payouts.com

SOC 2 Type II Report

For the Period of October 1, 2024 to September 30, 2025

REPORT ON CONTROLS PLACED IN OPERATION AT
PAYOUTS TECHNOLOGIES L.B.O. LTD.
RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY
WITH THE INDEPENDENT SERVICE AUDITOR'S REPORT
INCLUDING TEST PERFORMED AND RESULTS THEREOF

Table of Contents

payouts.com

Section I – Payouts Technologies Ltd.’s Management Assertion

March 25, 2026

We have prepared the accompanying description titled "Description of the Payouts Platform relevant to security, availability and confidentiality throughout the period October 01, 2024 to September 30, 2025" (Description) of Payouts Technologies Ltd. (Service Organization) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (Description Criteria). The Description is intended to provide report users with information about the Payouts Platform (System) that may be useful when assessing the risks arising from interactions with the System , particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its 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, in AICPA Trust Services Criteria*.

Carved-out Unaffiliated Subservice Organization: Payouts Technologies Ltd. uses Amazon Web Services (AWS) to provide infrastructure management services. The Description indicates that complementary controls at Amazon Web Services (AWS) that are suitably designed and operating effectively are necessary, along with controls at PAYOUTS TECHNOLOGIES LTD. to achieve Payouts Technologies Ltd.'s service commitments and system requirements, based on the applicable trust services criteria. The Description presents Payouts Technologies Ltd.'s controls and the types of complementary subservice organization controls assumed in the design of Payouts Technologies Ltd.'s controls. The Description does not disclose the actual controls at the carved-out Amazon Web Services (AWS).

Complementary user entity controls: The Description also indicates complementary user entity controls that are suitably designed and operating effectively are necessary along with Payouts Technologies Ltd.'s controls to achieve the service commitments and system requirements. The Description presents Payouts Technologies Ltd.'s controls and the complementary user entity controls assumed in the design of Payouts Technologies Ltd.'s controls.
We confirm, to the best of our knowledge and belief, that:

a. The Description presents the System that was designed and implemented throughout the period October 01, 2024, to September 30,2025,5 in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed throughout the period October 01, 2024 to September 30, 2025 to provide reasonable assurance that Payouts Technologies Ltd.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if user entities applied the complementary user entity controls and the carved-out subservice organization applied the complementary controls assumed in the design of Payouts Technologies Ltd.'s controls throughout that period.

c. The Payouts Technologies Ltd. controls stated in the Description operated effectively throughout the period October 01, 2024 to September 30, 2025 to provide reasonable assurance that Payouts Technologies Ltd.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary user entity controls and the complementary carved-out subservice organization controls assumed in the design of Payouts Technologies Ltd.'s controls operated effectively throughout that period.

Signature Leor Ceder
Title Leor Ceder, CEO

Shape the future with confidence

Kost Forer Gabbay & Kasierer
144 Menachem Begin Road, Building A
Tel-Aviv 6492102, Israel

Tel: +972-3-6232525
Fax: +972-3-5622555
ey.com

Section II – Independent service auditor's report

To the Management of Payouts Technologies Ltd.

Scope

We have examined Payouts Technologies Ltd. 's accompanying description titled "Description of the Payouts Platform relevant to security, availability and confidentiality throughout the period October 01, 2024 to September 30, 2025" (Description) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report*, (Description Criteria) and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period October 01, 2024 to September 30, 2025 to provide reasonable assurance that the 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,* in AICPA Trust Services Criteria.

Carved-out Unaffiliated Subservice Organization: Payouts Technologies Ltd. uses Amazon Web Services (AWS) (subservice organization) to provide infrastructure management services. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Payouts Technologies Ltd., to provide reasonable assurance that Payouts Technologies Ltd.'s service commitments and system requirements are achieved based on the applicable trust services criteria. The description presents Payouts Technologies Ltd.'s system; its controls relevant to the applicable trust services criteria; and the types of complementary subservice organization controls that the service organization assumes have been implemented, suitably designed, and are operating effectively at Amazon Web Services (AWS). The Description does not disclose the actual controls at Amazon Web Services (AWS). Our examination did not include the services provided by Amazon Web Services (AWS) and we have not evaluated whether the controls management assumes have been implemented at Amazon Web Services (AWS) have been implemented or whether such controls were suitably designed and operated effectively throughout the period October 01, 2024, to September 30, 2025.

Complementary user entity controls: The Description indicates that Payouts Technologies Ltd.'s controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Payouts Technologies Ltd.'s controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Payouts Technologies Ltd.s' ***responsibilities***

Payouts Technologies Ltd. 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 its service commitments and system requirements were achieved. Payouts Technologies Ltd. has provided the accompanying assertion titled, Payouts Technologies Ltd.'s Management Assertion (Assertion) about the presentation of the Description based on the Description Criteria and the suitability of design and operating effectiveness of controls stated therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria. Payouts Technologies Ltd. is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) selecting the trust services categories addressed by the engagement and stating the applicable trust services criteria and related controls in the Description; (5) identifying the risks that threaten the achievement of the service organization's service commitments and system requirements; and (6) designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve its service commitments and system requirements.

Shape the future with confidence

Service auditor's responsibilities

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of design and operating effectiveness of controls stated therein to achieve the service organization's service commitments and system requirements based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants ("AICPA"). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria throughout the period October 01, 2024 to September 30, 2025. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the Description is not presented in accordance with the Description Criteria and that controls were not suitably designed or operating effectively based on the applicable trust services criteria.
- performing procedures to obtain evidence about whether the Description is presented in accordance with the Description Criteria.
- performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- testing the operating effectiveness of those controls to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.
- evaluating the overall presentation of the Description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Our examination was not conducted for the purpose of evaluating the performance or integrity of Payouts Technologies Ltd.'s AI services. Accordingly, we do not express an opinion or any other form of assurance on the performance or integrity of Payouts Technologies Ltd.'s AI services.

We are required to be independent of Payouts Technologies Ltd. and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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 at a service organization may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any

Shape the future with confidence

evaluation of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the service commitments and system requirements based on the applicable trust services criteria, is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Description of tests of controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in the accompanying Description of Criteria, Controls, Tests, and Results of Tests (Description of Tests and Results).

Opinion

In our opinion, in all material respects:

a. the Description presents the Payouts Platform system that was designed and implemented throughout the period October 01, 2024, to September 30, 2025, in accordance with the Description Criteria.
b. the controls stated in the Description were suitably designed throughout the period October 01, 2024 to September 30, 2025, to provide reasonable assurance that Payouts Technologies Ltd.'s service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Payouts Technologies Ltd.'s controls throughout that period.
c. the controls stated in the Description operated effectively throughout the period October 01, 2024 to September 30, 2025 to provide reasonable assurance that Payouts Technologies Ltd. service commitments and system requirements were achieved based on the applicable trust services criteria if the complementary subservice organization and user entity controls assumed in the design of Payouts Technologies Ltd.'s controls operated effectively throughout that period.

Restricted use

This report , including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Payouts Technologies Ltd., user entities of Payouts Technologies Ltd.'s Payouts Platform system during some or all of the period October 01, 2024 to September 30, 2025 and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- the nature of the service provided by the service organization
- how the service organization's system interacts with user entities, subservice organizations, or other parties
- internal control and its limitations
- complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- user entity responsibilities and how they interact with related controls at the service organization
- the applicable trust services criteria
- the risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Kost Forer Gabbay and Kasierer
A member firm of Ernst & Young Global Limited

Kost Forer Gabbay and Kasierer

March 25, 2026
Tel-Aviv, Israel

Section III – Description of the Payouts.com Platform relevant to Security, Availability and Confidentiality for the period October 1, 2024, to September 30, 2025

Company Overview and Background

Payouts Technologies L.B.O. Ltd., headquartered at 10 Hasadanot St. Hertzeliya, Israel, is specializing in automated payout solutions specifically engineered for the dynamic marketing industry. Payouts's mission is to streamline and enhance financial operations through automation, simplifying the payout process for marketing vendors and addressing the intricate financial challenges inherent in the marketing sector. Leveraging a comprehensive global operational network, Payouts delivers not only seamless integration with clients' existing systems—ensuring real-time data flow and financial accuracy—but also offers advanced payment services tailored to the needs of the industry.

