Report on Higlobe, Inc.’s Higlobe WebApp Relevant to Security Throughout the Period January 1, 2023 to March 31, 2023

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

Table of Contents

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: Higlobe, Inc. ("Higlobe")

Scope

We have examined Higlobe's accompanying assertion titled "Assertion of Higlobe, Inc. Management" (assertion) that the controls within the Higlobe WebApp (system) were effective throughout the period January 1, 2023 to March 31, 2023, to provide reasonable assurance that Higlobe's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* (2017 TSC).

Higlobe uses subservice organizations to provide Infrastructure as a Service (IaaS) and ancillary security operations services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Higlobe, to achieve Higlobe's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Higlobe's controls. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Higlobe 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 Higlobe's service commitments and system requirements were achieved. Higlobe has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Higlobe is responsible for selecting, and identifying in its assertion, the applicable trust service 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 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 Higlobe'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 Higlobe'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 the Higlobe WebApp were effective throughout the period January 1, 2023 to March 31, 2023, to provide reasonable assurance that Higlobe's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Higlobe's controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Greenwood Village, Colorado
May 10, 2023

Section 2

Assertion of Higlobe, Inc. Management

Higlobe, Inc.
228 Hamilton Ave
3rd Floor
Palo Alto CA 94301-2583
United States

Higlobe.com

Assertion of Higlobe, Inc. ("Higlobe") Management

We are responsible for designing, implementing, operating and maintaining effective controls within the Higlobe WebApp (system) throughout the period January 1, 2023 to March 31, 2023, to provide reasonable assurance that Higlobe's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* (2017 TSC). Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

Higlobe uses subservice organizations for Infrastructure as a Service (IaaS) and ancillary security operations services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Higlobe, to achieve Higlobe's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Higlobe's controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2023 to March 31, 2023, to provide reasonable assurance that Higlobe's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Higlobe's controls operated effectively throughout that period. Higlobe'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.

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 January 1, 2023 to March 31, 2023, to provide reasonable assurance that Higlobe's service commitments and system requirements were achieved based on the applicable trust services criteria.

Higlobe, Inc.

Attachment A

Higlobe, Inc.’s Description of the Boundaries of Its Higlobe WebApp

Type of Services Provided

Higlobe, Inc. (“the Company”) is a United States (U.S.) payment services company that serves non-U.S. professionals and companies with U.S. business clients. Currently serving clients in Mexico and Brazil, the Company helps independent workers, contractors, and businesses get paid for work performed for U.S. companies through the Higlobe WebApp. The Company uses stablecoins issued by companies that are regulated and supervised by U.S. federal or state agencies and that are 1:1 backed by U.S. dollars or U.S. government treasury securities.

The boundaries of the system in this section details the Higlobe WebApp. Any other Company services are not within the scope of this report.

The Boundaries of the System Used to Provide the Services

The boundaries of the Higlobe WebApp are the specific aspects of the Company’s infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Higlobe WebApp.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

The Company utilizes Infrastructure as a Service (IaaS) to host infrastructure resources in support of the Higlobe WebApp. The Company leverages the experience and resources of IaaS providers to scale quickly and securely as necessary to meet current and future demand.

The Company also utilizes a digital asset security platform, to help protect digital assets by securing private keys and application programming interface (API) credentials and eliminating the need for deposit addresses. Additionally, the Company hosts software on a virtual machine to sign transactions using multi-party computation (MPC) technology.

The Company is responsible for designing and configuring the Higlobe WebApp architecture as it pertains to IaaS to ensure that security and resiliency requirements are met.

