lab, and production projects. Isolation is enforced through firewall and a multi-factor authentication (MFA) virtual private

network (VPN). The systems are further isolated as inbound, and outbound traffic is routed through Cloudflare access. The Site Reliability Engineering (SRE) team maintains the network diagrams, which are reviewed and approved quarterly.



MaxMind maintains an inventory of infrastructure, hardware, and networking equipment in line with the Inventory of Assets Policy. The equipment is used to support its services and includes a description of all devices. While a real-time inventory is maintained by a Google Cloud Platform (GCP), the SRE team reviews and updates the inventory as needed following reports from GCP. The SRE team reviews the reports manually and updates the inventory accordingly.

## Software

MaxMind maintains a comprehensive software and software-as-a-service (SaaS) tools inventory in line with the Inventory of Assets Policy. The inventory is used for performing the organization's IP Address Intelligence and Fraud Detection Services. The inventory includes the version numbers of the software and tools in use by the organization.

## People

MaxMind maintains a standard traditional hierarchy that enforces a separation of duties for each department and clear reporting lines. The company is privately held, and the Chief Executive Officer (CEO) and Chief Operating Officer (COO) are responsible for providing company oversight and direction. The CEO is responsible for company strategy and final decisions. The organization is divided into business and technical departments. The business departments include management, Human Resources (HR), Financial, and Legal, and the technical departments include SRE, Development, and Architecture. The company's organization chart illustrates the company structure, division of duties, and reporting lines.

## Data

MaxMind transmits, processes, and stores various types of data. The customer data collected includes potentially personally identifiable information (PII) data, such as IP address, billing, shipping addresses, and phone. The company maintains a formally documented data flow diagram that illustrates the flow of data within the minFraud and GeoIP service environments.

As described in the Information Classification Policy, the organization has a process for classifying data, as public, sensitive, or confidential. Once an asset is identified in the asset tracking system, a classification level is assigned for the data residing on the asset. Assets are then handled per their classification by the protection or handling of the asset. A "sensitive data" classification is an internal classification independent of and distinct from the definition of "sensitive data" under data privacy and protection laws such as the GDPR, CPRA, or Virginia Consumer Data Protection Act (CDPA).

All data transmissions within the organization's environment are encrypted via HTTPS using Transport Layer Security (TLS) 1.2 or higher and using the Advanced Encryption Standard (AES) encryption method. Some API endpoints for the Legacy GeoIP service do not require HTTPS and function over plaintext. All internal subnet network traffic is natively encrypted by default within the GCP virtual private cloud (VPC) network.

The organization manages encryption keys securely using Google Key Management System (KMS). An infrastructure-as-code tool is used to create and destroy encryption keys.

## 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

## **Section B: Principal Service Commitments and System Requirements**

---

### **Regulatory Commitments**

MaxMind works with internal corporate counsel, external privacy counsel, and an external Data Protection Officer (DPO) to advise MaxMind on compliance with relevant regulations applicable to MaxMind. The organization completes the applicable Payment Card Industry Data Security Standard (PCI DSS) SAQ A questionnaire. Privacy requirements such as General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) as replaced by the California Privacy Rights Act (CPRA), and other state requirements are considered when forming privacy and data retention policies.

### **Contractual Commitments**

All clients sign contracts, either through MaxMind's standard online clickwrap End-User License Agreement (EULA) or through negotiated contracts and agreements. Contracts detail the licensing terms applicable to those customers, which may include SLAs for GeoIP Web-Based Service and minFraud Service customers.

MaxMind maintains SLAs that document commitments for certain clients, and the service objectives are tracked throughout reporting and monitoring tools. SLA commitments are documented in the license agreement with the client, tracked through the customer relationship management (CRM) reporting tool, and monitored through the website performance and availability monitoring tool. The SLAs are reviewed internally on a monthly basis, and if an SLA is triggered during monitoring for these clients, the Customer Success Team works directly with the client to resolve the issue.

### **System Design**

MaxMind designs its IP Address Intelligence and Fraud Detection Services system to meet its regulatory and contractual commitments. These commitments are based on the services that MaxMind provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that MaxMind has established for its services. MaxMind establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in MaxMind's system policies and procedures, system design documentation, and contracts with clients.