Purpose and scope of the report

The scope of this report is limited to the controls supporting Payouts.com Platform and does not extend to other available Payouts products and services or the controls at third-party service providers.

Types of Services Provided

Payouts Technologies L.B.O. Ltd. offers the "Payouts.com Platform," an advanced Finance Operations solution aimed at streamlining marketing and financial operations. This platform is the primary service and the subject of the SOC 2 report.

Payouts.com Platform is designed to consolidate all the financial operations of a marketing team into a single, unified system. This includes budget management, vendor payments, cash flow projections, real-time financing, and more. Additionally, the platform also includes advanced banking capabilities.

One of the features is the advanced payment feature, which is facilitated by real-time data accessible through 600 connectors, allowing marketers to scale their operations without cash flow disruptions. Payouts's MVP with strategic partners such as Fiverr is an integral part of this service.

The scope of SOC 2 report covers all these services provided by the Payouts.com Platform, adhering to the principles of security, availability and confidentiality.

The core features and services of the Payouts Payouts.com Platform, which are all included in SOC 2 report, are as follows:

Marketing Dashboard - provides a consolidated and comprehensive view of all marketing data, segmented by teams like Affiliation, PPC, Social, etc. It allows customers to understand their marketing activities and spend time in real-time.

Payment Automation: The platform automates payments to all marketing vendors, including larger ones like Google and Facebook, and smaller affiliates. This streamlines cash flow and ensures consistent monthly payments.

Budget Management: The platform provides a dedicated tool for marketing teams, allowing both Finance and Marketing departments to maintain control over the budget. It includes alerts for potential overspending per team or source.

Advanced Payment Feature: The feature, facilitated by real-time data accessible through 600 connectors, allows affiliates to receive instant financing, enabling them to increase traffic without the constraint of Net 45/60 payment terms.

Banking Capabilities: Payouts' s platform offers global accounts in 15 countries and 130 currencies, the ability to issue cards per employee or company purpose and acquiring services.

Data Integration and Management: With 600 connectors, payouts.com platform integrates with various data sources, providing valuable insights and enabling data-driven decision making.

Cash Flow Projections: The platform provides projections of the company's cash flow based on current marketing spend and budget, enabling better financial planning.

All these features are designed to work in a seamless, integrated manner, providing an all-in-one FinOps solution for customers' marketing needs.

Principal Service Commitments and System Requirements

Service commitments are declarations made by management to customers regarding the performance of the Platform. Commitments are communicated in Subscription and Services Agreements, Data Protection Agreements and the Terms of Service and Privacy Policy that are made available to customers, prospects and business partners on the Company's website.

System requirements are specifications regarding how the Platform should function to meet the Company's principal commitments to user entities. System requirements are specified in Payouts's policies and procedures, which are available to all employees.

The Components of the System Used to Provide the Services

Payouts Technologies Ltd.. designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Payouts Technologies Ltd. makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Payouts Technologies Ltd.. has established for the services. The system services are subject to the Security commitments established internally for its services.
At Payouts, we are dedicated to maintaining clear, open, and consistent communication with customers. We communicate system and service commitments to customers in the following ways:

User Agreement and Policies: When a customer signs up for the platform, they are provided with a user agreement and Payouts' s policies which clearly outline the services customers will receive, company's commitments to them, and their responsibilities as a user.

Onboarding and Training: During the customer onboarding process, Payouts conduct training sessions which detail the use of the platform and commitments regarding each feature and service. The company also address any queries or concerns they might have about services.

Regular Updates and Notifications: Payouts continuously keep customers informed about any changes or updates to the system or services through emails, in-app notifications, and newsletters. This includes updates on new features, maintenance schedules, and system improvements.

Customer Support: Payouts' s dedicated customer support team is available to assist with any questions or issues regarding the system or services. Customer support team provides timely, clear, and accurate information to customers to ensure their satisfaction and success with the platform.

Website and Marketing Material: Detailed information about the system, services, and commitments to users are also communicated through the website and marketing material. Payouts makes sure that all the information is accurate and

up to date to provide a clear understanding of what customers can expect. By consistently communicating system and service commitments, Payouts aims to build trust with customers and provide them with a reliable, high-quality service.

Boundaries of the system

The boundaries of the primary offering of Payouts Technologies L.B.O. Ltd. are a Finance Operations Platform, a comprehensive solution that aligns marketing and financial operations. This platform is the focal point of customer interaction and the core of product suite. Designed with an emphasis on efficiency and transparency, it incorporates different functionalities such as real-time budget management, streamlined payments to vendors, cash flow forecasting, and instant financing. These features are tailored to facilitate smooth financial operations for marketing teams. The Finance Operations Platform adheres strictly to SOC 2 standards, demonstrating commitment to data security and integrity. This platform is the cornerstone of Payouts services and the embodiment of the mission to revolutionize financial operations within the marketing realm.

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

Security commitments

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system
- Regular vulnerability scans over the system and network, and penetration tests over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Up-time availability of production systems

Components of the system

The System description is comprised of the following components:

- Software - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- People - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- Data – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- Procedures – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

Infrastructure

Payouts Technologies Ltd.. maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents are the name, inventory type, description and owner. To outline the topology of its network, the organization maintains the following network diagram(s).

Hardware	Type	
AWS Elastic Compute Cloud (EC2)	AWS	Running application and infrastructure workloads
AWS Elastic Load Balancers	AWS	Load balance internal and external traffic
Virtual Private Cloud	AWS	Protects the network perimeter and restricts inbound and outbound access
S3 Buckets	AWS	Storage, upload and download

Software: Payouts Technologies L.B.O. Ltd is responsible for managing the development and operation of the primary offering of Payouts Technologies L.B.O. Ltd. is advanced Finance Operations Platform, a comprehensive solution that aligns marketing and financial operations. The platform is the focal point of customer interaction and the core of product suite. Designed with an emphasis on efficiency and transparency, it incorporates sophisticated functionalities such as real-time budget management, streamlined payments to vendors, cash flow forecasting, and instant financing. These features are specifically tailored to facilitate smooth financial operations for marketing teams. The Payouts.com Platform adheres strictly to SOC 2 standards, demonstrating Payouts commitment to data security and integrity. The platform is the cornerstone of services and the embodiment of Payouts' s mission to revolutionize financial operations within the marketing realm. system including infrastructure components such as servers, databases, and storage systems. The in-scope Payouts Technologies Ltd.. infrastructure and software components are shown in the table provided below:

System/Application	Operating System	Purpose
GuardDuty	AWS	Security application used for automated intrusion detection (IDS)
Amazon Web Services	AWS	Cloud provider user to host k8s cluster, LBs, build machines, etc.
GitHub	GitHub	Storing source code and code history, build pipelines
Google Workspace	Google Workspace	Used for emails communication
Vanta	Vanta	The organization compliance and security monitoring platform

Human Resources and Recruiting: The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

Payouts Technologies Ltd. has a staff of approximately 1 organized in the following functional areas:

Management: Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.
This includes:

- CEO
- CFO
- CTO
- CRO

Operations: Responsible for maintaining the availability of production infrastructure and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment.

Members of the Operations team may also be members of the Engineering team.

Information Technology: Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.

Product Development: Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

Data: Data as defined by Payouts Technologies Ltd., constitutes the following:

User and account data - includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilized by the company in delivering its services.

All employees and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Payouts Technologies Ltd. has policies and procedures in place to proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

Control Environment

Integrity and Ethical Values - The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Payouts Technologies Ltd. 's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Payouts Technologies Ltd. 's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees to sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Board of Directors - The Board of Directors is composed of 3 members, which includes 1 director that is independent of management, who serves on behalf of the investors and provides organizational oversight to the Company. The role of the Board of Directors is to establish short-term and long-term strategic goals and objectives for the Company, as outlined

in the Board of Directors' Charter, and is ultimately responsible for corporate governance. The Board of Directors holds annual meetings to review operating results, discuss business initiatives and oversee corporate governance and risks.