The in-scope hosted infrastructure also consists of multiple supporting tools, as shown in the table below:

Infrastructure	
Infrastructure Component	**Business Function**
Virtual WorkSpaces	OTP server
	Virtual workspaces
Development Platform	Code pipeline runner
	Code repository

Infrastructure	
Infrastructure Component	**Business Function**
Firewalls	Border firewalls
	Firewall management
Security Operations console	Intrusion detection
	Vulnerability scanning
Admin console	Application administration
User Application	Account management
	Multi-party computation (MPC)
	Flow of funds
	Ledger
	WebApp

Software

Software consists of the programs and software that support the Higlobe WebApp (operating systems [OSs], middleware, and utilities). The software used to build, support, secure, maintain, and monitor the Higlobe WebApp supports the following business functions, as listed below:

- Threat detection service
- Credential and secret management
- Relational database
- Data caching service
- Documentation storage
- Workload orchestrator
- User application protection
- Multi-party computation (MPC)
- Antivirus
- Application and infrastructure monitoring
- Code repository
- Firewall, intrusion detection and prevention
- Security information and event management (SIEM)
- Vulnerability scanning
- Admin console
- Configuration management

People

The Company develops, manages, and secures the Higlobe WebApp via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Business Development	Responsible for identifying and taking advantage of growth opportunities and partnerships by looking at emerging market trends and proposing opportunities for growth and expanded market reach.
Compliance	Responsible for the development and operational execution of policies and procedures related to statutory, regulatory, and contractual obligations.
Creative	Responsible for the design and execution of campaigns that encourage a target audience to buy the Company's products and services. The team is also responsible for creating a consistent brand image for the Company through its look, voice, and messaging.
Customer Success	Responsible for providing support to all customers, including handling inbound customer tickets, answering product questions, and escalating bug reports and data loss issues.
Engineering	Responsible for the development, testing, deployment, and maintenance of new code for the Higlobe WebApp.
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.
Finance	Responsible for obtaining and handling any monies on behalf of the organization. The department controls the income and expenditure in addition to ensuring the business runs effectively with minimum disruptions.
Information Security	Responsible for managing access controls and the security of the production environment.
Legal	Responsible for making sure that services are performed consistently with applicable legal and regulatory requirements.
Marketing	Responsible for handling internal and external communications about the Company, such as new features or product releases and noteworthy business or regulatory developments.
People	Responsible for onboarding new personnel, defining the roles and positions of new hires, performing background checks, and facilitating the employee termination process.
Product Management	Responsible for overseeing the product life cycle, including adding new product functionality.

Procedures

Automated and manual procedures involved in the operation of the Higlobe WebApp are documented. Procedures are established by the respective teams for a variety of processes, including but not limited to those relating to engineering and information security. These procedures are drafted in alignment with the overall information security policies and are periodically updated and approved as necessary for changes in the business.

The following table details the procedures as they relate to the operation of the Higlobe WebApp:

Procedures	
Procedure	**Procedure**
Logical Access	How the Company restricts logical access, provides and removes that access, and prevents unauthorized access.
System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical security deviations.
Incident Management	How the Company establishes and maintains a capability to respond to cybersecurity incidents.
Risk Management	How the Company consistently identifies, assesses, categorizes, and remediates risks.
Secure Baseline Configurations	How the Company defines hardening standards and requirements.
Software Development Life Cycle (SDLC) and Software Change Control	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Third-Party Security Management	How the Company minimizes security risks associated with third parties.
Vulnerability and Patch Management	How the Company utilizes a risk-based approach to vulnerability and patch management practices to minimize the attack surface of systems, applications, and services.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Using the Higlobe WebApp, the customer or end user defines and controls the data they load into and store in the Higlobe production network. Once stored in the environment, the data is accessed remotely from customer systems via the WebApp graphical user interface.

Customer data is managed, processed, and stored in accordance with relevant data protection laws and regulations.

The Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Encryption is enabled for databases housing sensitive customer data.

