# 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, 2025, through February 28, 2026.

# Table of Contents

# 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, 2025, to February 28, 2026, 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*, in AICPA *Trust Services Criteria*. Our description of the boundaries of the system is presented in attachment 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, 2025, to February 28, 2026, to provide reasonable assurance that MaxMind, Inc.'s service commitments and system requirements were achieved based on the applicable 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 attachment B.

Complementary subservice organization and user entity controls that are suitably designed and operating effectively are necessary, along with controls at MaxMind, Inc., to achieve MaxMind, Inc.'s service commitments and system requirements based on the applicable trust services criteria.

MaxMind, Inc. uses the subservice organizations listed below, and MaxMind, Inc. management has elected to use the indicated method with respect to the services provided by subservice organizations:

| Subservice Organization | Service Provided | Carve-Out or Inclusive |
|---|---|---|
| Google Cloud Platform | Data center infrastructure and storage services | Carve-out |
| Cloudflare | Network perimeter protection services | Carve-out |
| HubSpot | Customer ticketing and customer relationship management | Carve-out |
| Google Workspace | Business productivity services | Carve-out |

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, 2025, to February 28, 2026, 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

Thomas Mather
Chief Executive Officer
MaxMind, Inc.
51 Pleasant St, STE 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, 2025, to February 28, 2026, 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*, in 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.

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

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.

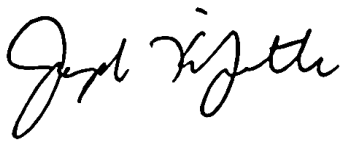
### Inherent Limitations

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, 2025, to February 28, 2026, 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

April 27, 2026

# Attachment 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 are 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 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.

MaxMind generates clients in one of two major approaches:

- Referrals from partner businesses that use GeoIP and minFraud as part of their services
- Conversion from GeoLite free accounts to paid accounts

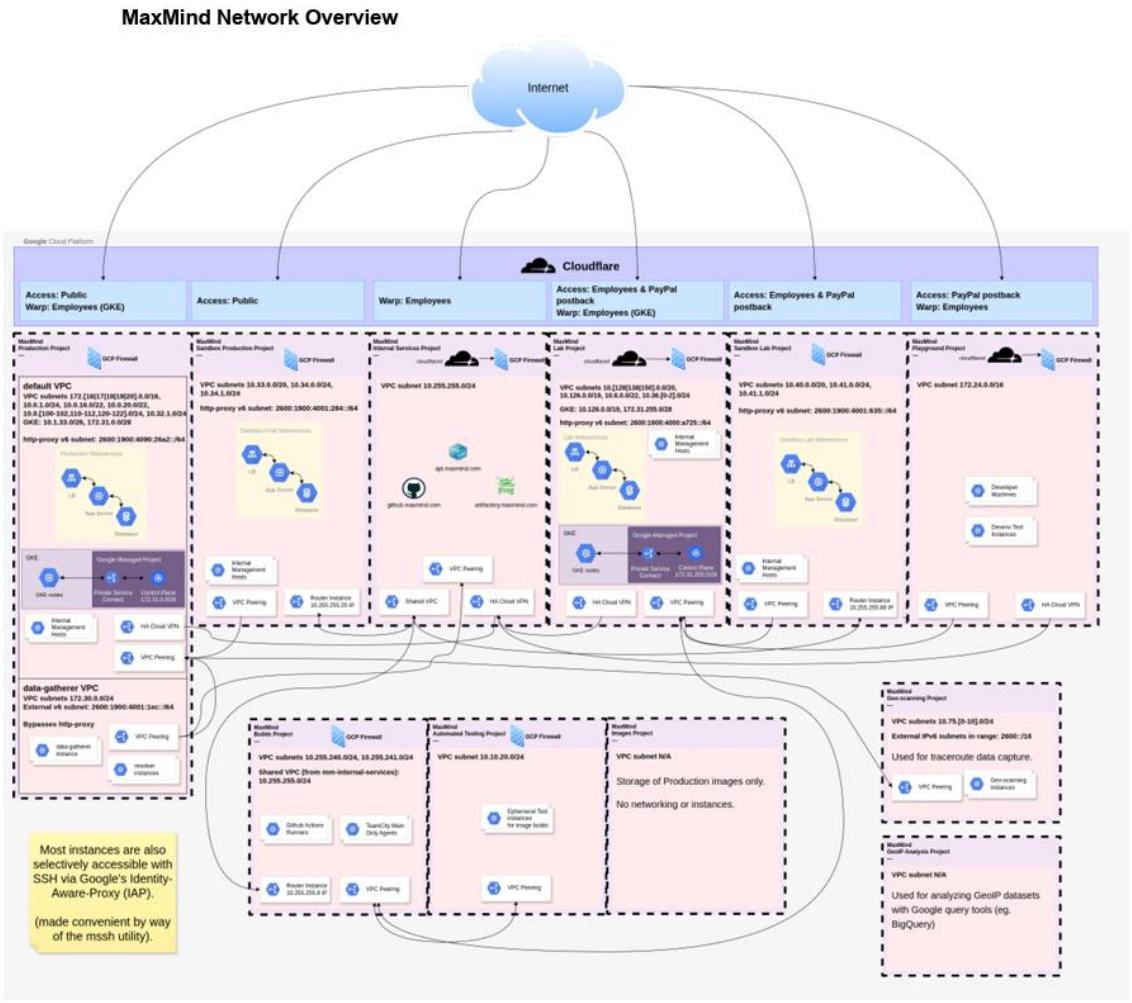
Many clients are onboarded to MaxMind through a self-service model. Free accounts are created online by users. Some clients are considered high value accounts and are set up with a true onboarding implementation driven by an assigned account executive. The onboarding with these clients may include executing 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

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

## Infrastructure

The organization has implemented access controls that restrict both ingress and egress at network boundaries, with firewall rules limiting inbound and outbound traffic to authorized ports, protocols, sources, and destinations. MaxMind also maintains a detailed network diagram that illustrates Cloudflare protection, connectivity to the internet and external networks, access restrictions, virtual private cloud (VPC) subnets and proxies, Google Cloud connectivity, trust boundaries, technologies within each environment, and paths between those environments. The network diagram is provided below:




## Software

MaxMind maintains a detailed inventory of all software applications and software-as-a-service (SaaS) tools that are in use. The inventory details software name, version, vendor, function, and whether the software was included in the most recent annual review.