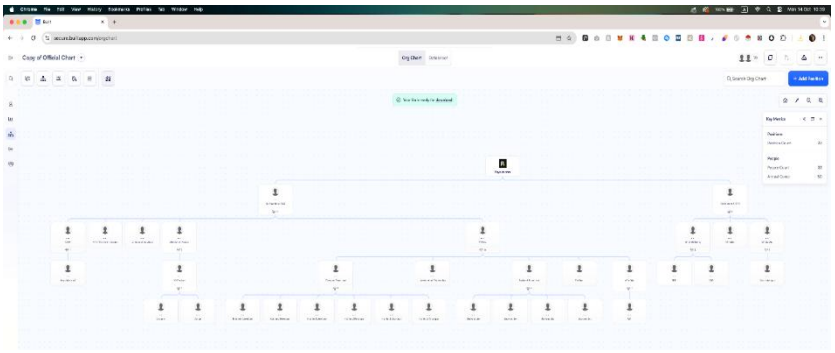
Organizational Structure

Payouts Technologies Ltd. 's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Payouts Technologies Ltd. 's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.



Commitment to competence - Payouts Technologies Ltd. 's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style - The Payouts Technologies Ltd. management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly sensitive data and workflows customers entrust to us.

Authority and Responsibility - The management team meets frequently to be briefed on technology changes that impact the way Payouts Technologies Ltd.. can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Payouts Technologies Ltd.. to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with Payouts's core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

Human Resources Policy and Practices - Payouts Technologies Ltd. 's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensure the service organization is operating at maximum efficiency. Payouts Technologies Ltd. 's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgment forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

Control Activities

Payouts's control activities are defined through its established policies and procedures. Policies are dictated through management of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control

- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

Risk Assessment

Risk identification: Payouts Technologies Ltd..'s risk assessment process identifies and manages risks that could potentially affect Payouts Technologies Ltd..'s ability to provide reliable and secure services to customers. As part of this process Payouts Technologies Ltd. maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Payouts Technologies Ltd.. product development process so they can be dealt with predictably and iteratively.

***Risk assessment*:** The environment in which the system operates; the commitments, agreements, and responsibilities of Payouts Technologies Ltd..'s system; as well as the nature of the components of the system result in risks that the criteria will not be met. Payouts Technologies Ltd.. addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Payouts Technologies Ltd..'s management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Risk Mitigation: Management identifies and assesses changes that could significantly impact on the system of internal control. The risk identification process considers changes to the regulatory, economic, and physical environment in which the Company operates. The Company considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations, rapid growth, and new technologies on the system of internal control. Identified risks are analyzed through a process that includes estimating the potential significance of the risk. Payouts' s risk assessment process includes considering how the risk should be managed and whether to accept, avoid, mitigate, or share the risk. Management determines mitigation strategies for the risks that have been identified and designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy. Security risks related to external parties (such as contractors and vendors) are identified and addressed based on the Company's vendor review process.

Payouts considers the inherent risk of working with vendors and business partners as part of the annual risk assessment performed by the engineering team. Internal and external cyber threats and vulnerabilities are identified and assessed based on the likelihood that they could prevent the Company from achieving its objectives. Consideration is given to cyber threats and the vulnerabilities such relationships may present and whether the Company's controls reduce such risks to a level consistent with objectives and risk acceptance.

Communication and Information

Information and communication are an integral component of Payouts Technologies L.B.O. Ltd.'s internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

Payouts Technologies Ltd.. uses several information and communication channels internally to share information with management, employees, contractors, and customers. Payouts Technologies L.B.O. Ltd uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, Payouts Technologies Ltd.. uses in-person and video “all hands” meetings to communicate company priorities and goals from management to all employees.

Monitoring

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Payouts Technologies Ltd..’s management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-going monitoring

Payouts Technologies Ltd..’s management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management’s close involvement in Payouts Technologies Ltd.. ’s operations help to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision to address any control’s weakness is made based on whether the incident was isolated or requires a change in the company’s procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Payouts Technologies Ltd..’s personnel.

Reporting deficiencies

Payouts’s internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

- Changes to the system (Type 1) - No significant changes have occurred.
- Changes to the system (Type 2) - No significant changes have occurred.
- Incidents (Type 1) - No Incidents, not live yet.
- Incidents (Type 2) - No Incidents, not live yet.

Logical and Physical Access

A security policy is documented by Payouts management, reviewed and approved on an annual basis by the management team. The security policy is available to Payouts employees and reviewed annually within the compliance management platform, versioned documentation platform, and shared folders.

Access Control, User and Permissions Management

The System Access Control Policy establishes the access control requirements for requesting and provisioning user access to the system. The policy requires that access be denied by default, follow a least privilege principle, and be granted only upon business need. Each user account is unique and is identifiable to an individual user. Segregation of duties is established for critical functions within the environment to minimize the risk of unauthorized changes to production systems.

Payouts Technologies Ltd. employs a structured access provisioning process to ensure secure and appropriate access to its systems. Domain account management requests are routed to designated asset owners or associated employees for

approval, following established provisioning and de-provisioning procedures. Access is managed through individual user accounts added to domain security groups, with explicit approval required from security group owners for any access requests. Payouts Technologies Ltd.. provides employees and contractors access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and reportable user provisioning and deprovisioning processes. Access to these systems is split into admin roles, user roles, and no access roles. User access and roles are reviewed on an annual basis to ensure least privileged access. Management is responsible for providing access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Payouts Technologies Ltd., completing security training. These steps must be completed within 14 days of hire.

Recertification of Access Permissions

Periodic reviews have been implemented to manage the appropriateness of access granted to information systems. Manual periodic reviews of individual accounts and security group memberships on assets are performed by authorized individuals, as appropriate, to evaluate whether access is still required. Remediation action is taken, as necessary, based on the review.

Policies and standards have been established and implemented to enforce appropriate user account password length and complexity. Personnel are required to follow the password standards established in the Information Security Program for all domains, as well as local user accounts for all assets.

Revocation Process

Employee status data is used to facilitate the provisioning and removal of user accounts in the System. Account management processes prevent the creation of an account for individuals that do not have valid HR records. Select users can request the removal of user accounts from the System. In addition, system owners can directly remove users from security groups. Upon termination, employees are required to return their keys and devices to Payouts. When an employee is terminated, management is responsible for deprovisioning access to all in scope systems within 3 days for that employee's termination.

Production Environment Logical Access

Access to the production environment is controlled through a designated set of access points and restricted to authorized individuals. Users are authenticated to access points using domain credentials depending on where the production assets are located. Passwords, along with two factor authentication used to access network devices, are restricted to authorized individuals and system processes based on job responsibilities.

Information System's Inventory

The Company maintains an inventory of information systems. All such assets are assigned ownership by a designated department or team within Payouts Technologies Ltd.. and prioritized based on the asset's business value and criticality to the Company. The classification process is owned by the engineering team. Information and data assets are subject to the Data Management Policy that defines parameters for the ownership, classification, security, storage, and retention of data. Software and hardware assets are subject to the Asset Management Policy and Third-Party Management Policy that defines parameters for the acquisition, development, maintenance, security, and disposal of information system assets.

Physical security

Payouts Technologies Ltd..'s production servers are maintained by AWS. Physical and environmental security protection are the responsibility of AWS. Payouts Technologies Ltd.. reviews the attestation reports and performs a risk analysis of AWS on at least an annual basis.

Software Development Lifecycle (SDLC) Overview

Payouts Technologies Ltd.. maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Production Monitoring

At Payouts, a comprehensive vulnerability management process is in place to ensure the security and reliability of systems. Vulnerability process is divided into next steps:

Regular Vulnerability Scans: Payouts conducts automated vulnerability scans of systems on a weekly basis. These scans help to identify potential security weaknesses in networks, applications, and systems.

External Assessments: In addition to internal scans, we also engage third-party cybersecurity firms to conduct an annual penetration test. This independent assessment provides an unbiased review of security posture and helps uncover potential vulnerabilities that could be missed in internal scans.

Patch Management: After vulnerabilities are identified, they are prioritized based on the risk they pose. Critical vulnerabilities are patched immediately, while other less severe vulnerabilities are scheduled for patching in accordance with their risk level. All patches are tested in a controlled environment before deployment to ensure they do not disrupt services.

