Proprietary & Confidential

Follow Up Boss System

SOC 3

Relevant to Security and Confidentiality

APRIL 1, 2024 TO SEPTEMBER 30, 2024

MOSSADAMS

Table of Contents

I. Independent Service Auditor’s Report

Zillow, Inc.
1301 2nd Ave, Floor 36
Seattle, WA 98101

To the Management of Zillow, Inc.:

Scope

We have examined Zillow, Inc.’s accompanying assertion in Section II titled “Zillow, Inc.’s Assertion" (assertion) that the controls within Zillow, Inc.’s Follow Up Boss System (system) were effective throughout the period April 1, 2024 to September 30, 2024, to provide reasonable assurance that Zillow, Inc.’s service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (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*.

Zillow, Inc. uses a subservice organization for system hosting (subservice organization). Zillow, Inc.’s description of the boundaries of its system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Zillow, Inc., to achieve Zillow, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Zillow, Inc.'s controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization’s Responsibilities

Zillow, Inc. 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 Zillow, Inc.’s service commitments and system requirements were achieved. Zillow, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Zillow, 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 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 AICPA. 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 Zillow, 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 Zillow, 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 Zillow, Inc.'s Follow Up Boss System were effective throughout the period April 1, 2024 to September 30, 2024, to provide reasonable assurance that Zillow, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Moss Adams LLP

Seattle, Washington
October 31, 2024

II. Zillow, Inc.’s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Zillow, Inc.’s Follow Up Boss System (system) throughout the period April 1, 2024 to September 30, 2024, to provide reasonable assurance that Zillow, Inc.’s service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (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 April 1, 2024 to September 30, 2024, to provide reasonable assurance that Zillow, Inc.’s service commitments and system requirements were achieved based on the trust services criteria. Zillow, 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.

Zillow, Inc. uses a subservice organization for system hosting (subservice organization). The description of the boundaries of our system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Zillow, Inc., to achieve Zillow, Inc.’s service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Zillow, Inc.’s controls. The description does not disclose the actual controls at the subservice organization.

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, 2024 to September 30, 2024, to provide reasonable assurance that Zillow, Inc.’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A - Zillow, Inc.'s Description of the Boundaries of Its Follow Up Boss System

A. System Overview

1. Services Provided

COMPANY BACKGROUND

Zillow, Inc. (Zillow) houses a portfolio of real estate and home-related brands on the web and mobile. The company's brands focus on the stages of the home lifecycle: renting, buying, selling, financing, and home improvement. Zillow is committed to empowering consumers with data, inspiration, and knowledge around homes, and connecting them with the right local professionals to help.

Follow Up Boss, LLC is a wholly owned subsidiary of Zillow, Inc. and is responsible for developing and maintaining the Follow Up Boss System. The system optimizes core sales activities for real estate agents and teams to help them manage their relationships with home shoppers, set more appointments, and close more deals with their leads, past clients, and sphere of influence.

SERVICES PROVIDED

The Follow Up Boss System makes it easy for real estate teams and operators to manage their clients, contacts, and relationships in a single platform, offering users tools to communicate directly with those contacts (email, phone, and text). Follow Up Boss is delivered as a web and mobile application; it automatically syncs with a customer's email and calendar system.

2. Infrastructure

Follow Up Boss System infrastructure is supported by cloud platform technologies, including application and database hosting, networking tools, and cloud storage.

3. Software

Follow Up Boss System is developed for web browsers, iOS and Android platforms. Follow Up Boss web browser application is delivered via a single-page application architecture that interfaces with Follow Up Boss application programming interfaces (APIs). iOS and Android applications are natively developed and interface with Follow Up Boss APIs.

4. People

The Zillow personnel supporting the Follow Up Boss System include the following:

- *Executive Management* – Responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives.
- *Human Resources (HR)* – Responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).

- *Corporate Legal, Risk Compliance, Security, Audit* – Responsible for risk management and identification at the Zillow entity level.
- *Corporate IT Personnel* – Responsible for risk management and identification, monitoring, and compliance of security issues and incidents at the Zillow entity level.
- *Zillow Group Security and Compliance Teams* – Responsible for security development, and compliance of security issues and incidents throughout the brand-specific infrastructure and audit and analysis of services provided.
- *Product* – Responsible for understanding customer needs, creating new features, and working with the internal team to bring them to market.
- *Development* – Responsible for designing and maintaining the Follow Up Boss product, including the web interface, the proprietary sync engine, infrastructure, and debugging tools.