## People

MaxMind is a privately held organization led by Chief Executive Officer (CEO), supported by upper management that includes the Chief Operating Officer (COO), Directors of Business Development, Chief Technology officer (CTO), Chief Product Officer (CPO), and Support. These leaders meet regularly with the CEO, supporting accountability. While the CEO sets the strategy and serves as the ultimate decision maker within the company, the supporting leadership roles provide guidance, counsel, and constructive criticism on proposed and implemented decisions.

## Data

MaxMind collects and processes data including cookies, website support data, privacy request data, data correction requests, customer-submitted data via API services, customer portal data, and internal corporate data. Individuals may submit privacy requests, which include the personal information necessary to validate identity and locate records, and may also submit requests to correct IP address intelligence data, which would require an individual to submit the data they wish to correct as well as an email address.

MaxMind labels and tags data according to sensitivity level to guide handling and protection requirements, ensuring that personnel understand classification levels and protection requirements for each classification.

MaxMind only stores personal data for as long as is necessary for the purposes for which it is being processed. Retention is based on legal and regulatory requirements, contractual obligations, and business needs. Records are not kept longer than required unless there is a business reason or litigation hold. Electronic records are stored using SaaS cloud services, with access restricted to authorized personnel. No personal data is stored on local scanner machines or shared folders, and devices storing personal data are encrypted and patched. Paper Records utilization are kept to a minimum. The Protection of Records document lists retention periods and data retention procedures for various data types, including customer records, log records, backups, personnel records, payroll records, corporate records, accounting and finance, tax records, and legal and insurance records. The organization's online Data Protection Agreement (DPA) includes specific retention requirements and transfer descriptions.

Encryption keys are protected during generation, storage, and use, and only authorized systems and users can decrypt protected information. The Use of Cryptography Policy outlines MaxMind's secure approach to key management. MaxMind uses Google's Cloud Key Management Service to manage cryptographic keys and uses Google Secrets Management for its secret management.

Data is stored in Google Cloud Storage (GCS) buckets, databases, server disks, and internal systems, all hosted within Google Cloud Platform and encrypted both at rest and in transit. The Application Security Requirements Policy defines the controls that help ensure the confidentiality, integrity, and authenticity of data in transit. All of MaxMind's internet connectivity is encrypted via HTTPS using Transport Layer Security (TLS) v1.2 or higher. All public web endpoints are proxied through Cloudflare, which

enforces TLS policies and provides web application firewall protections. All internal data at rest—including backups in GCS buckets and server disk contents—is encrypted by default using Google Cloud Platform's (GCP) encryption by default. Additionally, all internal subnet network traffic is natively encrypted by default within the GCP VCP network.

The Secure Disposal or Re-Use of Equipment Policy governs the destruction of both hardcopy and electronic media. Paper media is shredded, and processes for the physical destruction of electronic media are defined based on whether the device's drive can be reused. Approved device decommissioning services are documented, and a certificate of destruction is provided. Approved sanitization methods for electronic media are outlined in accordance with operating system requirements. Leased or cloud-hosted equipment is disposed of in accordance with vendor procedures.

## Procedures

MaxMind has developed and communicated policies and procedures involved in the operation of the IP address intelligence and fraud detection services system. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to risk management, data backup, system and facility access, auditing, configuration management, incidents, disaster recovery, intrusion detection, vulnerability assessment, data integrity, vendor management, and so on. These procedures are developed in alignment with the overall information security policy and are reviewed, updated, and approved as necessary for changes in the business, but no less than once annually.

# Attachment B: Principal Service Commitments and System Requirements

MaxMind designs its processes and procedures related to the IP address intelligence and fraud detection services system to meet its business objectives. Such objectives are based on the service commitments that MaxMind makes to its customers, business partners, vendors, and subservice organizations and the operational and compliance requirements that MaxMind has established for the services. Service commitments are declarations made by management to its customers regarding the performance of the IP address intelligence and fraud detection services system.

## Contractual Commitments

Contracts are implemented with users of MaxMind services, addressing terms, granting of rights in accordance with licensing, usage restrictions, security and disclosure, data destruction, ownership and IP rights, data processing, fees, warranties and liability, indemnification, use of APIs, insurance coverage, and relevant contractual addendums. Where a potential customer requests confidential information from MaxMind, the organization requires them to sign a non-disclosure agreement (NDA) prior to providing such potential customer with confidential information.

## Regulatory Commitments

MaxMind provides services globally and is compliant with all local and federal regulations in the regions where it operates, as well as all other applicable industry regulations. MaxMind's privacy policy outlines how it complies with various privacy laws. In addition to privacy laws, the organization tracks other relevant regulatory and industry requirements. MaxMind works with internal corporate counsel, external privacy counsel, and an external Data Protection Officer (DPO) for guidance on compliance with relevant regulations applicable to MaxMind.