Security Incident and Event Management (SIEM): Payouts utilizes SIEM tools to monitor and analyze activity across the network in real-time. This helps in the early detection of potential security incidents and suspicious activities.

Threat Intelligence: Payouts subscribe to industry-leading threat intelligence feeds to stay informed about the latest vulnerabilities and threats in the cybersecurity landscape. This information is used to enhance security measures and preemptively protect against emerging threats.

This rigorous approach ensures that we identify and address vulnerabilities in a timely and efficient manner, thereby reducing the risk of security incidents.

Security Incident Management

Payouts Technologies Ltd.. maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting and acting upon breaches or other incidents.

Payouts Technologies Ltd.. internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

Payouts Technologies Ltd.. utilizes 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.

Availability

Database Backup

Backup infrastructure is maintained in AWS with physical access restricted according to the policies. Backups are fully backed up daily, encrypted, with access restricted to key personnel. The backup system automatically generates a backup log. In case of failure, a notification is sent to the Engineering team. Replicas are used to achieve high availability in case of a disaster.

Amazon RDS instance is configured with automatic daily snapshots to ensure the availability and durability of Payouts' s data. These snapshots are taken automatically and can be used to restore database to a specific point in time. Additionally, RDS instance is deployed in a multi-AZ configuration for high availability. This means that database is replicated synchronously across multiple AZs within the same AWS Region. In the event of a hardware failure or AZ outage, RDS instance can failover to a standby instance in another AZ, minimizing downtime and ensuring continuous availability of the database.

Business Continuity Plan (BCP)

Payouts Technologies Ltd.. maintains a Business Continuity and Disaster Recovery (BC/DR) Plan designed to support the continuity of critical business functions and minimize downtime in the event of a disruption. The plan outlines procedures for maintaining operations during incidents and restoring services in a timely manner.
Payouts maintains infrastructure and platform-level backups that support system recovery and data restoration capabilities. These backups are taken regularly and retained in accordance with internal data retention policies. Restoration procedures are documented and designed to enable recovery of essential systems and services.
While formal disaster recovery testing is not currently conducted, the organization has the capability to restore critical systems and data based on predefined recovery steps. This capability is supported by cloud-based infrastructure, automated backup processes, and role-based access to restoration tools.
Payouts continuously reviews and updates its BC/DR documentation to reflect changes in systems, personnel, and business needs, ensuring preparedness and alignment with evolving risks and operational priorities.

Confidentiality

Customer confidentiality is a key factor in Payouts. As such, Payouts has implemented security measures to ensure the confidentiality of its customer's sensitive personal information. The security measures aim to prevent unauthorized access, disclosure, alteration or destruction of sensitive personal information.

Data Encryption

Data in transit:
Payouts utilizes an ALB to manage incoming traffic, which acts as a termination point for TLS connections. This ensures that all data exchanged between clients and services is encrypted during transmission.

The TLS configuration on load balancer adheres to best practices and industry standards to ensure the security and integrity of data in transit. This includes the use of strong cryptographic algorithms and key lengths, as well as regular updates and patching to mitigate any vulnerabilities.

Communication to RDS also employs TLS for encryption. This ensures that all data transmitted between the application servers and the RDS instance is encrypted, further enhancing the security of data in transit. The TLS configuration for RDS

is configured to meet best practices and industry standards, including the use of strong cryptographic algorithms and regular updates to maintain security.

Data at rest:
Payouts' s data is stored in Amazon S3 and Amazon RDS and encrypted using industry-standard encryption algorithms. In Amazon S3, data is encrypted using the AES-256 algorithm. This ensures that all objects stored in S3 are encrypted at rest, providing an additional layer of security for our data.

Similarly, in Amazon RDS, data is encrypted using the same AES-256 algorithm. This means that all data stored in RDS instances, including databases and backups, is encrypted at rest. This encryption helps protect the data from unauthorized access and ensures its confidentiality and integrity.

To manage the encryption keys securely, Payouts uses AWS KMS They. KMS allows to create and control encryption keys used to encrypt data in S3 and RDS. By using KMS, Payouts can enforce access controls, audit encryption key usage, and rotate encryption keys regularly, further enhancing the security of Payouts's data.

Changes in Controls

There were no changes in controls during the period under examination that would affect user entities' understanding of the Payouts.com Platform and the services provided.

In addition to this, minor changes to processes and procedures were implemented to continually improve Payouts Technologies Ltd..'s security and operations for clients.

Criteria not applicable to the system

All Common Criteria/Security, Security criteria were applicable to the Payouts Technologies Ltd..'s The primary offering of Payouts Technologies L.B.O. Ltd. is Finance Operations Platform, a comprehensive solution that aligns marketing and financial operations. This platform is the focal point of customer interaction and the core of the product suite. Designed with an emphasis on efficiency and transparency, it incorporates sophisticated functionalities such as real-time budget management, streamlined payments to vendors, cash flow forecasting, and instant financing. These features are specifically tailored to facilitate smooth financial operations for marketing teams. Payouts's Finance Operations Platform adheres strictly to SOC 2 standards, demonstrating commitment to data security and integrity. This platform is the cornerstone of services and the embodiment of mission to revolutionize financial operations within the marketing realm. system.

Report Use

The Description does not omit or distort information relevant to the Platform while acknowledging that the Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

Subservice organizations

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

Subservice description of services

The Cloud Hosting Services provided by AWS support the physical infrastructure of the entity's services.

Complementary Subservice Organization Controls

Payouts Technologies Ltd..'s services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Payouts Technologies Ltd..'s services to be solely achieved by Payouts Technologies Ltd. control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Payouts Technologies Ltd..

The following subservice organization controls have been implemented by AWS and included in this report to provide additional assurance that the trust services criteria are met.

Category	Applicable Trust Services Criteria	Complementary Subservice Organization Controls
Security	CC 6.4	Physical access to data centers is approved by an authorized individual.
Security	CC 6.4	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
Security	CC 6.4	Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
Security	CC 6.4	Closed circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
Security	CC 6.4	Access to server locations is managed by electronic access control devices.
Availability	A 1.2	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment.
Availability	A 1.2	AWS has a process in place to review environmental and geo-political risks before launching a new region.
Availability	A 1.2	Amazon-owned data centers are protected by fire detection and suppression systems.
Availability	A 1.2	Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
Availability	A 1.2	Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon owned data centers
Availability	A 1.2	Amazon-owned data centers have generators to provide backup power in case of electrical failure.
Availability	A 1.2	Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies. Contracts also include provisions requiring

Category	Applicable Trust Services Criteria	Complementary Subservice Organization Controls
		communication of incidents or events that impact Amazon assets and/or customers to AWS.

The Company also utilizes other, less significant, third-party service organizations to support its services. These organizations are generally referred to as vendors.

Payouts Technologies Ltd. management, along with the subservice provider, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Payouts Technologies Ltd. performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organization(s)
- Making regular site visits to vendor and subservice organization(s') facilities
- Testing controls performed by vendors and subservice organization(s)
- Reviewing attestation reports on services provided by vendors and subservice organization(s)
- Monitoring external communications, such as customer complaints relevant to the services of the subservice organization

Complementary User Entity Controls (CUECs)

In designing its system, Payouts allows for certain complementary controls to be implemented by user organizations to meet certain criteria applicable to security. A customer organization's overall internal control structure should be in operation and evaluated in conjunction with Payouts's controls presented in this section of the report.

The Kost Forer Gabbay and Kasierer (KFGK) examination was limited to the design of the controls in place at Payouts as they relate to Payouts's customers. Accordingly, the examination did not extend to any controls beyond those listed in this report or those in place at customer organizations. The Complementary User Entity Controls section describes controls that have to be placed in operation at customers to complement Payouts's controls. It is each interested party's responsibility to evaluate the user entity control considerations presented in this section in relation to the internal controls that are in place at customer organizations in order to obtain a complete understanding of the total internal control structure surrounding the Payouts hosted services and application and to assess risk control. The portions of the internal control provided by the customer organizations are to be evaluated together with Payouts. If effective internal customer organization controls are not in place, Payouts's controls may not be adequate to compensate for such weaknesses. Furthermore, this list is only a partial list of controls that customer organizations should have in place in order to complement the controls of Payouts.