5. Data

Follow Up Boss classifies its data to ensure appropriate security measures are implemented to protect the confidentiality, integrity, and availability of the data. The data collected from customers is subject to the Follow Up Boss Privacy Policy and Terms of Service.

Customer data is retained and deleted in line with Follow Up Boss' Privacy Policy and Terms of Service. Databases, data stores, and file systems are encrypted according to Follow Up Boss's Encryption Policy.

6. Processes and Procedures

ACCESS REQUESTS AND ACCESS REVOCATION

A service request is opened at the time of onboarding an employee or contractor and an internal user account is created. Once the account is created, based on their role, a new hire is provisioned access to applicable systems. Additional access, if required, is requested and tracked via a ticketing system and approval is received from a system owner. The ticket includes employee name and job title and role requested as required per job responsibility. Employees are provisioned access on a least-privilege basis.

Follow Up Boss's employees are supplied with company-provided computers to perform their duties. Company-provided devices are equipped with full-disk encryption and endpoint protection.

Access termination requests are tracked by the People Operations team and documented in the Human Resources Information System (HRIS). When an employee is terminated, access to systems is removed and company-owned devices are collected in accordance with the company's Asset Management Policy.

User access reviews, including privileged users, are performed on a quarterly basis to help ensure that access to data is restricted and authorized. Accounts identified as inappropriate are investigated and resolved.

COMPUTER OPERATIONS – BACKUPS

Customer data is backed up by Follow Up Boss to ensure continuation and continuity of service.

COMPUTER OPERATIONS – AVAILABILITY

Internally, the Follow Up Boss infrastructure team monitors the health of applications, including the Follow Up Boss web user interface (UI), databases, and cloud storage.

Monitoring occurs 24x7 and includes the availability and performance of the web UI, the throughput and queuing latency of the job scheduler, and any faults or errors encountered by users while configuring Follow Up Boss or while their data is being synced by Follow Up Boss.

Follow Up Boss employs vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues.

CHANGE CONTROL

Follow Up Boss maintains documented Software Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes through a process that is consistent and repeatable. This policy defines the high-level requirements for providing program and project stakeholders guidance to support the approval, planning, and life-cycle development for Follow Up Boss, including change requirements, test procedures and results, change approval, and release notification.

B. Complementary Subservice Organization Controls

Zillow's controls related to the Follow Up Boss System cover only a portion of overall internal control for each user entity of Zillow. It is not feasible for the criteria related to the Follow Up Boss System to be achieved solely by Zillow. Therefore, each user entity's internal controls must be evaluated in conjunction with Zillow's controls, taking into account the types of controls expected to be implemented by the subservice organizations as described below.

Complementary Subservice Organization Controls	
1	Physical access to data centers is approved by an authorized individual.
2	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
3	Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
4	Physical access points to server locations are recorded by closed-circuit television cameras (CCTV). Images are retained for 90 days unless limited by legal or contractual obligations.
5	Physical access points to server locations are managed by electronic access control devices.
6	Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

C. User Entity Responsibilities

There are no controls at the user entity that are necessary, in combination with Zillow's controls, to provide reasonable assurance that Zillow's service commitments and system requirements were achieved based on the applicable trust services criteria (complementary user entity controls).

There are, however, certain responsibilities that users of the system must fulfill for the user entity to derive the intended benefits of the services of the Follow Up Boss System. The user entity responsibilities presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities. User entities are responsible for their own control environments and their operational effectiveness.

User Entity Responsibilities	
1	Understanding and complying with their contractual obligations to Follow Up Boss.
2	Maintaining their own system(s) of record.
3	Ensuring the supervision, management, and control of the use of Follow Up Boss services by their personnel.
4	Notifying Follow Up Boss of changes made to technical or administrative contact information.
5	Immediately notifying Follow Up Boss of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
6	Developing their own disaster recovery and business continuity plans that address the inability to access or utilize Follow Up Boss services.

Attachment B – Principal Service Commitments and System Requirements

Zillow strives to meet specific service level commitments for general or broad-based agreements with customers or partners. Zillow maintains commercially reasonable administrative and technical safeguards for the protection and integrity of the application products and customer data within the services system for the Follow Up Boss System.

Security and confidentiality commitments to user entities are documented and communicated in the Terms of Service, Privacy Policy, and any Service Level Agreements (SLAs) or other customer agreements, as well as in the description of the service offering provided online.

MOSSADAMS