The following table details the types of data contained in the production application for the Higlobe WebApp:

Data	
Production Application	**Description**
WebApp	The Company may store functional, analytics, technical, and marketing-related cookies in accordance with the Higlobe Cookie Policy to better understand user behavior.
Log and alert infrastructure	The Company logs information about customers, including Internet Protocol (IP) address, which may be used to assist in detecting security violations, performance problems, and flaws in applications.
Account management	The Company stores user account information data and statuses. This information may be used to keep track of the user actions inside the WebApp.
Ledger	The Company stores user transaction data and statuses. This information may be used to keep track of the user fund movements inside the WebApp.
Flow of funds	The Company stores data pertaining to the tracking of internal movement of funds including but not limited to customer transaction data and the state of the internal movement of funds.

User Entity Responsibilities

Management of user entities is responsible for the following, which should not be regarded as a comprehensive list of all controls that should be employed by user entities.

- User entities should have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames.
- Controls to provide reasonable assurance that the Company is notified of changes in:
  - User entity vendor security requirements
  - The authorized users list
- It is the responsibility of the user entity to have policies and procedures to:
  - Inform their employees and users that their information or data is being used and stored by the Company.
  - Determine how to file inquiries, complaints, and disputes to be passed on to the Company.
- User entities should only grant access to the Company's system to authorized and trained personnel.
- Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company.
- User entities should deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company uses subservice organizations for Infrastructure as a Service (IaaS). The Company also uses a subservice organization for ancillary security operations services. The Company's controls related to the Higlobe WebApp cover only a portion of the overall internal control for each user entity of the Higlobe WebApp.

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. CSOCs are expected to be in place at subservice organizations for IaaS related to physical security and environmental protection. CSOCs are expected to be in place at subservice organizations for ancillary security operations related to monitoring alerts and escalation of anomalies to Higlobe management.

The Company management receives and reviews subservice organizations' SOC 2 reports annually. In addition, through its operational activities, Company management monitors the services performed by the subservice organizations to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organizations to monitor compliance with the service agreements, stay informed of changes planned at the hosting facilities, and relay any issues or concerns to the subservice organization's management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the Higlobe WebApp to be achieved solely by the Company. The CSOCs that are expected to be implemented at the subservice organizations are described below.

Criteria	Complementary Subservice Organization Controls
CC6.1	• IaaS providers are responsible for encrypting databases in their control.
CC6.4	• IaaS providers are responsible for restricting data center access to authorized personnel. • IaaS providers are responsible for the 24x7 monitoring of data centers by closed circuit cameras and security personnel.
CC6.5 CC6.7	• IaaS providers are responsible for securely decommissioning and physically destroying production assets in their control.
CC7.2	• IaaS providers are responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers. • IaaS providers are responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • IaaS providers are responsible for overseeing the regular maintenance of environmental protections at data centers.
CC7.3	• Ancillary security operations service provider is responsible for monitoring alerts related to network traffic and security logs and notifying Higlobe of any potential security events.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the Higlobe WebApp. Commitments are communicated in the Company's privacy policy.

System requirements are specifications regarding how the Higlobe WebApp should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to the Higlobe WebApp include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• Higlobe will implement reasonable security measures to prevent data from unauthorized or accidental access, destruction, loss, theft, alteration, communication, or use. • Higlobe will encrypt customer data stored by the Company and entered on Hypertext Markup Language (HTML) pages using Transport Layer Security (TLS). • Higlobe will notify customers and any applicable authority about any suspected or actual data breach, including the following: – The nature of the incident – The data compromised – Recommendations about the measures to adopt to protect customer interests – The corrective actions taken – The means by which further information may be obtained regarding the data breach	Standards pertaining to: • Security & Privacy Governance • Asset Management • Capacity & Performance Planning • Change Management • Compliance • Continuous Monitoring • Configuration Management • Cryptographic Protections • Data Classification & Handling • Human Resources Security • Identification & Authentication • Incident Response • Network Security • Risk Management • Secure Engineering & Architecture • Security Operations • Security Awareness & Training • Technology Development & Acquisition • Third-party Vendor Management • Threat Management • Vulnerability & Patch Management • Web Security