#	Complementary User Entity Controls	Criteria
1	Implementing sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with Payouts.	CC6.1, CC6.2, CC6.6
2	Ensuring timely removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with Payouts's services.	CC6.2, CC6.3
3	Maintaining authorized, secure, timely, and complete transactions for user organizations relating to Payouts's services.	CC7.2, CC7.3

4	Protecting data that is sent to Payouts by using appropriate methods to ensure confidentiality, privacy, integrity, availability, and non-repudiation.	CC6.6
5	Implementing controls requiring additional approval procedures for critical transactions relating to Payouts's services.	CC6.3, CC7.3
6	Reporting to Payouts in a timely manner any material changes to their overall control environment that may adversely affect services being performed by Payouts.	CC4.1, CC9.2
7	Notifying Payouts in a timely manner of any changes to personnel directly involved with services performed by Payouts. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by Payouts.	CC9.2, CC2.2
8	Adhering to the terms and conditions stated within their contracts with Payouts.	CC1.2, CC2.1
9	Developing, and if necessary, implementing a business continuity and disaster recovery plan (DRP) that will aid in the continuation of services provided by Payouts.	CC7.4
10	Validating the accuracy and appropriateness of information submitted through the Payouts AI Service to ensure that inputs are suitable for their intended use and do not include unnecessary sensitive data.	CC7.2
11	Reviewing AI-generated outputs provided by the Payouts AI Service prior to relying on them for business or operational decisions to ensure the results meet the customer's requirements.	CC7.2, CC7.3
12	Safeguarding access credentials, API keys, and authentication mechanisms used to interact with the Payouts AI Service, ensuring that only authorized personnel have access.	CC6.1, CC6.2, CC6.4
13	Customers are responsible for monitoring their own usage of Payouts and reviewing logs or alerts provided to detect unauthorized or anomalous activity.	CC7.2, CC7.3
14	Customers are responsible for defining and enforcing data retention, deletion, and archival policies for data submitted to or generated by Payouts services.	CC8.1, CC8.2
15	Customers should establish and enforce acceptable use policies governing employee interaction with Payouts's AI services, including restrictions on prohibited or high-risk use cases.	CC1.1, CC2.1

.

Section IV - Description of Criteria, Controls, Tests and Results of Tests

Testing Performed and Results of Tests of Entity-Level Controls

In planning the nature, timing and extent of its testing of the controls specified by Payouts, KFGK considered the aspects of the Payouts control environment, risk assessment processes, information and communication and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For tests of controls requiring the use of IPE, including Electronic Audit Evidence (EAE) (e.g., controls requiring system-generated populations for sample-based testing), we performed a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspect the source of the IPE, (2) inspect the query, script, or parameters used to generate the IPE, (3) tie data between the IPE and the source, and/or (4) inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity. In addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), we inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Criteria and controls

On the pages that follow, the applicable Trust Services Criteria and the controls to meet the criteria have been specified by and are the responsibility of Payouts. The testing performed by Kost Forer Gabbay and Kasierer (KFGK) and the results of tests are the responsibility of the service auditor. Refer to the Trust Services criteria mapping section for the mapping of these controls to the Trust Services criteria.

Control Environment

CC1.1 / COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
11	The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	Inspected the code of conduct acknowledgement evidence for a sample new contractor and determined that Payouts required contractors to acknowledge a code of conduct at the time of hire.	No deviations noted.
12	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with disciplinary policy.	Inspected the code of conduct acknowledgement evidence for a sample of new employees and determined that Payouts required employees to acknowledge a code of conduct at the time of hire. Inspected the Payouts's code of conduct and determined that policy was established where employees who violate the code of conduct were subject to disciplinary actions in accordance with a disciplinary policy. No violation occurred during the audit period.	No deviations noted.
26	The company performs reference checks on new employees.	Inspected the reference check evidence of new employees and determined that Payouts performed reference checks on new employees.	No deviations noted.

CC1.2 / COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
8	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the Board Charter official documentation and determined that Company had documented charter that outlined its oversight responsibilities for internal control.	No deviations noted.
9	The company's board of directors meets at least annually and maintains formal meeting minutes.	Inspected the board meeting minutes and determined that Payouts's board of directors met at least annually and maintained formal meeting minutes	No deviations noted.

CC1.3 / COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
33	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected management roles and responsibilities policy and determined Payouts management established defined roles and responsibilities to oversee the design and implementation of information security controls.	No deviations noted.
36	The company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected the organizational chart and determined that Payouts maintained an organizational chart that described the organizational structure and reporting lines.	No deviations noted.
48	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the roles and responsibilities policy.	Inspected information security roles and responsibilities policy and an example of job description and determined that roles and responsibilities of the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in job descriptions or the roles and responsibilities policy.	No deviations noted.

CC1.4 / COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
26	The company performs reference checks on new employees.	Inspected the reference check evidence of new employees and determined that Payouts performed reference checks on new employees.	No deviations noted.
48	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the roles and responsibilities policy.	Inspected information security roles and responsibilities policy and an example of job description and determined that roles and responsibilities of the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in job descriptions or the roles and responsibilities policy.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
49	The company requires employees to complete security awareness training within thirty days of hire.	Inspected the security awareness training for a sample of new employees and determined that new employees completed security awareness training within thirty days of hire.	No deviations noted.

CC1.5 / COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
11	The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	Inspected the code of conduct acknowledgement evidence for a sample new contractor and determined that Payouts required contractors to acknowledge a code of conduct at the time of hire.	No deviations noted.
12	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with disciplinary policy.	Inspected the code of conduct acknowledgement evidence for a sample of new employees and determined that Payouts required employees to acknowledge a code of conduct at the time of hire. Inspected the Payouts's code of conduct and determined that policy was established where employees who violate the code of conduct were subject to disciplinary actions in accordance with a disciplinary policy. No violation occurred during the audit period.	No deviations noted.
48	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the roles and responsibilities policy.	Inspected information security roles and responsibilities policy and an example of job description and determined that roles and responsibilities of the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in job descriptions or the roles and responsibilities policy.	No deviations noted.

Communication and Information

CC2.1 / COSO Principle 13: The entity obtains or generates or uses relevant, quality information to support the functioning of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
32	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the logs from the compliance monitoring tool and determined that log management tool was utilized to identify events that may have a potential impact on Payouts's ability to achieve its security objectives.	No deviations noted.
62	Host-based vulnerability scans are performed continuously on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the integration with GitHub in the compliance monitoring tool and the dashboard for vulnerability scanning and determined that host-based vulnerability scans were performed continuously on external-facing systems.	No deviations noted.

CC2.2 / COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
30	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the incident response policy and determined that Payouts had security and privacy incident response policies and procedures that were documented and communicated to authorized users.	No deviations noted.
33	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected management roles and responsibilities policy and determined Payouts management established defined roles and responsibilities to oversee the design and implementation of information security controls.	No deviations noted.
48	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the roles and responsibilities policy.	Inspected information security roles and responsibilities policy and an example of job description and determined that roles and responsibilities of the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in job descriptions or the roles and responsibilities policy.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
49	The company requires employees to complete security awareness training within thirty days of hire.	Inspected the security awareness training for a sample of new employees and determined that new employees completed security awareness training within thirty days of hire.	No deviations noted.
50	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the information security policy and determined that Payouts's information security policies and procedures were documented and reviewed at least annually.	No deviations noted.
51	The company provides a description of its products and services to internal and external users.	Inspected Payouts's website and determined that company provided a description of its products and services to internal and external users.	No deviations noted.
64	The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.	Inspected the whistleblower policy and determined that Payouts established a formalized whistleblower policy. Inspected the google form configured for anonymous reporting and determined that an anonymous communication channel was in place for users to report potential issues or fraud concerns.	No deviations noted.

CC2.3 / COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
13	The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Inspected Payouts's website and determine that company's security commitments were communicated to customers through Terms of Service.	No deviations noted.
28	The company provides guidelines and technical support resources relating to system operations to customers.	Inspected Payouts's website and determined that company had guidelines and technical support resources relating to system operations available to customers.	No deviations noted.
51	The company provides a description of its products and services to internal and external users.	Inspected Payouts's website and determined that company provided a description of its products and services to internal and external users.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
53	The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected Payouts's website and determined that Payouts had an external-facing support system in place that allowed users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	No deviations noted.
54	The company communicated system changes to authorized internal users	Inspected Payouts's internal communication tool and determined that company communicated system changes to authorized internal users.	No deviations noted.
55	The company notifies customers of critical system changes that may affect their processing.	Inspected Payouts's website and determined that company notified customers of critical system changes that may affect their processing.	No deviations noted.
56	The company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the link to the agreement with the infrastructure provider and determined that Payouts had a written agreements in place with vendors and related third parties that included confidentiality and privacy commitments applicable to entity.	No deviations noted.

Risk Assessment

CC3.1 / COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
45	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the risk assessment objectives and determined that Company specified its objectives in order to identify and assess risk associated with the objectives.	No deviations noted.
46	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy and determined that Company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No deviations noted.
47	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk assessment exercise and determined that Payouts's risk assessments were performed at least annually. Inspected the risk assessment exercise and determined that the risk assessment process, threats and changes (environmental, regulatory, and technological) to service commitments were identified and the risks were formally assessed. Inspected the risk assessment exercise and determined that the risk assessment included a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	No deviations noted.

CC3.2 / COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
17	The company has Business Continuity and Disaster Recovery Plan in place that outlines communication plans in order to maintain security continuity in the event of the unavailability of key personnel.	Inspected the business continuity and disaster recovery plan and determined that the BC/DR plan in place outlined communication plans to maintain information security continuity.	No deviations noted.
18	The company has a documented business continuity/disaster recovery (BC/DR) plan.	Inspected the Business Continuity and Disaster Recovery plan and determined that Company had a documented business continuity/disaster recovery (BC/DR) plan.	No deviations noted.
38	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the penetration test report and determined that the company's penetration testing was performed at least annually. A remediation plan was developed, and changes were implemented to remediate vulnerabilities in accordance with SLAs. Inspected the results of the penetration test and determined that high issues were remediate in accordance with SLA's.	No deviations noted.
46	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy and determined that Company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No deviations noted.
47	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk assessment exercise and determined that Payouts's risk assessments were performed at least annually. Inspected the risk assessment exercise and determined that the risk assessment process, threats and changes (environmental, regulatory, and technological) to	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		service commitments were identified and the risks were formally assessed. Inspected the risk assessment exercise and determined that the risk assessment included a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	
60	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	I have invested in the third-party management policy and determined that Company had a vendor management program in place. Components of the program included: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	No deviations noted.

CC3.3 / COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
46	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy and determined that Company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No deviations noted.
47	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk assessment exercise and determined that Payouts's risk assessments were performed at least annually. Inspected the risk assessment exercise and determined that the risk assessment process, threats and changes (environmental, regulatory, and technological) to service commitments were identified and the risks were formally assessed.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected the risk assessment exercise and determined that the risk assessment included a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	

CC3.4 / COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
16	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the configuration management procedure test from monitoring compliance tool and determined that Payouts had a configuration management procedure to ensure that system configurations were consistently deployed throughout the environment.	No deviations noted.
38	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the penetration test report and determined that the company's penetration testing was performed at least annually. A remediation plan was developed, and changes were implemented to remediate vulnerabilities in accordance with SLAs. Inspected the results of the penetration test and determined that high issues were remediate in accordance with SLA's.	No deviations noted.
46	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy and determined that Company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No deviations noted.
47	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified	Inspected the risk assessment exercise and determined that Payouts's risk assessments were performed at least annually.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk assessment exercise and determined that the risk assessment process, threats and changes (environmental, regulatory, and technological) to service commitments were identified and the risks were formally assessed. Inspected the risk assessment exercise and determined that the risk assessment included a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	

Monitoring Activities

CC4.1 / COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
38	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the penetration test report and determined that the company's penetration testing was performed at least annually. A remediation plan was developed, and changes were implemented to remediate vulnerabilities in accordance with SLAs. Inspected the results of the penetration test and determined that high issues were remediate in accordance with SLA's.	No deviations noted.
62	Host-based vulnerability scans are performed continuously on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the integration with GitHub in the compliance monitoring tool and the dashboard for vulnerability scanning and determined that host-based vulnerability scans were performed continuously on external-facing systems.	No deviations noted.

CC4.2 / COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
38	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the penetration test report and determined that the company's penetration testing was performed at least annually. A remediation plan was developed, and changes were implemented to remediate vulnerabilities in accordance with SLAs. Inspected the results of the penetration test and determined that high issues were remediate in accordance with SLA's.	No deviations noted.

Control Activities

CC5.1 / COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the access control policy document and determine that Payouts's the policy documented the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	No deviations noted.
46	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy and determined that Company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No deviations noted.
47	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk assessment exercise and determined that Payouts's risk assessments were performed at least annually. Inspected the risk assessment exercise and determined that the risk assessment process, threats and changes (environmental, regulatory, and technological) to service commitments were identified and the risks were formally assessed. Inspected the risk assessment exercise and determined that the risk assessment included a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	No deviations noted.
50	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the information security policy and determined that Payouts's information security policies	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		and procedures were documented and reviewed at least annually.	

CC5.2 / COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
25	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the System development life cycle (SDLC) policy document and determined that Company had a formal systems development life cycle (SDLC) methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No deviations noted.
38	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the penetration test report and determined that the company's penetration testing was performed at least annually. A remediation plan was developed, and changes were implemented to remediate vulnerabilities in accordance with SLAs. Inspected the results of the penetration test and determined that high issues were remediate in accordance with SLA's.	No deviations noted.
50	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the information security policy and determined that Payouts's information security policies and procedures were documented and reviewed at least annually.	No deviations noted.

CC5.3 / COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
7	The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the operations security policy and determined that Company's data backup policy had documented	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		requirements for backup and recovery of customer data.	
10	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. The company uses a tool to manage and prioritize changes.	Inspected the change management tickets for a sample of commits and determined that changes to the software and infrastructure were authorized and formally documented before implemented in the production environment. Inspected the test pipeline for a sample of committees and determined that changes to the software were tested prior to being implemented in the production environment. I have inspected the merge request for a sample of committees and determined that changes to the software and infrastructure were reviewed and approved before implemented in the production environment.	No deviations noted.
23	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the data management policy and procedure and determined that Payouts had a formal retention and disposal procedures in place to guide the secure retention and disposal of Payouts and customer data.	No deviations noted.
25	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the System development life cycle (SDLC) policy document and determined that Company had a formal systems development life cycle (SDLC) methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No deviations noted.
30	The company has security and privacy incident response policies and procedures that are	Inspected the incident response policy and determined that Payouts had security and privacy incident response	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	documented and communicated to authorized users.	policies and procedures that were documented and communicated to authorized users.	
40	The company performs periodic backups for production data. Data is backed up to a different location than the production system.	Inspected RDS backup configuration from AWS and determined that Payouts performed periodic backups for production data. Data was backed up to a different location than the production system.	No deviations noted.
45	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the risk assessment objectives and determined that Company specified its objectives in order to identify and assess risk associated with the objectives.	No deviations noted.
46	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy and determined that Company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No deviations noted.
47	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk assessment exercise and determined that Payouts's risk assessments were performed at least annually. Inspected the risk assessment exercise and determined that the risk assessment process, threats and changes (environmental, regulatory, and technological) to service commitments were identified and the risks were formally assessed. Inspected the risk assessment exercise and determined that the risk assessment included a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
48	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the roles and responsibilities policy.	Inspected information security roles and responsibilities policy and an example of job description and determined that roles and responsibilities of the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in job descriptions or the roles and responsibilities policy.	No deviations noted.
50	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the information security policy and determined that Payouts's information security policies and procedures were documented and reviewed at least annually.	No deviations noted.

Logical and Physical Access Controls

CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the access control policy document and determine that Payouts's the policy documented the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	No deviations noted.
2	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the access request evidence for a sample of new employees and determined that user access to in-scope system components was based on job role and function or required a documented access request form and manager approval prior to access being provisioned.	No deviations noted.
21	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the data management policy and determined that a data classification policy was in place to ensure that confidential data was properly secured and restricted to authorized personnel.	No deviations noted.
22	The company's datastores housing sensitive customer data are encrypted at rest.	Inspected the AWS encryption setup test from monitoring compliance tool and determined that Payouts's datastores housing sensitive customer data were encrypted at rest.	No deviations noted.
27	The company restricts privileged access to encryption keys to authorized users with a business need.	Inspected the cryptography policy document and determined that Payouts restricted privileged access to encryption keys to authorized users with a business need. Inspected the list of users and their job titles and determined that Payouts reviewed and restricted privileged access to encryption keys to authorized users with a business need.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
35	The company's network is segmented to prevent unauthorized access to customer data.	Inspected AWS VPCs and determined that Company's network was segmented to prevent unauthorized access to customer data.	No deviations noted.
37	The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected the password policy and determined that passwords were required for in-scope system components to be configured. Inspected the authentication configuration test from monitoring compliance tool and determined that passwords were required for in-scope system components to be configured according to Company's policy.	No deviations noted.
41	The company restricts privileged access to databases to authorized users with a business need.	Inspected the list of users with privileged access to databases and their job titles and determined that Payouts restricted privileged access to the application to authorized users with a business need.	No deviations noted.
42	The company restricts access to migrate changes to production to authorized personnel.	Inspected the list of users with access to migrant changes to production and their job titles and determined that Company restricted access to migrant changes to authorized personnel.	No deviations noted.
57	The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	Inspected the company's authentication to system and determined that Payouts required authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	No deviations noted.
58	The company requires authentication of the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the company's authentication to the production network and determined that Payouts required authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No deviations noted.
59	The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key.	Inspected the company's authentication to the production datastores and determined that Payouts required authentication to production datastores to use	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		authorized secure authentication mechanisms using unique SSH key.	

CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the access control policy document and determine that Payouts's the policy documented the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	No deviations noted.
2	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the access request evidence for a sample of new employees and determined that user access to in-scope system components was based on job role and function or required a documented access request form and manager approval prior to access being provisioned.	No deviations noted.
3	The company conducts access reviews at least semi-annually for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the user access review documentation and determined that company conducted access review at least semi-annually for the in-scope system components to ensure that access was restricted appropriately.	No deviations noted.
4	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the information security policy and determined that the company had a process to ensure that access was revoked for terminated employees within SLAs.	No deviations noted.
41	The company restricts privileged access to databases to authorized users with a business need.	Inspected the list of users with privileged access to databases and their job titles and determined that Payouts restricted privileged access to the application to authorized users with a business need.	No deviations noted.
42	The company restricts access to migrate changes to production to authorized personnel.	Inspected the list of users with access to migrant changes to production and their job titles and	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		determined that Company restricted access to migrant changes to authorized personnel.	

CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the access control policy document and determine that Payouts's the policy documented the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	No deviations noted.
2	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the access request evidence for a sample of new employees and determined that user access to in-scope system components was based on job role and function or required a documented access request form and manager approval prior to access being provisioned.	No deviations noted.
3	The company conducts access reviews at least semi-annually for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the user access review documentation and determined that company conducted access review at least semi-annually for the in-scope system components to ensure that access was restricted appropriately.	No deviations noted.
4	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the information security policy and determined that the company had a process to ensure that access was revoked for terminated employees within SLAs.	No deviations noted.
41	The company restricts privileged access to databases to authorized users with a business need.	Inspected the list of users with privileged access to databases and their job titles and determined that Payouts restricted privileged access to the application to authorized users with a business need.	No deviations noted.
42	The company restricts access to migrate changes to production to authorized personnel.	Inspected the list of users with access to migrant changes to production and their job titles and	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		determined that Company restricted access to migrant changes to authorized personnel.	

CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
3	The company conducts access reviews at least semi-annually for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the user access review documentation and determined that company conducted access review at least semi-annually for the in-scope system components to ensure that access was restricted appropriately.	No deviations noted.
39	The company has processes in place for granting, changing, and terminating physical access to company offices based on authorization from control owners.	Inspected the physical security policy and determined that company had processes in place for granting, changing, and terminating physical access to Payouts's offices based on an authorization from control owners.	No deviations noted.
61	The company requires visitors to sign-in, wear a visitor badge, and be escorted by an authorized employee when accessing the data center or secure areas.	Inspected the physical access policy and determined that visitors were required to sign-in, wear a visitor badge, and be escorted by an authorized employee when accessing the data center or secure areas.	No deviations noted.

CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the information security policy and determined that the company had a process to ensure that access was revoked for terminated employees within SLAs.	No deviations noted.
6	Company has defined procedures that outline the purging or destroying of electronic media containing confidential information.	Inspected the asset management policy and determined that asset disposal procedure was documented.	No deviations noted.
20	The company purges or removes customer data containing confidential information from the	Inspected the data management policy and determined that Payouts purged or removed customer data	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	application environment, in accordance with best practices, when customers leave the service.	containing confidential information from the application environment in accordance with best practices, when customers leave the service. No customer termination request occurred during the audit period.	
23	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the data management policy and procedure and determined that Payouts had a formal retention and disposal procedures in place to guide the secure retention and disposal of Payouts and customer data.	No deviations noted.

CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
24	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected SSL/TLS encryption configuration test from monitoring compliance tool and determined that Payouts used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No deviations noted.
34	The company uses security groups and configures them to prevent unauthorized access.	Inspected the security groups test from monitoring compliance tool and determined that Payouts used security groups and configured them to prevent unauthorized access.	No deviations noted.
52	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the patch evidence extract from monitoring compliance tool and determined that Company infrastructure was patched as part of routine maintenance and ensured that servers supporting the service were hardened against security threats.	No deviations noted.

CC6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
24	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected SSL/TLS encryption configuration test from monitoring compliance tool and determined that Payouts used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No deviations noted.

CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
5	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on relevant systems.	Inspected the configuration policy and determined that company deployed anti-malware technology to environments commonly susceptible to malicious attacks and configured this to be updated routinely, logged, and installed on relevant systems.	No deviations noted.
25	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the System development life cycle (SDLC) policy document and determined that Company had a formal systems development life cycle (SDLC) methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No deviations noted.
52	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the patch evidence extract from monitoring compliance tool and determined that Company infrastructure was patched as part of routine maintenance and ensured that servers supporting the service were hardened against security threats.	No deviations noted.

System Operations

CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
10	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. The company uses a tool to manage and prioritize changes.	Inspected the change management tickets for a sample of commits and determined that changes to the software and infrastructure were authorized and formally documented before implemented in the production environment. Inspected the test pipeline for a sample of committees and determined that changes to the software were tested prior to being implemented in the production environment. I have inspected the merge request for a sample of committees and determined that changes to the software and infrastructure were reviewed and approved before implemented in the production environment.	No deviations noted.
16	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the configuration management procedure test from monitoring compliance tool and determined that Payouts had a configuration management procedure to ensure that system configurations were consistently deployed throughout the environment.	No deviations noted.
62	Host-based vulnerability scans are performed continuously on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the integration with GitHub in the compliance monitoring tool and the dashboard for vulnerability scanning and determined that host-based vulnerability scans were performed continuously on external-facing systems.	No deviations noted.
63	The company's formal policies outline the requirements for the following functions related to	Inspected the operations security policy and determined the policy outlined the requirements for the following	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	IT / Engineering: - vulnerability management; - system monitoring.	functions related to IT / Engineering: - vulnerability management; - system monitoring.	

CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
31	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected load balancers test from monitoring compliance tool and determined that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met.	No deviations noted.
32	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the logs from the compliance monitoring tool and determined that log management tool was utilized to identify events that may have a potential impact on Payouts's ability to achieve its security objectives.	No deviations noted.
52	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the patch evidence extract from monitoring compliance tool and determined that Company infrastructure was patched as part of routine maintenance and ensured that servers supporting the service were hardened against security threats.	No deviations noted.
62	Host-based vulnerability scans are performed continuously on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the integration with GitHub in the compliance monitoring tool and the dashboard for vulnerability scanning and determined that host-based vulnerability scans were performed continuously on external-facing systems.	No deviations noted.
63	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the operations security policy and determined the policy outlined the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	No deviations noted.

CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
29	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the incident response policy and determined that Payouts's security and privacy incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. No security incidents occurred during the audit period.	No deviations noted.
30	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the incident response policy and determined that Payouts had security and privacy incident response policies and procedures that were documented and communicated to authorized users.	No deviations noted.
31	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected load balancers test from monitoring compliance tool and determined that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met.	No deviations noted.

CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
29	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the incident response policy and determined that Payouts's security and privacy incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. No security incidents occurred during the audit period.	No deviations noted.
30	The company has security and privacy incident response policies and procedures that are	Inspected the incident response policy and determined that Payouts had security and privacy incident response	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	documented and communicated to authorized users.	policies and procedures that were documented and communicated to authorized users.	
52	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the patch evidence extract from monitoring compliance tool and determined that Company infrastructure was patched as part of routine maintenance and ensured that servers supporting the service were hardened against security threats.	No deviations noted.
62	Host-based vulnerability scans are performed continuously on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the integration with GitHub in the compliance monitoring tool and the dashboard for vulnerability scanning and determined that host-based vulnerability scans were performed continuously on external-facing systems.	No deviations noted.

CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
17	The company has Business Continuity and Disaster Recovery Plan in place that outlines communication plans in order to maintain security continuity in the event of the unavailability of key personnel.	Inspected the business continuity and disaster recovery plan and determined that the BC/DR plan in place outlined communication plans to maintain information security continuity.	No deviations noted.
18	The company has a documented business continuity/disaster recovery (BC/DR) plan.	Inspected the Business Continuity and Disaster Recovery plan and determined that Company had a documented business continuity/disaster recovery (BC/DR) plan.	No deviations noted.
29	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the incident response policy and determined that Payouts's security and privacy incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. No security incidents occurred during the audit period.	No deviations noted.
30	The company has security and privacy incident response policies and procedures that are	Inspected the incident response policy and determined that Payouts had security and privacy incident response	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	documented and communicated to authorized users.	policies and procedures that were documented and communicated to authorized users.	

Change Management

CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
10	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. The company uses a tool to manage and prioritize changes.	Inspected the change management tickets for a sample of commits and determined that changes to the software and infrastructure were authorized and formally documented before implemented in the production environment. Inspected the test pipeline for a sample of committees and determined that changes to the software were tested prior to being implemented in the production environment. I have inspected the merge request for a sample of committees and determined that changes to the software and infrastructure were reviewed and approved before implemented in the production environment.	No deviations noted.
25	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the System development life cycle (SDLC) policy document and determined that Company had a formal systems development life cycle (SDLC) methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
42	The company restricts access to migrate changes to production to authorized personnel.	Inspected the list of users with access to migrant changes to production and their job titles and determined that Company restricted access to migrant changes to authorized personnel.	No deviations noted.
52	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the patch evidence extract from monitoring compliance tool and determined that Company infrastructure was patched as part of routine maintenance and ensured that servers supporting the service were hardened against security threats.	No deviations noted.
62	Host-based vulnerability scans are performed continuously on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the integration with GitHub in the compliance monitoring tool and the dashboard for vulnerability scanning and determined that host-based vulnerability scans were performed continuously on external-facing systems.	No deviations noted.

Risk Mitigation

CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
46	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy and determined that Company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No deviations noted.
47	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk assessment exercise and determined that Payouts's risk assessments were performed at least annually. Inspected the risk assessment exercise and determined that the risk assessment process, threats and changes (environmental, regulatory, and technological) to service commitments were identified and the risks were formally assessed. Inspected the risk assessment exercise and determined that the risk assessment included a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	No deviations noted.

CC9.2: The entity assesses and manages risks associated with vendors and business partners.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
56	The company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the link to the agreement with the infrastructure provider and determined that Payouts had a written agreements in place with vendors and related third parties that included confidentiality and privacy commitments applicable to entity.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
60	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	I have invested in the third-party management policy and determined that Company had a vendor management program in place. Components of the program included: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	No deviations noted.

Availability

A1.1: The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
44	The company has a multi-location strategy for production environments employed to permit the resumption of operations at other company data centers in the event of loss of a facility.	Inspected configuration evidence from cloud provider and determined that Payouts had a multi-location strategy for production environments employed to permit the resumption of operations at other company data centers in the event of loss of a facility.	No deviations noted.

A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
7	The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the operations security policy and determined that Company's data backup policy had documented requirements for backup and recovery of customer data.	No deviations noted.
17	The company has Business Continuity and Disaster Recovery Plan in place that outlines communication plans in order to maintain security continuity in the event of the unavailability of key personnel.	Inspected the business continuity and disaster recovery plan and determined that the BC/DR plan in place outlined communication plans to maintain information security continuity.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
18	The company has a documented business continuity/disaster recovery (BC/DR) plan.	Inspected the Business Continuity and Disaster Recovery plan and determined that Company had a documented business continuity/disaster recovery (BC/DR) plan.	No deviations noted.
40	The company performs periodic backups for production data. Data is backed up to a different location than the production system.	Inspected RDS backup configuration from AWS and determined that Payouts performed periodic backups for production data. Data was backed up to a different location than the production system.	No deviations noted.
44	The company has a multi-location strategy for production environments employed to permit the resumption of operations at other company data centers in the event of loss of a facility.	Inspected configuration evidence from cloud provider and determined that Payouts had a multi-location strategy for production environments employed to permit the resumption of operations at other company data centers in the event of loss of a facility.	No deviations noted.
46	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy and determined that Company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No deviations noted.
47	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk assessment exercise and determined that Payouts's risk assessments were performed at least annually. Inspected the risk assessment exercise and determined that the risk assessment process, threats and changes (environmental, regulatory, and technological) to service commitments were identified and the risks were formally assessed. Inspected the risk assessment exercise and determined that the risk assessment included a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	No deviations noted.

A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
7	The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the operations security policy and determined that Company's data backup policy had documented requirements for backup and recovery of customer data.	No deviations noted.
17	The company has Business Continuity and Disaster Recovery Plan in place that outlines communication plans in order to maintain security continuity in the event of the unavailability of key personnel.	Inspected the business continuity and disaster recovery plan and determined that the BC/DR plan in place outlined communication plans to maintain information security continuity.	No deviations noted.
18	The company has a documented business continuity/disaster recovery (BC/DR) plan.	Inspected the Business Continuity and Disaster Recovery plan and determined that Company had a documented business continuity/disaster recovery (BC/DR) plan.	No deviations noted.
40	The company performs periodic backups for production data. Data is backed up to a different location than the production system.	Inspected RDS backup configuration from AWS and determined that Payouts performed periodic backups for production data. Data was backed up to a different location than the production system.	No deviations noted.

Confidentiality

C1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
21	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the data management policy and determined that a data classification policy was in place to ensure that confidential data was properly secured and restricted to authorized personnel.	No deviations noted.
23	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the data management policy and procedure and determined that Payouts had a formal retention and disposal procedures in place to guide the secure retention and disposal of Payouts and customer data.	No deviations noted.
24	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected SSL/TLS encryption configuration test from monitoring compliance tool and determined that Payouts used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No deviations noted.
56	The company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the link to the agreement with the infrastructure provider and determined that Payouts had a written agreements in place with vendors and related third parties that included confidentiality and privacy commitments applicable to entity.	No deviations noted.
57	The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	Inspected the company's authentication to system and determined that Payouts required authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	No deviations noted.
58	The company requires authentication of the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the company's authentication to the production network and determined that Payouts required authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
59	The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key.	Inspected the company's authentication to the production datastores and determined that Payouts required authentication to production datastores to use authorized secure authentication mechanisms using unique SSH key.	No deviations noted.

C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
20	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inspected the data management policy and determined that Payouts purged or removed customer data containing confidential information from the application environment in accordance with best practices, when customers leave the service. No customer termination request occurred during the audit period.	No deviations noted.

****